

IBM Security QRadar Network Anomaly Detection
Version 7.1.0 (MR1)

Guide d'utilisation



Remarque : Avant d'utiliser le présent document et le produit associé, lisez les informations dans [“Avis et Marques”](#) à page 425.

SOMMAIRE

A PROPOS DE CE MANUEL

Utilisateurs concernés	1
Conventions	1
Documentation technique	2
Contacteur le service clients	2

1 A PROPOS DE IBM SECURITY QRADAR NETWORK ANOMALY DETECTION

Navigateurs Web pris en charge	3
Activation de Compatibility View pour Internet Explorer	4
Connexion à QRadar Network Anomaly Detection	4
Onglet Dashboard	5
Onglet Offenses	5
Onglet Log Activity	5
Onglet Network Activity	5
Onglet Assets	6
Onglet Reports	6
Utilisation de QRadar Network Anomaly Detection	6
Tri de résultats	7
Actualisation de l'interface utilisateur	7
Mise en pause l'interface utilisateur	7
Etude des adresses IP	7
Etude des noms d'utilisateur	10
Affichage de l'heure du système	10
Mise à jour des détails de l'utilisateur	10
Accès à l'aide en ligne	11
Redimensionnement des colonnes	11
Configuration du format de page	11
Onglet Admin	12

2 UTILISATION DE L'ONGLET DASHBOARD

A propos de Dashboards	13
Gérer Dashboards	16
Affichage d'un tableau de bord	16
Création d'un tableau de bord personnalisé	17
Ajout d'articles	17

Etude de données à partir des éléments du tableau de bord	17
Configuration des graphiques	18
Suppression d'éléments	21
Détachement d'un élément	21
Modification d'un tableau de bord	21
Suppression d'un tableau de bord	22
Eléments du tableau de bord	22
Eléments de recherche de flux	22
Eléments de violation	23
Eléments d'activité de journal	24
Eléments de rapports	25
Eléments des récapitulatifs du système	26
Eléments de notifications du système	26
Centre de documentation des menaces Internet	28
Ajout d'éléments de tableau de bord basés sur des recherches à la liste d'ajout des éléments	28

3 ETUDE DES VIOLATIONS

Présentation de l'onglet l'onglet Offense	31
Utilisation de l'onglet Offenses	32
Affichage de My Offenses	34
Gestion des violations	34
Affichage des violations	35
Options de la table récapitulative de la source des violations	59
Ajout de remarques	69
Suppression des violations de l'onglet Offenses	71
Protection des violations	74
Exportation des violations	76
Affectation des violations aux utilisateurs	76
Envoi de notifications par courrier électronique	77
Marquage d'éléments pour suivi	79
Affichage des violations par catégories	80
Affichage des violations par IP de source	80
Affichage des violations par IP de destination	88
Affichage des violations par réseau	99

4 ETUDE D'ÉVÉNEMENTS

Présentation de l'onglet Log Activity	110
Utilisation de l'onglet Log Activity	111
Utilisation de la barre d'outils	111
Utilisation de Quick Filter Syntaxe	115
Utilisation des options du menu contextuel	116
Utilisation de la barre d'état	116
Affichage des événements	117
Affichage des événements en streaming	117
Affichage d'événements normalisés	118
Affichage d'événement bruts	124

Affichage des événements groupés	127
Affichage des violations associées	131
Modification du mappage des événements	131
Utilisation des propriétés des événements personnalisés	133
Création des propriétés d'événements personnalisés	133
Copie des propriétés d'événements personnalisés	142
Suppression d'une propriété d'événement personnalisée	143
Réglage des faux positifs	143
Gestion des données PCAP	144
Affichage de la colonne des données PCAP	144
Affichage des informations PCAP	146
Téléchargement du fichier PCAP sur votre système de bureau	147
Exportation des événements	147

5 ÉTUDE DES FLUX

Présentation de l'onglet Network Activity	148
Utilisation de l'onglet Network Activity	149
Utilisation de la barre d'outils	149
Utilisation de Quick Filter Syntaxe	152
Utilisation des options du menu contextuel	153
Utilisation de la barre d'état	154
Affichage des flux	154
Affichage des diffusions en flux	155
Affichage d'événements normalisés	156
>Affichage des flux groupés	163
Affichage des violations associées	166
Utilisation des propriétés de flux personnalisées	167
Création d'une propriété de flux personnalisée	168
Copie d'une propriété de flux personnalisée	173
Copie d'une propriété de flux personnalisée	175
Suppression d' une propriété de flux personnalisée	175
Réglage des faux positifs	176
Exportation des flux	177

6 UTILISATION DE LA FONCTION DES GRAPHIQUES

Présentation de la fonction des graphiques	179
Légendes des graphiques	180
Configuration des graphiques	180
Gestion des graphiques par séries temporelles	182
Création des recherches de séries temporelles	183
Graphiques des séries temporelles de navigation	184

7 RECHERCHE DE DONNÉES

Recherche d'événements ou de flux	187
Recherche des violations	191
Recherche de My Offenses et de All Offenses	192

Recherche des IP de source	197
Recherche des IP de source	199
Recherche des réseaux	200
Enregistrement des critères de recherche	201
Enregistrement des critères de recherche	202
Suppression des critères de recherche	204
Réalisation d'une sous-recherche	205
Gestion des résultats de recherche	207
Affichage des résultats de recherche gérés	207
Sauvegarde des résultats de recherche	209
Gestion des groupes de recherche	210
Affichage des groupes de recherche.	210
Création d'un nouveau groupe	211
Modification d'un groupe	211
Copie d'une recherche sauvegardée vers un autre groupe	211
Suppression d'une recherche enregistrée dans un groupe.	212
Suppression d'un groupe	212

8 CONFIGURATION DES RÈGLES

Présentation des règles	213
Types de règles	215
Conditions de règles.	217
Réponses de règles	217
Affichage des règles	218
Création d' une règle personnalisée.	221
Création d'une règle de détection d'anomalie	231
Gestion des règles	238
Activation/Désactivation des règles.	238
Modification d'une règle	238
Copie d'une règle	239
Suppression d'une règle	239
Groupement des règles	239
Affichage des groupes.	241
Création d'un groupe.	241
Modification d'un groupe	242
Copie d'un élément vers un autre groupe	242
Suppression d'un élément du groupe	243
Suppression d'un groupe	243
Affectation d'un élément à un groupe	243
Modification d'un bloc de construction	262

9 GESTION DES ACTIFS

Présentation de l'onglet l'onglet Asset	245
Affichage des profils d'actifs.	246
Affichage des détails de vulnérabilité	252
Gestion des profils d'actifs	254
Ajout d'un profil d'actif	255

Modification d'un actif	256
Suppression des actifs	256
Importation de profils d'actif	258
Exportation des actifs	258
Utilisation de la fonction de recherche	259
Recherche de profils d'actifs	259
Recherche d'actifs par attribut de vulnérabilité	262

10 GESTION DES RAPPORTS

Présentation de l'onglet l'onglet Reports	267
Utilisation de l'onglet Rapports	268
Affichage des rapports	268
Utilisation de la barre d'outils	270
Affichage des rapports générés	271
Suppression du contenu généré	272
Utilisation de la barre d'état	272
Création des rapports personnalisés	272
Création d'un rapport	273
Configuration des graphiques	277
Sélection d'un type de graphique	301
Personnalisation des rapports par défaut	302
Groupement des rapports	302
Création d'un groupe	303
Modification d'un groupe	303
Affectation d'un rapport à un groupe	304
Copie d'un rapport vers un autre groupe	304
Suppression d'un rapport d'un groupe	304
Création d'un rapport manuellement	305
Duplication d'un rapport	305
Partage d'un rapport	305
Marquage des rapports	306

A TESTS DE RÈGLES

Les tests de règle d'événement	309
Tests de profils d'hôte	310
Tests IP/Port	313
Tests de propriété d'événement (suite)	313
Tests de propriété communs	319
Tests de source de journal	320
Fonction - Tests de séquence	322
Fonction - Tests de compteur	334
Fonction - Tests simples	339
Tests de date/heure	340
Tests de propriété du réseau	341
Fonction - Tests négatifs	341
Tests de règles de flux	342
Tests de profils d'hôte	345

Tests IP/Port	345
Tests de propriété de flux	352
Tests de propriété communs	355
Fonction - Tests de séquence	366
Fonction - Tests de compteurs	370
Fonction - Tests simples	371
Tests de date/heure	371
Tests de propriété du réseau	373
Fonction - Tests négatifs	373
Tests de règles communs	375
Tests de profils d'hôte	377
Tests IP/Port	378
Tests de propriété communs	383
Fonctions - Tests de séquences	394
Fonction - Tests de compteurs	398
Fonction - Tests simples	399
Tests de date/heure	399
Tests de propriété du réseau	401
Fonctions - Tests négatifs	401
Tests de règles de violation	402
Tests IP/Port	402
Tests de fonctions	402
Tests de date/heure	404
Tests de source de journal	404
Tests de propriétés de violation	408
Tests de règles de détection d'anomalies	408
Tests de règles d'anomalies	410
Tests de règles de comportement	412
Tests de règles de seuil	413

B GLOSSAIRE

C AVIS ET MARQUES

Avis	425
Marques	427

INDEX

A PROPOS DE CE GUIDE

Le *Guide d'utilisation IBM Security QRadar Network Anomaly Detection* fournit des informations sur la gestion de QRadar Network Anomaly Detection y compris les onglets **Dashboard**, **Offenses**, **Log Activity**, **Network Activity**, **Assets**, et **Reports**.

Utilisateurs cible

Ce guide est destiné à tous les utilisateurs de QRadar Network Anomaly Detection chargés de l'étude et de la gestion de la sécurité des réseaux. Ce guide suppose que vous disposez d'un accès à QRadar Network Anomaly Detection et d'une connaissance de votre réseau d'entreprise et des technologies réseau.

Conventions

Les conventions suivantes s'appliquent dans ce guide :

- ▶ Indique que la procédure contient une seule instruction.

REMARQUE

Indique que les informations fournies viennent compléter la fonction ou l'instruction associée.



ATTENTION

Indique que les informations sont capitales. Une mise en garde vous avertit de l'éventuelle perte de données ou d'un éventuel endommagement de l'application, du système, du périphérique ou du réseau.



AVERTISSEMENT

Indique que les informations sont capitales. Un avertissement vous informe des éventuels dangers, des éventuelles menaces ou des risques de blessure. Lisez attentivement tout ou partie des messages d'avertissement avant de poursuivre.

Documentation technique

Pour plus d'informations sur la façon d'accéder à la documentation plus technique, aux notes techniques et aux notes sur l'édition, voir [Accessing IBM Security QRadar Documentation Technical Note](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).
(<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644>)

Contactez le service clients

Pour savoir comment contacter le service client, voir [Support and Download Technical Note](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).
(<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>)

1

A PROPOS DE IBM SECURITY QRADAR NETWORK ANOMALY DETECTION

IBM Security QRadar QFlow Collector est une plateforme de gestion de sécurité des réseaux qui offre une prise en charge de la géolocalisation et de la conformité grâce à une combinaison de la connaissance de réseau de flux, de la comparaison des événements de sécurité et de l'évaluation de la vulnérabilité des actifs.

Cette section comprend les rubriques suivantes :

- [Navigateurs Web pris en charge](#)
- [Connexion à Détection des anomalies QRadar](#)
- [Onglet Dashboard](#)
- [Onglet Offenses](#)
- [Onglet Log Activity](#)
- [Onglet Network Activity](#)
- [Onglet Assets](#)
- [Onglet Reports](#)
- [Utilisation de Détection des anomalies QRadar](#)
- [Onglet Admin](#)

REMARQUE

Lorsque vous naviguez dans Détection des anomalies QRadar, n'utilisez pas le bouton **Back** du navigateur. Utilisez les options de navigation disponibles avec Détection des anomalies QRadar afin de naviguer dans l'interface utilisateur.

Navigateurs Web pris en charge

Vous pouvez accéder à la console à partir d'un navigateur Web standard. Lorsque vous accédez au système, une invite s'affiche et demande un nom d'utilisateur et un mot de passe à configurer à l'avance par l'administrateur Détection des anomalies QRadar.

Tableau 1-1 Navigateurs Web pris en charge

Navigateur Web	Versions prises en charge
Mozilla Firefox	<ul style="list-style-type: none"> 10.0 <p>Compte tenu du cycle d'édition court de Mozilla, nous ne pouvons pas soumettre au test les toutes dernières versions du navigateur Mozilla Firefox. Cependant, nous pouvons tout à fait soumettre à l'étude les différents problèmes signalés.</p>
Microsoft® Windows Internet Explorer, avec vue de compatibilité activée	<ul style="list-style-type: none"> 8.0 9.0 <p>Pour obtenir des instructions sur la façon d'activer la vue Compatibility View, voir Activation de Compatibility View pour Internet Explorer.</p>

Activation de Compatibility View pour Internet Explorer

Pour activer Compatibility View pour Internet Explorer 8.0 et 9.0 :

Etape 1 Appuyez sur la touche F12 pour ouvrir la fenêtre Developer Tools.

Etape 2 Configurez les paramètres de compatibilité suivants :

Tableau 1-2 Paramètres de compatibilité d'Internet Explorer

Version du navigateur	Option	Description
Internet Explorer 8.0	Mode navigateur	Dans la zone de liste Browser Mode , sélectionnez Internet Explorer 8.0 .
	Mode document	Dans la zone de liste Document Mode , sélectionnez Internet Explorer 7.0 Standards .
Internet Explorer 9.0	Mode navigateur	Dans la zone de liste Browser Mode , sélectionnez Internet Explorer 9.0 .
	Mode document	Dans la zone de liste Document Mode , sélectionnez Internet Explorer 7.0 Standards .

Connexion à Détection des anomalies QRadar

Pour vous connecter à Détection des anomalies QRadar :

Etape 1 Ouvrez votre navigateur Web.

Etape 2 Entrez l'adresse suivante dans la barre d'adresse :

https://<IP Address>

Où < IP address > est l'adresse IP du système Détection des anomalies QRadar.

Etape 3 Entrez votre nom d'utilisateur et votre mot de passe.

Etape 4 Cliquez sur **Login To QRadar**.

Si vous utilisez Mozilla Firefox, vous devez ajouter une exception à Mozilla Firefox pour vous connecter à Détection des anomalies QRadar. Pour plus d'informations, voir votre documentation Mozilla.

Si vous utilisez Internet Explorer, un message de certificat de sécurité du site Web s'affiche. Vous devez sélectionner l'option **Continue to this website** pour vous connecter à Détection des anomalies QRadar.

REMARQUE

Pour vous déconnecter de Détection des anomalies QRadar, cliquez sur **Log out** dans le coin supérieur droit de l'interface utilisateur.

Une clé de licence par défaut vous permet d'accéder à l'interface utilisateur pendant cinq semaines. Une fenêtre indique la date d'expiration de la clé de licence temporaire. Pour plus d'informations sur l'installation d'une clé de licence, consultez le gui d'administration *IBM Security QRadar Network Anomaly Detection*.

Onglet Dashboard

L'onglet **Dashboard** est l'onglet par défaut qui s'affiche lorsque vous vous connectez à Détection des anomalies QRadar. Il fournit un environnement d'espace de travail qui prend en charge plusieurs tableaux de bord sur lesquels vous pouvez afficher vos affichages de sécurité de réseau, d'activité ou de données collectées par Détection des anomalies QRadar. Les tableaux de bord par défaut sont disponibles. Chaque tableau de bord contient des éléments qui fournissent des informations détaillées et résumées sur les violations se produisant sur votre réseau. Vous pouvez également créer un tableau de bord personnalisé pour vous permettre de vous concentrer sur vos responsabilités d'opération réseau ou de sécurité.

Pour plus d'informations sur l'utilisation de l'onglet **Dashboard**, consultez [Utilisation de l'onglet](#).

Onglet Offenses

L'onglet **Offenses** vous permet d'afficher les violations se produisant sur votre réseau, que vous pouvez localiser à l'aide des différentes options de navigation ou grâce aux recherches avancées. L'onglet **Offenses** vous permet d'étudier une violation afin de déterminer la cause première d'un problème. Vous pouvez également résoudre le problème.

Pour plus d'informations sur l'onglet **Offenses**, consultez [Enquêter sur les violations](#).

Onglet Log Activity

L'onglet **Log Activity** vous permet d'étudier les journaux d'événement envoyés Détection des anomalies QRadar en temps réel, d'effectuer des recherches avancées et d'afficher l'activité du journal à l'aide des graphiques de séries temporelles configurables. L'onglet **Log Activity** vous permet d'effectuer des études approfondies des données d'événements.

Pour plus d'informations, voir [Enquête sur les événements](#).

Onglet Network Activity

L'onglet **Network Activity** vous permet d'étudier les flux envoyés à Détection des anomalies QRadar en temps réel, d'effectuer des recherches avancées et d'afficher l'activité du réseau à l'aide des graphiques de séries temporelles configurables. Un flux est une session de communication entre deux hôtes. L'affichage des informations sur le flux permet de déterminer comment le trafic est communiqué, ce qui est communiqué (si l'option de capture de contenu est activée) et qui est en communication. Les données de flux contiennent également les détails tels que le protocole, les valeurs ASN, les valeurs IFIndex et les priorités.

Pour plus d'informations, voir [Enquête sur les flux](#).

Onglet Assets

Détection des anomalies QRadar reconnaît automatiquement les actifs (serveurs et hôtes) qui fonctionnent sur votre réseau, en fonction des données de flux passifs et des données de vulnérabilité, permettant à Détection des anomalies QRadar d'établir un profil d'actif. Les profils d'actifs fournissent des informations sur chaque actif connu sur votre réseau, notamment les informations d'identité (si disponibles) et les services exécutés sur chaque actif. Ces données de profil sont utilisées à des fins de comparaison, ce qui permet de réduire le nombre de faux positifs. Par exemple, si une attaque tente d'exploiter un service spécifique s'exécutant sur un actif spécifique, Détection des anomalies QRadar peut déterminer si l'actif est vulnérable à cette attaque en comparant l'attaque au profil d'actif. L'onglet **Assets** vous permet d'afficher les actifs étudiés ou de rechercher des actifs spécifiques afin d'afficher leur profil.

Pour plus d'informations, voir [Gestion des actifs](#).

Onglet Reports

L'onglet **Reports** vous permet de créer, distribuer, et gérer les rapports pour toutes les données au sein de Détection des anomalies QRadar. La fonction Reports vous permet de créer des rapports personnalisés pour une utilisation de fonctionnement et d'exécution. Afin de créer un rapport, vous pouvez combiner les informations (telles que celles de sécurité ou de réseau) au sein d'un seul rapport. Vous pouvez également utiliser des modèles de rapport préinstallés inclus avec Détection des anomalies QRadar.

L'onglet **Reports** vous permet également de marquer vos rapports avec des logos personnalisés. Cette option est intéressante pour la distribution des rapports auprès d'audiences différentes.

Pour plus d'informations sur les rapports, voir [Gestion de rapports](#).

Utilisation de Détection des anomalies QRadar

Cette section comprend les rubriques suivantes :

- [Résultats triés de Détection des anomalies QRadar](#)
- [Actualisation de l'interface utilisateur](#)
- [Mise en pause de l'interface utilisateur de](#)
- [Etude des adresses IP](#)
- [Affichage de l'heure du système](#)
- [Mise à jour des détails de l'utilisateur](#)
- [Accès à l'aide en ligne](#)
- [Redimensionnement des colonnes](#)
- [Configuration de la taille de page](#)

Résultats triés de Détection des anomalies QRadar

Sur les onglets **Log Activity**, **Offenses**, **Network Activity** et **Reports**, vous pouvez trier les tableaux en cliquant sur une en-tête de colonne. Un seul clic sur la colonne trie les résultats en ordre décroissant et un second clic sur l'en-tête trie les résultats par ordre croissant. Une flèche au-dessus de la colonne indique la direction du tri.

Par exemple, si vous souhaitez trier des événements par Event Name, cliquez sur l'en-tête de **Event Name**. Une flèche s'affiche sur l'en-tête de la colonne pour indiquer que les résultats sont triés par ordre décroissant.

Cliquez sur l'en-tête de la colonne de **Event Name** à nouveau si vous souhaitez trier les informations par ordre croissant.

Actualisation de l'interface utilisateur

Plusieurs onglets de Détection des anomalies QRadar, notamment l'onglet **Dashboard**, **Log Activity**, **Offenses** et **Network Activity** vous permettent d'actualiser manuellement l'onglet. Cette option refresh se trouve à droite de l'onglet. L'onglet **Dashboard** et **Offenses** s'actualisent automatiquement chaque 60 secondes. Les onglets **Log Activity** et **Network Activity** s'actualisent automatiquement chaque 60 secondes si vous affichez l'onglet en mode dernière intervalle (actualisation automatique). Le minuteur indique le temps de la dernière actualisation de l'onglet. Afin d'actualiser l'onglet, cliquez sur l'icône **Refresh**.

Mise en pause de l'interface utilisateur de Détection des anomalies QRadar

Lorsque vous affichez les onglets **Log Activity** ou **Network Activity** en mode temps réel (diffusion en flux) ou en mode dernière minute (actualisation automatique), vous pouvez utiliser le minuteur d'actualisation, qui se trouve à droite, pour mettre en pause l'affichage en cours. Vous pouvez également mettre en pause l'affichage en cours à l'aide de l'onglet **Dashboard**.

- ▶ Afin de mettre l'affichage en pause, cliquez sur l'icône **Pause**.

En cliquant sur n'importe où à l'intérieur de l'élément dashboard, l'onglet se met en pause automatiquement. Le minuteur clignote en rouge pour indiquer que l'affichage en cours est en pause.

- ▶ Cliquez sur l'icône **Play** pour redémarrer le minuteur.

Etude des adresses IP

Si des informations géographiques sont disponibles pour une adresse IP, le pays est indiqué visuellement par une balise.

- ▶ Mettez le pointeur de votre souris sur une adresse IP pour afficher son emplacement.

Vous pouvez effectuer un clic droit sur n'importe quelle adresse IP ou nom d'actif pour accéder aux menus supplémentaires, qui vous permettent de préciser s'il s'agit d'une adresse IP ou d'un actif. Pour plus d'informations sur les actifs, consultez [Gestion des actifs](#). Pour plus d'informations sur la personnalisation du menu contextuel, voir la note technique de la *personnalisation du menu contextuel*.

Le menu More Options contient :

Tableau 1-3 Menu More Options

Menu	Description
Navigate	<p>Le menu Navigate fournit les options suivantes :</p> <ul style="list-style-type: none"> • View By Network - Affiche la fenêtre List of Networks, qui affiche tous les réseaux associés avec l'adresse IP sélectionnée. • View Source Summary - Affiche la fenêtre List of offenses, qui affiche toutes les violations associées avec l'adresse IP source sélectionnée. • View Destination Summary - Affiche la fenêtre list of offenses, qui affiche toutes les violations associées à l'adresse IP de destination associée.

Tableau 1-3 Menu More Options (suite)

Menu	Description
Information	<p>Le menu Information fournit les options suivantes :</p> <ul style="list-style-type: none"> • DNS Lookup - Recherche les entrées DNS en fonction de l'adresse IP. • WHOIS Lookup - Recherche le propriétaire enregistré d'une adresse IP distante. Le serveur WHOIS par défaut est whois.arin.net. • Port Scan - Effectue une analyse Network Mapper (NMAP) de l'adresse IP sélectionnée. Cette option est uniquement disponible si NMAP est installé sur votre système. Pour plus d'informations sur l'installation de NMAP, consultez la documentation de votre fournisseur. • Asset Profile - Affiche les informations de profil d'actif. Cette option de menu est uniquement disponible lorsque Détection des anomalies QRadar a acquis les données de profil activement via une analyse ou passivement via des sources de flux. Pour plus d'informations, consultez le Manuel d'administration <i>IBM Security QRadar Network Anomaly Detection</i>. • Search Events - Sélectionnez l'option Search Events afin de rechercher les événements associés avec cette adresse IP. Pour plus d'informations, consultez Recherche des événements ou des flux. • Search Flows - Sélectionnez l'option Search Flows afin de rechercher les flux associés avec cette adresse IP. Pour plus d'informations, consultez Recherche des événements ou des flux. • Search Connections - Sélectionnez l'option Search Connections afin de rechercher les connexions associées avec cette adresse IP. Cette option est uniquement affichée si vous avez acheté et obtenu une licence pour utiliser IBM Security QRadar Risk Manager et que vous avez établi la connexion entre la console et le dispositif IBM Security QRadar Risk Manager. Pour plus d'informations, voir le manuel d'utilisation <i>IBM Security QRadar Risk Manager</i>. • Switch Port Lookup - Sélectionnez l'option Switch Port Lookup pour déterminer le port de commutation sur un périphérique Cisco IOS pour cette adresse IP. Cette option s'applique uniquement aux commutateurs reconnus à l'aide de l'option Discover Devices sur l'onglet Risk Manager. Pour plus d'informations, voir <i>IBM Security QRadar Risk Manager Users Guide</i>. • View Topology - Sélectionnez l'option View Topology afin d'afficher l'onglet Topology, qui représente la topologie de la couche 3 de votre réseau. Cette option est uniquement affichée si vous avez acheté et obtenu une licence pour utiliser IBM Security QRadar Risk Manager et que vous avez établi la connexion entre la console et le dispositif IBM Security QRadar Risk Manager. Pour plus d'informations, voir le manuel d'utilisation <i>IBM Security QRadar Risk Manager</i>.

Etude des noms d'utilisateurs

Cliquez avec le bouton droit sur le nom d'utilisateur pour accéder aux options du menu supplémentaire, qui vous permet de préciser s'il s'agit d'un nom d'utilisateur ou d'une adresse IP. Les options du menu comprennent :

Tableau 1-4 Options supplémentaires relatives au nom d'utilisateur

Menu	Description
View Assets	Affiche la fenêtre Assets Lists, qui affiche les actifs en cours associés au nom d'utilisateur sélectionné. Pour plus d'informations sur l'affichage des actifs, consultez Gestion des actifs .
View User History	Affiche la fenêtre Assets Lists, qui affiche tous les actifs associés au nom d'utilisateur sélectionné au cours des dernières 24 heures. Pour plus d'informations sur l'affichage des actifs, consultez Gestion des actifs .
View Events	Affiche la fenêtre List of Events, qui affiche les événements associés au nom d'utilisateur sélectionné. Pour plus d'informations sur la fenêtre List of Events, consultez Afficher les événements .

REMARQUE

Pour plus d'informations sur la personnalisation du menu contextuel consultez la note technique de la personnalisation du menu contextuel.

Affichage de l'heure du système

A droite de Détection des anomalies QRadar l'interface utilisateur s'affiche l'heure du système, qui correspond à l'heure de la console. L'heure de la console synchronise tous les systèmes Détection des anomalies QRadar dans le déploiement de Détection des anomalies QRadar et est utilisé pour déterminer l'heure de la réception des événements à partir d'autres dispositifs pour la corrélation de synchronisation de l'heure correcte.

Dans un déploiement distribué, la console peut se trouver dans un fuseau horaire différent de celui de votre ordinateur de bureau. Lors de l'application des filtres basés sur le temps et des recherches sur les onglets **Log Activity** et **Network Activity**, vous devez utiliser l'heure du système de la console lorsque vous spécifiez l'intervalle de l'heure.

Mise à jour des détails de l'utilisateur

Vous pouvez accéder aux détails d'utilisateur sur l'interface utilisateur Détection des anomalies QRadar. Pour accéder aux informations de l'utilisateur, cliquez sur **Preferences**. La fenêtre User Preferences fournit les informations suivantes :

Tableau 1-5 Détails de la fenêtre User Preferences

Paramètre	Description
Username	Affiche votre nom d'utilisateur.

Tableau 1-5 Détails de la fenêtre User Preferences (suite)

Paramètre	Description
Password	Facultatif. Entrez un nouveau mot de passe. Le mot de passe doit répondre aux critères suivants : <ul style="list-style-type: none"> • Doit contenir six caractères au minimum • Doit contenir 255 caractères au maximum • Doit contenir au moins un caractère spécial • Doit contenir au moins un caractère en majuscule
Password (Confirm)	Entrez le mot de passe à nouveau pour confirmation.
Email Address	Facultatif. Entrez votre adresse e-mail. L'adresse e-mail doit répondre aux conditions suivantes : <ul style="list-style-type: none"> • Elle doit être une adresse e-mail valide • Doit contenir 10 caractères au minimum • Doit contenir 255 caractères au maximum
Enable Popup Notifications	Sélectionnez cette case à cocher si vous souhaitez activer les notifications du système popup pour qu'il soit affiché sur votre interface utilisateur.

Accès à l'aide en ligne

Vous pouvez accéder à l'aide en ligne de Détection des anomalies QRadar grâce à l'interface utilisateur de Détection des anomalies QRadar. Pour accéder à l'aide en ligne, cliquez sur **Help > Help Contents**.

Redimensionnement des colonnes

Plusieurs onglets de Détection des anomalies QRadar, notamment l'onglet **Offenses**, **Log Activity**, **Network Activity**, **Assets** et **Reports** vous permettent de redimensionner les colonnes de l'affichage. Placez le pointeur de votre souris sur la ligne qui sépare les colonnes et glissez l'arête de la colonne vers un nouvel emplacement. Vous pouvez également redimensionner les colonnes en double cliquant sur la ligne qui sépare les colonnes pour redimensionner automatiquement la colonne vers la largeur de la zone la plus large.

REMARQUE

Le redimensionnement de la colonne ne fonctionne pas sur Internet Explorer 7.0 lorsque l'onglet **Log Activity** ou **Network Activity** sont des enregistrements affichés en mode diffusion en flux..

Configuration de la taille de page

Dans les tableaux d'onglets **Offenses**, **Assets**, **Log Activity**, **Network Activity** et **Reports**, Détection des anomalies QRadar s'affiche un maximum de 40 résultats par défaut. Si vous possédez des privilèges d'administration, vous pouvez configurer le nombre maximal des résultats en utilisant l'onglet **Admin**. Pour plus d'informations, voir *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Onglet Admin

Si vous possédez des privilèges d'administration, vous pouvez accéder à l'onglet **Admin**. L'onglet **Admin** fournit aux administrateurs l'accès aux fonctionnalités administratives, notamment :

- **Configuration du système** - vous permet de configurer les options systèmes et les options de gestion d'utilisateur.
- **Data sources** - vous permettent de configurer les sources du journal, les sources de flux, et les options de vulnérabilité.
- **Remote Networks and Services Configuration** - Vous permettent de configurer les réseaux distants et les groupes de services.
- **Plug-ins** - Donne accès aux composants plug-in, tel que le IBM Security QRadar Risk Manager plug-in. Cette option est affichée uniquement si des plug-ins sont installés sur votre console.
- **Deployment** - Vous permet de vous connecter et de gérer les composants individuels de votre déploiement Détection des anomalies QRadar.

Toutes les mises à jour de configuration que vous avez effectuées dans l'onglet **Admin** sont sauvegardées dans la zone de transfert. Lorsque tous les changements sont complets, vous pouvez déployer les mises à jour de configuration pour l'hôte géré dans votre déploiement.

Pour plus d'informations sur l'onglet **Admin**, consultez le guide d'administration IBM Security QRadar Network Anomaly Detection.

2

UTILISATION DE L'ONGLET DASHBOARD

L'onglet **Dashboard** correspond à la vue par défaut lorsque vous vous connectez à IBM Security QRadar QFlow Collector. Il fournit un environnement d'espace de travail qui prend en charge plusieurs tableaux de bord sur lesquels vous pouvez afficher vos vues de sécurité de réseau, d'activité ou de données collectées par Détection des anomalies QRadar.

Cette section comprend les rubriques suivantes :

- [A propos des tableaux de bord](#)
- [Gestion des tableaux de bord](#)
- [Éléments de tableau de bord](#)

A propos des tableaux de bord

Grâce aux tableaux de bord, vous pouvez organiser les éléments de votre tableau de bord en vues fonctionnelles, ce qui vous permet de vous concentrer sur les domaines spécifiques de votre réseau.

L'onglet **Dashboard** propose des tableaux de bord par défaut axés sur la sécurité, l'intelligence du réseau, l'activité de l'application et la surveillance du système. Chaque tableau de bord affiche un ensemble par défaut d'éléments de tableau de bord. Les éléments du tableau de bord agissent comme points de lancement pour accéder à des données plus détaillées.

Le tableau suivant définit les tableaux de bord par défaut.

Tableau 2-1 Tableaux de bord par défaut

Tableau de bord par défaut	Eléments
Application Overview	Inbound Traffic by Country (time series)
	Outbound Traffic by Country (time series)
	Top Applications (time series)
	Top Applications Inbound from Internet (time series)
	Top Applications Outbound from Internet (time series)
	Top Applications Outbound from Internet (time series)
	DSCP - Precedence (time series)
Intelligence du réseau	Top Talkers (real time)
	ICMP Type/Code (time series)
	Top Networks by Traffic Volume (time series)
	Firewall Deny by DST Port (time series)
	Firewall Deny by DST IP (time series)
	Firewall Deny by SRC IP (time series)
	Top Applications (time series)
	Link Utilization (real-time)
	DSCP - Precedence (time series)
	Top Talkers (real time)
System Monitoring	Top Log Sources (Event Count)
	Link Utilization (real-time)
	System Notifications
	Event Processor Distribution (time series)
	Event Rate (Events per Second Coalesced - Average 1 Min)
	Flow Rate (Flows per Second - Peak 1 Min)

Tableau 2-1 Tableaux de bord par défaut (suite)

Tableau de bord par défaut	Éléments
Threat and Security Monitoring	Default-IDS/IPS-All: Top Alarm Signatures (time series)
	Top Systems Attacked (IPD/IDP/IPS) (time series)
	Top Systems Sourcing Attacks (IPD/IDP/IPS) (time series)
	My Offenses
	Most Severe Offenses
	Most Recent Offenses
	Événements sortants par pays (temps réel)
	Internet Threat Information Center
	Flow Bias
	Top Category Types
	Top Sources
	Top Local Destinations

Le contenu affiché sur l'onglet **Dashboard** est spécifique à l'utilisateur. Vous pouvez personnaliser vos tableaux de bord. Les modifications apportées au sein d'une session Détection des anomalies QRadar affectent uniquement votre système.

Pour personnaliser l'onglet **Dashboard**, vous pouvez procéder comme suit :

- Créer des tableaux de bord personnalisés qui sont adaptés à vos responsabilités.

Détection des anomalies QRadar prend en charge jusqu'à 255 tableaux de bord par utilisateur. Toutefois, nous vous recommandons de ne pas créer plus de 10 tableaux de bord.

- Ajouter et supprimer des éléments de tableau de bord à partir des tableaux de bord personnalisés ou par défaut.
- Déplacer et positionner des éléments selon vos besoins.

Lors du positionnement des éléments, chaque élément se redimensionne automatiquement en fonction du tableau de bord.

- Ajoutez des éléments personnalisés en fonction des données de votre tableau de bord.

Par exemple, vous pouvez afficher un élément de tableau de bord qui fournit un graphique de série temporelle ou un graphique à barres représentant les N premières activités du réseau.

Pour créer des éléments personnalisés, vous pouvez créer des recherches enregistrées sur les onglets **Network Activity** ou **Log Activity** et choisir comment représenter les résultats dans le tableau de bord. Chaque tableau de bord affiche les données actualisées en temps réel. Les graphiques de série temporelle sur le tableau de bord sont actualisés toutes les 5 minutes.

Gestion des tableaux de bord

Cette section comprend les rubriques suivantes :

- [Affichage d'un tableau de bord](#)
- [Création d'un tableau de bord personnalisé](#)
- [Ajout d'éléments](#)
- [Configuration des graphiques](#)
- [Suppression d'éléments](#)
- [Détachement d'un élément](#)
- [Modification d'un tableau de bord](#)
- [Suppression d'un tableau de bord](#)

Affichage d'un tableau de bord

Détection des anomalies QRadar fournit des tableaux de bord par défaut auxquels vous pouvez accéder à partir de la zone de liste **Show Dashboard**. Lorsque vous créez des tableaux de bord personnalisés, ils sont également répertoriés dans la zone de liste **Show Dashboard**.

REMARQUE

Si vous avez précédemment consulté un tableau de bord et que vous retournez à l'onglet **Dashboard**, le dernier tableau de bord consulté est affiché.

Pour afficher un tableau de bord :

- Etape 1** Cliquez sur l'onglet **Dashboard**.
- Etape 2** Dans la zone de liste **Show Dashboard**, sélectionnez le tableau de bord que vous souhaitez afficher.

Création d'un tableau de bord personnalisé Pour créer un tableau de bord personnalisé :

- Etape 1** Cliquez sur l'onglet **Dashboard**.
- Etape 2** Cliquez sur l'icône **New Dashboard**.
- Etape 3** Dans la zone **Name**, entrez le nom du tableau de bord. La longueur maximale est 65 caractères.
- Etape 4** Dans le champ **Description**, entrez une description pour le tableau de bord. La longueur maximale est 255 caractères. Cette description s'affiche dans l'info-bulle pour le nom du tableau de bord dans la zone de liste **Show Dashboard**.
- Etape 5** Cliquez sur **OK**.

Le nouveau tableau de bord s'affiche sur l'onglet **Dashboard** et apparaît dans la zone de liste **Show Dashboard**. Par défaut, le tableau de bord est vide. Pour plus d'informations sur l'ajout d'éléments, voir [Ajout d'éléments](#).

Ajout d'éléments Pour ajouter un élément à un tableau de bord :

- Etape 1** Cliquez sur l'onglet **Dashboard**.
- Etape 2** Dans la zone de liste **Show Dashboard**, sélectionnez le tableau de bord auquel vous souhaitez ajouter un élément.
- Etape 3** Dans la zone de liste **Add Item**, sélectionnez un élément. Pour plus d'informations sur les éléments de tableau de bord disponibles, voir [Eléments de tableau de bord](#).

Etude des données provenant d'un élément de tableau de bord Les éléments de tableau de bord basés sur une recherche fournissent un lien vers les onglets **Log Activity** ou **Network Activity**, ce qui vous permet d'étudier davantage l'activité du journal ou du réseau. Les éléments de tableau de bord basés sur une recherche sont disponibles dans les menus **Add Items > Network Activity > Flow Searches** et **Add Items > Log Activity > Event Searches**. Pour plus d'informations sur les éléments de tableau de bord, voir [Eléments de tableau de bord](#).

REMARQUE

Cette procédure s'applique également aux éléments du tableau de bord Risk Manager. Les éléments de tableau de bord du gestionnaire de risques s'affiche uniquement que lorsque IBM Security QRadar Risk Manager a été acheté sous licence et que vous avez établi la connexion entre la console et le dispositif IBM Security QRadar Network Anomaly Detection. Pour plus d'informations, voir *IBM Security QRadar Risk Manager Users Guide*.

Pour étudier les flux à partir d'un élément du tableau de bord **Log Activity** :

- ▶ Cliquez sur le lien **View in Log Activity**. L'onglet **Log Activity** s'affiche avec les résultats et deux graphiques qui correspondent aux paramètres de l'élément de votre tableau de bord.

Pour étudier les flux à partir d'un élément de tableau de bord **Network Activity** :

- ▶ Cliquez sur le lien **View in Network Activity**. L'onglet **Network Activity** s'affiche avec les résultats et deux graphiques qui correspondent aux paramètres de l'élément de votre tableau de bord.

Les types de graphiques affichés sur l'onglet **Log Activity** ou **Network Activity** dépendent du graphique qui est configuré dans l'élément de tableau de bord :

- **Bar, Pie, and Table** - L'onglet **Log Activity** ou **Network Activity** affiche un graphique à barres, un graphique circulaire et un tableau avec les détails de flux.
- **Time Series** - L'onglet **Log Activity** ou **Network Activity** affiche des graphiques en fonction des critères suivants :
 - Si votre plage horaire est inférieure ou égale à 1 heure, un graphique de série temporelle, un graphique à barres et une table avec les détails d'événement ou de flux sont affichés.
 - Si votre plage horaire est supérieure à 1 heure, un graphique de série temporelle s'affiche et vous êtes invité à cliquer sur **Update Details**. Cette action démarre la recherche qui remplit les détails d'événement ou de flux et génère le graphique à barres. Une fois la recherche terminée, le graphique à barres et le tableau avec les détails d'événement ou de flux sont affichés.

Configuration des graphiques

Vous pouvez configurer les éléments des tableaux de bord **Log Activity**, **Network Activity** et **Connections** (le cas échéant) pour indiquer le type de graphique et le nombre d'objets de données que vous souhaitez afficher. Les configurations personnalisées de vos graphiques sont conservées afin que les graphiques s'affichent selon la configuration à chaque fois que vous accédez à l'onglet **Dashboard**.

Pour configurer des graphiques dans un élément de tableau de bord :

- Etape 1** Cliquez sur l'onglet **Dashboard**.
- Etape 2** Dans la zone de liste **Show Dashboard**, sélectionnez le tableau de bord qui contient l'élément que vous souhaitez personnaliser.
- Etape 3** Dans l'en-tête de l'élément de tableau de bord, cliquez sur l'icône **Settings**.
Les options de configuration s'affichent.
- Etape 4** Configurez les paramètres suivants :

Tableau 2-2 Options du menu Chart

Paramètres	Description
Value to Graph	<p>Dans la zone de liste, sélectionnez le type d'objet que vous voulez représenter sur le graphique. Les options comprennent tous les paramètres d'événements normalisés et personnalisés ou de flux inclus dans vos paramètres de recherche.</p> <p>Remarque : <i>Détection des anomalies QRadar accumule des données de sorte que lorsque vous exécutez une recherche enregistrée de série temporelle, il existe une mémoire cache des données d'événements ou de flux disponibles pour afficher les données relatives à la période de temps précédente. Les paramètres accumulés sont indiqués par un astérisque (*) dans la zone de liste Value to Graph. Si vous sélectionnez une valeur pour graphique qui n'est pas accumulée (sans astérisque), les données de série temporelle ne sont pas disponibles.</i></p>
Chart Type	<p>Dans la zone de liste, sélectionnez le type de graphique que vous souhaitez afficher. Ces options incluent :</p> <ul style="list-style-type: none"> • Bar Chart - Affiche les données dans un graphique à barres. Cette option est uniquement disponible pour les événements ou flux regroupés. • Pie Chart - Affiche les données dans un graphique circulaire. Cette option est uniquement disponible pour les événements ou flux regroupés. • Table - Affiche les données dans un tableau. Cette option est uniquement disponible pour les événements ou flux regroupés. • Time Series - Affiche un graphique à courbes interactif qui représente les enregistrements mis en correspondance selon un intervalle de temps spécifié. <p>Pour plus d'informations sur la configuration des critères de recherche de séries temporelles pour l'activité du journal, voir Enquêter sur les événements.</p> <p>Pour plus d'informations sur la configuration des critères de recherche de séries temporelles pour l'activité du journal, voir Enquêter sur les flux.</p>
Display Top	<p>Dans la zone de liste, sélectionnez le nombre d'objets que vous voulez afficher dans le graphique. Ces options incluent 5 et 10. La valeur par défaut est 10.</p>

Tableau 2-2 Options du menu Chart (suite)

Paramètres	Description
Capture Time Series Data	<p>Cochez cette case pour activer la capture de série temporelle. Lorsque vous cochez cette case, la fonction de graphique commence à accumuler des données pour les graphiques de série temporelle. Cette option est désactivée par défaut.</p> <p>Remarque : Cette option est uniquement disponible sur les graphiques de série temporelle. Vous devez disposer des autorisations appropriées pour gérer et afficher des graphiques de série temporelle. Pour plus d'informations sur les permissions du rôle, consultez le guide d'administration IBM Security QRadar Network Anomaly Detection.</p>
Time Range	<p>Dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez afficher.</p> <p>Remarque : Cette option est uniquement disponible sur les graphiques de série temporelle.</p>

Suppression d'éléments La suppression d'un élément ne supprime pas l'élément de Détection des anomalies QRadar. La suppression d'un élément supprime l'élément de votre tableau de bord. Vous pouvez de nouveau ajouter l'élément à tout moment.

Pour supprimer un élément de votre tableau de bord :

- Etape 1** Cliquez sur l'onglet **Dashboard**.
- Etape 2** Dans la zone de liste **Show Dashboard**, sélectionnez le tableau de bord à partir duquel vous souhaitez supprimer un élément.
- Etape 3** Sur l'en-tête de l'élément de tableau de bord, cliquez sur l'icône [x] rouge pour supprimer l'élément du tableau de bord.
- Etape 4** Cliquez sur **Yes**.

Détachement d'un élément Le détachement d'un élément vous permet de contrôler temporairement un ou plusieurs éléments particuliers sur votre bureau. Vous pouvez détacher l'élément, puis retirer l'élément de votre tableau de bord. La fenêtre détachée reste ouverte et s'actualise selon des intervalles planifiés. Si vous fermez l'application Détection des anomalies QRadar, la fenêtre détachée reste ouverte pour la surveillance et continue de s'actualiser jusqu'à ce que vous fermiez manuellement la fenêtre ou que vous éteigniez votre ordinateur.

REMARQUE

Détection des anomalies QRadar n'enregistre pas le statut d'un élément de tableau de bord détaché lorsque vous terminez votre session Détection des anomalies QRadar.

Pour détacher un élément de votre tableau de bord :

- Etape 1** Cliquez sur l'onglet **Dashboard**.
- Etape 2** Dans la zone de liste **Show Dashboard**, sélectionnez le tableau de bord à partir duquel vous souhaitez détacher un élément.
- Etape 3** Sur l'en-tête de l'élément de tableau de bord, cliquez sur l'icône verte pour détacher l'élément de tableau de bord et l'ouvrir dans une fenêtre séparée.

REMARQUE

Le détachement d'un élément ne supprime pas l'élément de Détection des anomalies QRadar ; le détachement d'un élément duplique les données dans une nouvelle fenêtre.

Modification d'un tableau de bord Vous pouvez modifier le nom et la description des tableaux de bord. Pour modifier un tableau de bord :

- Etape 1** Cliquez sur l'onglet **Dashboard**.
- Etape 2** Dans la zone de liste **Show Dashboard**, sélectionnez le tableau de bord que vous souhaitez modifier.
- Etape 3** Dans la barre d'outils, cliquez sur l'icône **Rename Dashboard**.

Etape 4 Dans la zone **Name**, entrez un nouveau nom pour le tableau de bord. La longueur maximale est 65 caractères.

Etape 5 Dans le champ **Description**, entrez une nouvelle description pour le tableau de bord. La longueur maximale est 255 caractères.

Etape 6 Cliquez sur **OK**.

Suppression d'un tableau de bord Pour supprimer un tableau de bord :

Etape 1 Cliquez sur l'onglet **Dashboard**.

Etape 2 Dans la zone de liste **Show Dashboard**, sélectionnez le tableau de bord que vous souhaitez supprimer.

Etape 3 Dans la barre d'outils, cliquez sur **Delete Dashboard**.

Etape 4 Cliquez sur **Yes**.

L'onglet **Dashboard** s'actualise et le premier tableau de bord dans la zone de liste **Show Dashboard** s'affiche. Le tableau de bord que vous avez supprimé n'est plus affiché dans la zone de liste **Show Dashboard**.

Eléments de tableau de bord

Cette section comprend les rubriques suivantes :

- [Eléments de recherche de flux](#)
- [Eléments de violation](#)
- [Eléments d'activité journal](#)
- [Eléments de rapports](#)
- [Elément de récapitulatif du système](#)
- [Elément de notification du système](#)
- [Centre d'information de menace Internet](#)
- [Ajouter des éléments de tableau de bord basés sur une recherche à la liste Ajouter éléments](#)

Eléments de recherche de flux

Vous pouvez afficher un élément de tableau de bord personnalisé en fonction des critères de recherche enregistrés à partir de l'onglet **Network Activity**. Des éléments de recherche de flux figurent dans le menu **Add Item > Network Activity > Flow Searches**. Le nom de l'élément de recherche de flux correspond au nom des critères de recherche enregistrés sur lequel l'élément est basé.

Détection des anomalies QRadar comprend des critères de recherche enregistrés par défaut qui sont préconfigurés pour afficher les éléments de recherche de flux dans le menu de votre onglet **Dashboard**. Vous pouvez ajouter des éléments de tableau de bord de recherche de flux supplémentaires dans le menu de votre onglet **Dashboard**. Pour plus d'informations, [Ajouter des éléments de tableau de bord basés sur une recherche à la liste Ajouter éléments](#).

Sur un élément de tableau de bord de recherche de flux, les résultats de recherche affichent des données actualisées en temps réel sur un graphique. Les graphiques de série temporelle, les tableaux, les graphiques circulaires et les graphiques à barres sont les types de graphiques pris en charge. Le type de graphique par défaut est bar. Ces graphiques sont configurables. Pour plus d'informations sur les graphiques de configuration, voir [Configuration des graphiques](#).

Les tableaux de série temporelle sont interactifs. En utilisant les graphiques de série temporelle, vous pouvez agrandir et parcourir un calendrier pour étudier l'activité du réseau.

Eléments de violation Vous pouvez ajouter plusieurs éléments de violation dans votre tableau de bord. L'onglet **Offenses** affiche les données pour les violations, les sources et les destinations locales détectées sur votre réseau. Ces violations incluent :

- [Violations](#)
- [Sources et Destinations](#)
- [Catégories](#)

REMARQUE

Les violations cachées ou fermées ne sont pas incluses dans les valeurs qui sont affichées dans l'onglet **Dashboard**. Pour plus d'informations sur les événements cachés ou fermés, voir [Enquêter sur les violations](#).

Violations

L'élément de menu **Add Item > Offenses > Offenses** sur le menu de l'onglet **Dashboard** affiche les éléments de tableau de bord suivants :

- **Les violations les plus graves** - Les cinq violations les plus récentes sont identifiées par une barre d'amplitude pour vous informer de l'importance de la violation. Pointez votre souris sur le nom de la violation pour afficher des informations détaillées sur l'adresse IP.
- **Les violations les plus graves** - Les cinq violations les plus graves sont identifiées par une barre d'amplitude pour vous informer de l'importance de la violation. Pointez votre souris sur le nom de la violation pour afficher des informations détaillées sur l'adresse IP.
- **Mes violations** - L'élément **My Offenses** affiche cinq des plus récentes violations qui vous sont assignées. Les violations sont identifiées par une barre d'amplitude pour vous informer de son importance. Pointez votre souris sur l'adresse IP pour afficher des informations détaillées sur l'adresse IP.

Sources et Destinations

L'élément de menu **Ajouter élément > Infractions > Sources et Destinations** sur le menu de l'onglet **Dashboard** affiche les éléments de tableau de bord suivants :

- **Sources Top** - L'élément **Top Sources** affiche les sources de violations top. Chaque source est identifiée par une barre d'amplitude pour vous informer de

son importance. Pointez votre souris sur l'adresse IP pour afficher des informations détaillées sur l'adresse IP.

- **Destinations locales top** - L'élément **Top Local Destinations** affiche les destinations locales top. Chaque destination est identifiée par une barre d'amplitude pour vous informer de son importance. Pointez votre souris sur l'adresse IP pour afficher des informations détaillées sur l'adresse IP.

Catégories

L'élément **Top Categories Types** affiche les cinq principales catégories associées avec le plus grand nombre de violations.

Eléments d'activité journal

Les éléments de tableau de bord d'activité journal vous permet de surveiller et enquêter sur les événements en temps réel. Ces éléments d'activité journal incluent :

- [Recherches d'événements](#)
- [Evénements par gravité](#)
- [Sources de journal top](#)

REMARQUE

Les violations cachées ou fermées ne sont pas incluses dans les valeurs qui sont affichées dans l'onglet **Dashboard**.

Recherches d'événements

Vous pouvez afficher un élément de tableau de bord personnalisé en fonction des critères de recherche enregistrés à partir de l'onglet **Log Activity**. Des recherches d'événements figurent dans le menu **Add Item > Network Activity > Event Searches**. Le nom de l'élément de recherche d'événements correspond au nom des critères de recherche enregistrés sur lequel l'article est basé.

Détection des anomalies QRadar comprend des critères de recherche enregistrés par défaut qui sont préconfigurés pour afficher les éléments de recherche d'événements sur votre menu de l'onglet **Dashboard**. Vous pouvez ajouter d'autres éléments de tableau de bord de recherche d'événements à votre menu de l'onglet **Dashboard**. Pour plus d'informations. [Ajouter des éléments de tableau de bord basés sur une recherche à la liste Ajouter éléments](#).

Sur un élément de tableau de bord **Log Activity**, des résultats de recherche affichent des données de dernière minute en temps réel sur un graphique. Les types de graphiques prises en charge sont les séries temporelles, le tableau, le graphique circulaire, et une barre. Le type de graphique par défaut est bar. Ces graphiques sont configurables. Pour plus d'informations sur les graphiques de configuration, voir [Configuration des graphiques](#).

Les tableaux de série temporelle sont interactifs. En utilisant les graphiques de série temporelle, vous pouvez agrandir et parcourir un calendrier pour étudier l'activité du journal.

Événements par gravité

L'élément de tableau de bord **Events By Severity** affiche le nombre d'événements actifs regroupés par ordre de gravité. Cette option vous permet de voir le nombre d'événements qui sont reçus par le niveau de gravité qui a été attribué. La gravité indique le niveau de menace créé par une source de violation par rapport à la préparation de la destination pour l'attaque. La plage de gravité est de 0 (faible) à 10 (élevé). Les types de graphiques prises en charge sont le tableau, le graphique circulaire, et une barre.

Sources de journal top

L'élément de tableau de bord **Top Log Sources** affiche les cinq principales sources de journal qui ont envoyé des événements à Détection des anomalies QRadar dans les 5 dernières minutes. Le nombre d'événements envoyés à partir de la source de journal spécifiée est indiqué dans le graphique. Cette option vous permet de visualiser des changements potentiels dans le comportement, par exemple, si une source du journal pare-feu qui n'est généralement pas dans la liste des 10 meilleurs contribue actuellement à un grand pourcentage du comptage de message global, vous devriez étudier cet événement. Les types de graphiques prises en charge sont le tableau, le graphique circulaire, et une barre.

Eléments de rapports L'élément de tableau de bord **Most Recent Reports** affiche les meilleurs rapports récemment générés. L'affichage fournit le titre du rapport, l'heure et la date que rapport a été généré, et le format du rapport.

Élément de récapitulatif du système

L'élément de tableau de bord **System Summary** fournit un récapitulatif de haut niveau de l'activité au cours des 24 dernières heures. Dans la rubrique récapitulative, vous pouvez afficher les informations suivantes :

- **Flux actuel par seconde** - Indique le débit de flux par seconde.
- **Flux (24 dernières heures)** - Indique le nombre total de flux actifs observés au cours des 24 dernières heures
- **Événements actuels par seconde** - Spécifie le débit d'événements par seconde.
- **Nouveau événements (24 dernières heures)** - Indique le nombre total d'événements reçus au cours des 24 dernières heures.
- **Infractions mises à jour (24 dernières heures)** - Indique le nombre total de violations qui ont été créés ou modifiées avec de nouvelles preuves au cours des dernières 24 heures.
- **Ratio de réduction de données** - Spécifie le ratio de réduction de données en fonction des événements détectés au total au cours des 24 dernières heures et le nombre de violations modifiées au cours des dernières 24 heures.

Élément de notification du système

Les éléments de tableau de bord **Systems Notification** affichent des notifications d'événements de votre système. Pour que les notifications s'affichent dans l'élément de tableau de bord **System Notification**, l'administrateur doit créer une règle basée sur chaque type de message de notification et sélectionner la case **Notify** dans l'assistant de règles personnalisées. Pour plus d'informations sur la configuration des notifications d'événements et la création de règles d'événement, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Cette section comprend les rubriques suivantes :

- [Affichage des notifications du système](#)
- [Gestion des notifications du système](#)
- [Affichage de notifications contextuelles](#)

Affichage des notifications du système

Sur l'élément de tableau de bord **System Notifications** vous pouvez afficher les informations suivantes :

- **Balise** - Spécifie des symboles pour indiquer le niveau de gravité de la notification. Pointez votre souris sur le symbole pour afficher plus de détails sur le niveau de gravité.
 - **Icône** d'information (?)
 - **Icône** d'erreur (X)
 - **Icône** d'avertissement (!)
- **Créé** - Indique la quantité de temps qui s'est écoulé depuis la création de la notification.

- **Description** - Indique les informations sur la notification.
- **Icône de fermeture (x)**- Vous permet de fermer une notification du système. Vous pouvez pointer votre souris sur la notification pour afficher plus de détails :
 - **adresse IP de l'hôte** - Indique l'adresse IP de l'hôte qui a créé la notification.
 - **Gravité** - Indique le niveau de gravité de l'incident qui a créé cette notification.
 - **Catégorie à faible niveau** - Indique la catégorie associée à l'incident qui a généré cette notification. Par exemple : interruption service. Pour plus d'informations sur les catégories, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
 - **Payload** - Indique le contenu de la charge utile associée à l'incident qui a généré cette notification.
 - **Created** - Indique la quantité de temps qui s'est écoulé depuis la création de la notification.

Gestion des notifications du système

En utilisant l'élément de tableau de bord **System Notification** sur votre tableau de bord, vous pouvez indiquer le nombre de notifications que vous voulez afficher dans votre tableau de bord et fermer toutes les notifications du système.

Pour gérer l'affichage de notification du système :

Etape 1 Assurez-vous que l'élément de tableau de bord **System Notification** est ajouté à votre tableau de bord.

Pour plus d'informations, voir [Ajout d'éléments](#).

Etape 2 - Dans l'en-tête de l'élément de tableau de bord de la notification du système, cliquez sur l'icône **Settings**.

Etape 3 Dans la zone de liste **Display** sélectionnez le nombre de notifications que vous souhaitez afficher.

Les options sont **5**, **10** (par défaut), **20**, **50**, et **TOUT**.

Pour afficher toutes les notifications système connectées dans les dernières 24 heures, cliquez sur **All**. Une fenêtre détaillant les notifications du système s'affiche. Pour plus d'informations sur les événements, voir [Enquêter sur les événements](#).

Etape 4 Pour fermer une notification de système, cliquez sur l'icône **Delete**.

Affichage de notifications contextuelles

Lorsque que vous ajoutez l'élément de tableau de bord **System Notifications**, des notifications du système peuvent également s'afficher comme des notifications contextuelles dans l'interface utilisateur Détection des anomalies QRadar. Ces notifications contextuelles sont affichées sur le coin droit inférieur de l'interface utilisateur, quel que soit l'onglet sélectionné.

REMARQUE

Les notifications contextuelles ne sont disponibles que pour les utilisateurs ayant des autorisations administratives. Les notifications contextuelles sont activées par défaut. Pour désactiver les notifications contextuelles, sélectionnez **User Preferences** et désélectionnez la case **Enable Pop-up Notifications**. Pour plus d'informations, voir *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Dans la fenêtre contextuelle des notifications de système, le nombre de notifications dans la file d'attente est mis en évidence. Par exemple, si (1 à 12) est affiché dans l'en-tête, la notification en cours est de 1 sur 12 notifications à afficher.

La fenêtre contextuelle des notifications de système offre les options suivantes :

- **Icône Suivant (>)** - Affiche le message de notification suivant. Par exemple, si le message de notification actuel est 3 sur 6, cliquez sur l'icône pour afficher 4 sur 6.
- **Icône Fermer (X)** - Ferme la fenêtre contextuelle de cette notification.
- **(détails)** - Affiche des informations supplémentaires concernant cette notification de système.

Centre d'information de menace Internet

L'élément de tableau de bord du Centre d'information de menace Internet est un flux RSS intégré qui vous fournit des mises à jour des recommandations sur les questions de sécurité, des évaluations de menaces quotidiennes, des nouvelles de la sécurité et des référentiels de menace.

Le diagramme niveau actuel de menace indique le niveau actuel de menace et fournit un lien vers la page Niveau actuel de menace Internet du site d'IBM Internet Security Systems.

Les recommandations actuelles sont répertoriées dans l'élément de tableau de bord. Pour voir un récapitulatif de la recommandation :

- ▶ Cliquez sur l'icône en forme de flèche à côté de la recommandation. La recommandation se développe pour afficher un récapitulatif Cliquez sur l'icône en forme de flèche à nouveau pour masquer le récapitulatif.

Pour étudier la recommandation complète :

- ▶ Cliquez sur le lien associé. Le site d'IBM Internet Security Systems s'ouvre dans une autre fenêtre du navigateur, affichant les détails de recommandation complets.

Ajouter des éléments de tableau de bord basés sur une recherche à la liste Ajouter éléments

Pour ajouter un événement et un élément de tableau de bord de recherche de flux au menu **Add Item** sur l'onglet **Dashboard**, vous devez accéder à l'onglet **Log Activity** ou **Network Activity** pour créer des critères de recherche qui indiquent que les résultats de la recherche peuvent être affichés sur l'onglet **Dashboard**. Les critères de recherche doivent également préciser que les résultats sont regroupés sur un paramètre.

REMARQUE

Cette procédure s'applique également aux éléments de tableau de bord du gestionnaire de risques. Les éléments de tableau de bord du gestionnaire de risques s'affiche uniquement que lorsque IBM Security QRadar Risk Manager a été acheté sous licence et que vous avez établi la connexion entre la console et le dispositif IBM Security QRadar Risk Manager. Pour plus d'informations, voir *IBM Security QRadar Risk Manager Users Guide*.

Pour plus d'informations sur les événements et les éléments de tableau de bord de flux, voir [Éléments de tableau de bord](#).

Pour ajouter un événement ou un élément de tableau de bord de recherche de flux à la liste **Add Items** :

Étape 1 Sélectionnez l'une des options suivantes :

- Pour ajouter un élément de tableau de bord de recherche de flux, cliquez sur l'onglet **Network Activity**.
- Pour ajouter un élément de tableau de bord de recherche, cliquez sur l'onglet **Log Activity**.

Étape 2 Dans la zone de liste **Search**, sélectionnez l'une des options suivantes :

- Pour créer une nouvelle recherche, sélectionner **New Search**.
- Pour modifier une recherche enregistrée, sélectionner **Edit Search**.

Étape 3 Configurer ou modifier vos paramètres de recherche, tel que requis. Pour plus d'informations sur les éléments de recherche, voir [Enquêter sur les flux](#).

Étape 4 Assurez-vous de configurer les paramètres suivants :

- Dans le panneau Rechercher Édition, sélectionnez l'option **Include in my Dashboard**.
- Dans le panneau Définitions de colonne, sélectionnez une colonne et cliquez sur l'icône **Add Column** pour déplacer la colonne vers la liste **Group By**.

Étape 5 Cliquez sur **Filter**.

Les résultats de la recherche sont affichés.

Étape 6 Cliquez sur **Save Criteria**

Étape 7 Configurer vos paramètres, tel que requis. Pour plus d'informations, voir [Recherche de données](#).

Étape 8 Cliquez sur **OK**.

Étape 9 Assurez-vous que vos critères de recherche enregistrés ont ajouté avec succès l'événement ou l'élément de tableau de bord de recherche de flux à la liste **Add Items**

- a Cliquez sur l'onglet **Dashboard**.
- b Sélectionnez une des options suivantes :

- Pour vérifier un élément de recherche d'événements, sélectionnez **Add Item > Log Activity > Event Searches**.
- Pour vérifier un élément de recherche de flux, sélectionnez **Add Item > Network Activity > Flow Searches**.

L'élément de tableau de bord doit être affiché sur la liste en utilisant le même nom que vos critères de recherche enregistrés.

3

ETUDE DES INFRACTIONS

L'onglet **Offenses** vous permet d'étudier les infractions, les adresses IP source et cible, les comportements de réseau et les anomalies de votre réseau.

Cette section comprend les rubriques suivantes :

- [Présentation de l'onglet Offense](#)
- [Utilisation de l'onglet infractions](#)
- [Affichage de mes infractions](#)
- [Gestion des infractions](#)
- [Affichage des infractions par catégorie](#)
- [Affichage des infractions par source IP](#)
- [Affichage des infractions par cible IP](#)
- [Affichage des infractions par réseau](#)

Présentation de l'onglet Offense

IBM Security QRadar Network Anomaly Detection peut comparer les événements et les flux aux adresses IP cible localisées dans plusieurs réseaux de la même infraction et, si possible, le même incident de réseau. Ceci vous permet d'étudier efficacement chaque infraction dans votre réseau. Vous pouvez explorer les différentes pages de l'onglet **Offenses** pour étudier les détails d'événements et de flux afin de déterminer les événements uniques à l'origine de l'infraction.

En utilisant l'onglet **Offenses**, vous pouvez rechercher des infractions en fonction de critères différents. Pour plus d'informations sur la recherche des infractions, voir [Recherche de données](#).

REMARQUE

L'onglet **Offenses** n'utilise pas les autorisations d'utilisateur au niveau du périphérique afin de déterminer les infractions que chaque utilisateur devrait être capable d'afficher; ceci est déterminé par les autorisations réseau. Par conséquent, tous les utilisateurs peuvent afficher toutes les infractions quelle que soit la source de journal ou la source de flux associée à l'infraction. Pour plus d'informations sur les autorisations au niveau du périphérique, voir le *QRadar Network Anomaly Detection Guide d'administration*.

En utilisant l'onglet **Offenses**, vous pouvez accéder et analyser les éléments suivants :

- **Offenses** - Une infraction comprend plusieurs événements ou flux provenant d'une seule source, comme un hôte ou une source de journal. L'onglet **Offenses** affiche les infractions, notamment le trafic et les vulnérabilités qui collaborent et valident l'ampleur d'une infraction. L'ampleur d'une infraction est déterminée par plusieurs tests effectués sur l'infraction chaque fois qu'elle est ré-évaluée. La réévaluation se produit lorsque des événements sont ajoutés à l'infraction et à intervalles planifiés.
- **Source IP Addresses** - Une adresse IP source indique le périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Une adresse IP source peut utiliser plusieurs méthodes d'attaque, comme les attaques de reconnaissance ou de déni de service (DoS), pour tenter un accès non autorisé.
- **Destination IP Addresses** - Une adresse IP cible indique le périphérique réseau auquel tente d'accéder l'adresse IP source.

En utilisant l'onglet **Offenses**, vous pouvez ajouter des notes, marquer une infraction pour un suivi, attribuer des infractions aux utilisateurs et masquer des infractions, des infractions e-mail, des infractions fermées et résolues ou des infractions protégées de la suppression. L'onglet **Offenses** vous permet d'enquêter sur les événements et les flux associés à des infractions spécifiques pour une analyse médico-légale.

Utilisation de l'onglet Infractions

En utilisant l'onglet **Offenses**, vous pouvez accéder aux options suivantes dans le menu de navigation :

Tableau 3-1 Options de menu de navigation

Menu	Description
My Offenses	Affiche toutes les infractions qui vous sont affectées.
All Offenses	Affiche toutes les infractions globales sur le réseau.
By Category	Affiche toutes les infractions regroupées par catégorie de haut et de bas niveau. Pour plus d'informations sur les catégories de haut et de bas niveau, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
By Source IP	Affiche toutes les adresses IP source qui sont impliquées dans une infraction. Pour plus d'informations, voir Affichage des infractions par source IP .
By Destination IP	Affiche toutes les adresses IP cible qui sont impliquées dans une infraction. Pour plus d'informations, voir Affichage des infractions par cible IP .
By Network	Affiche tous les réseaux qui sont impliqués dans une infraction. Pour plus d'informations, voir Affichage des infractions par réseau .

Tableau 3-1 Options de menu de navigation (suite)

Menu	Description
Rules	Permet d'accéder à l'onglet Rules, à partir duquel vous pouvez créer des règles personnalisées. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .

Chaque page dans l'onglet **Offenses** fournit une barre d'outils, vous permettant d'effectuer des actions sur les infractions affichées sur la page.

Affichage de Mes infractions

Par défaut, la page All Offenses s'affiche lorsque vous cliquez sur l'onglet **Offenses**. Vous pouvez afficher les infractions qui vous sont affectées sur la page My Offenses.

Pour afficher les infractions qui vous sont affectées :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de navigation, cliquez sur < **My Offenses**.

La page My Offenses fournit une liste de toutes les infractions que l'administrateur vous a affectées. Pour plus d'informations sur la gestion de vos infractions, voir [Gestion des infractions](#).

Gestion des infractions

La page All Offenses page sur l'onglet **Offenses** affiche une liste des infractions que QRadar Network Anomaly Detection a identifiées sur votre réseau. Les infractions sont énumérées en premier en fonction de la plus grande ampleur.

REMARQUE

Sur l'onglet **Admin**, vous pouvez configurer les paramètres du système pour supprimer les infractions de la base de données après une période de temps configurée. Vous devez disposer d'une autorisation administrative pour accéder à l'onglet **Admin** et configurer les paramètres du système. Lors de la configuration des seuils, QRadar Network Anomaly Detection ajoutez 5 jours pour tout seuil défini. Pour plus d'informations, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration - Configuring System Settings*.

Cette section comprend les rubriques suivantes :

- [Affichage des infractions](#)
- [Options du récapitulatif de la source d'infraction](#)
- [Ajout de notes](#)
- [Suppression des infractions de l'onglet Offenses](#)
- [Protection des infractions](#)
- [Exportation des infractions](#)
- [Affectation des infractions aux utilisateurs](#)
- [Envoi de notification par e-mail](#)
- [Marquage d'un article pour suivi](#)

Affichage des infractions Pour afficher les infractions :

Etape 1 Cliquez sur l'onglet **Offenses**.

REMARQUE

Pour accéder à la page All Offenses à partir d'autres pages de l'onglet **Offenses**, cliquez sur **All Offenses** dans le menu de navigation.

La barre d'outils All Offenses fournit les fonctions suivantes :

Tableau 3-2 Barre d'outils de toutes les infractions

Fonction	Description
Search	<p>Cliquez sur Search pour effectuer des recherches avancées sur les infractions, y compris :</p> <ul style="list-style-type: none">• New Search - Sélectionnez cette option pour créer une nouvelle recherche d'infraction.• Edit Search - Sélectionnez cette option pour sélectionner et modifier une recherche d'infraction. <p>Pour plus d'informations sur la fonctionnalité de recherche, voir Recherche de données.</p>
Save Criteria	<p>Cliquez sur Save Criteria pour enregistrer les critères de recherche en cours. Voir Enregistrer les critères de recherche.</p>

Tableau 3-2 Barre d'outils de toutes les infractions (suite)

Fonction	Description
Actions	<p>A partir de la zone de liste Actions vous pouvez sélectionner l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Hide - Sélectionnez cette option pour masquer l'infraction sélectionnée. Pour plus d'informations sur le masquage des infractions, voir Masquage des infractions. • Show - Sélectionnez cette option pour afficher toutes les infractions masquées. Pour plus d'informations sur l'affichage des infractions masquées, voir Affichage des infractions masquées. • Close - Sélectionnez cette option pour fermer les infractions sélectionnées. Pour plus d'informations sur la fermeture des infractions, voir Fermeture d'une infraction. • Close Listed - Sélectionnez cette option pour fermer toutes les infractions listées dans l'onglet Offenses. Pour plus d'informations sur la fermeture des infractions listées, voir Fermeture des infractions listées. • Protect - Sélectionnez cette option pour protéger les infractions sélectionnées. Pour plus d'informations sur la protection des infractions, voir Protection des infractions. • Protect Listed - Sélectionnez cette option pour protéger toutes les infractions listées dans l'onglet Offenses. Pour plus d'informations sur la protection des infractions listées, voir Protection des infractions listées. • Unprotect - Sélectionnez cette option pour déprotéger les infractions protégées. Pour plus d'informations sur la déprotection des infractions, voir Déprotection des infractions. • Unprotect Listed - Sélectionnez cette option pour déprotéger les infractions protégées sélectionnées listées dans l'onglet Offenses. Pour plus d'informations sur la déprotection des infractions listées, voir Déprotection des infractions listées. • Export to XML - Sélectionnez cette option pour exporter des infractions au format XML. Voir Exportation des infractions. • Export to CSV - Sélectionnez cette option pour exporter les infractions au format CSV. Voir Exportation des infractions. • Assign - Sélectionnez cette option pour affecter une infraction sélectionnée à un utilisateur. Voir Affectation des infractions aux utilisateurs.
Print	Cliquez sur Print pour imprimer les infractions affichées sur la page.

La page All Offenses fournit les informations suivantes :

Tableau 3-3 Paramètres de page de toutes les infractions

Paramètre	Description
View Offenses	En utilisant cette zone de liste, vous pouvez filtrer les infractions que vous souhaitez afficher sur cette page. Vous pouvez consulter toutes les infractions ou filtrer les infractions basées sur un intervalle. A partir de la zone de liste, vous pouvez sélectionner l'intervalle que vous souhaitez filtrer.
Current Search Parameters	La partie supérieure du tableau affiche les détails des paramètres de recherche appliqués aux résultats de la recherche. Pour supprimer ces paramètres de recherche, cliquez sur Clear Filter . Pour plus d'informations sur la recherche d'infraction, voir Recherche de données .
Flag	Indique les mesures prises sur l'infraction. Les actions sont représentées par les icônes suivantes : <ul style="list-style-type: none"> • Flag - Indique que l'infraction est marquée pour suivi. Ceci vous permet de contrôler un article particulier pour une investigation complémentaire. Pour plus d'informations sur le marquage d'une infraction pour suivi, voir Marquage d'un article pour suivi. • User - Indique que l'infraction a été affectée à un utilisateur. Lorsqu'une infraction est affectée à un utilisateur, elle est affichée sur la page My Offenses de cet utilisateur. Pour plus d'informations sur l'affectation des infractions aux utilisateurs, voir Affectation des infractions aux utilisateurs. • Notes - Indique qu'un utilisateur a ajouté des notes à l'infraction. Les notes peuvent inclure toute information que vous souhaitez capturer pour l'infraction. Par exemple, vous pourriez ajouter une note qui indique une information qui n'est pas automatiquement incluse dans une infraction, telle un numéro de ticket de service clients ou des informations de gestion d'infraction. Pour plus d'informations sur l'ajout des notes, voir Ajout de notes. • Protected - Indique que cette infraction est protégée. La fonction Protect empêche les infractions spécifiées d'être supprimées de la base de données après que la période de conservation est écoulée. Pour plus d'information sur les infractions protégées, voir Protection des infractions.

Tableau 3-3 Paramètres de page de toutes les infractions (suite)

Paramètre	Description
	<ul style="list-style-type: none"> • Inactive Offense - Indique qu'il s'agit d'une infraction inactive. Une infraction devient inactive au bout de cinq jours après que l'infraction ait reçu le dernier événement. En outre, toutes les infractions deviennent inactives après la mise à niveau de votre logiciel QRadar Network Anomaly Detection. <p>Une infraction inactive ne peut pas redevenir active. Si de nouveaux événements sont détectés pour l'infraction, une nouvelle infraction est créée et l'infraction inactive est conservée jusqu'à ce que la durée de conservation de l'infraction soit écoulée. Vous pouvez effectuer les actions suivantes sur les infractions inactives: protéger, indiquer pour suivi, ajouter des notes, et affecter aux utilisateurs.</p> <p>Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.</p>
Id	Indique le numéro d'identification unique QRadar Network Anomaly Detection affecté à cette infraction.
Description	Indique les détails pour cette infraction.
Offense Type	Indique le type d'infraction. Le type d'infraction est déterminé par la règle qui a créé l'infraction. Par exemple, si le type d'infraction est l'événement source du journal, la règle qui a généré cette infraction est corrélée aux événements en fonction du périphérique qui a détecté l'événement.
Offense Source	Indique des informations sur la source de l'infraction. L'information qui s'affiche dans la zone Offense Source dépend du type d'infraction. Par exemple, si le type d'infraction est Source Port, la zone Offense Source affiche le port source de l'événement qui a créé cette infraction.
Magnitude	Indique l'importance relative de l'infraction. La barre d'ampleur offre une représentation visuelle de toutes les variables corrélées des événements et des flux pour cette infraction. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée.
	Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire .
Source IPs	Indique les adresses IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Si plus d'une adresse IP source est associée à cette infraction, cette zone indique Multiple et le nombre d'adresses IP source.
Destination IPs	Indique les adresses IP et le nom de l'actif (si disponible) des destinations locales ou distantes. Si plus d'une adresse IP cible est associée à cette infraction, cette zone indique Multiple et le nombre d'adresses IP cible.
Users	Indique les noms d'utilisateur associés à cette infraction. Si plus d'un nom d'utilisateur est associé à l'infraction, cette zone indique Multiple et le nombre de noms d'utilisateur.

Tableau 3-3 Paramètres de page de toutes les infractions (suite)

Paramètre	Description
Log Sources	Indique les sources de journal associées à cette infraction. Si plus d'une source de journal est associée à l'infraction, cette zone indique Multiple et le nombre de sources de journal.
Events	Indique le nombre d'événements pour cette infraction.
Flows	Indique le nombre de flux pour cette infraction. <i>Remarque : Si la colonne Flows affiche N/A, l'infraction peut avoir une date de début qui précède la date où vous avez effectué une mise à niveau vers IBM Security QRadar Network Anomaly Detection 7.1.0 (MR1).</i>
Start Date	Indique la date et l'heure du premier événement ou flux associé à cette infraction.
Last Event/Flow	Indique le temps écoulé depuis le dernier événement ou flux.

Etape 2 Cliquez deux fois sur l'infraction que vous souhaitez afficher.

REMARQUE

Si vous souhaitez afficher une infraction sur une nouvelle page, maintenez la touche de contrôle pendant que vous cliquez deux fois sur une infraction.

La page Offense Summary fournit les fonctions suivantes :

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction

Fonction	Description
Display	Dans la zone de liste Display , sélectionnez l'option pour les informations que vous souhaitez afficher.
Summary	Si vous avez cliqué pour afficher une autre option dans la zone de liste Display , vous pouvez cliquer sur Summary pour revenir à la vue sommaire détaillé.
Remarques	<p>Cliquez sur Notes pour afficher toutes les notes pour cette infraction, y compris :</p> <ul style="list-style-type: none"> • Notes - Indique les notes d'utilisateur pour cette infraction. • Username - Indique l'utilisateur qui a créé cette note. • Creation Date - Indique la date et l'heure où cette note a été créée. <p>Pour plus d'informations à propos des notes, voir Ajout de notes.</p>

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Sources	<p>Cliquez sur Sources pour afficher toutes les adresses IP source pour cette infraction, y compris :</p> <ul style="list-style-type: none"> • Flag - Indique l'action menée sur l'adresse IP source. Par exemple, si un indicateur s'affiche, l'adresse IP source est marquée pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires. • Source IP Indique l'adresse IP du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin, vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>. • Magnitude - Indique l'importance relative de l'adresse IP source. la barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS de l'actif associé à l'adresse IP source. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire. • Location - Indique l'emplacement réseau de l'adresse IP source. • Vulnerability - Indique si l'adresse IP source dispose de vulnérabilités. • User - Indique le nom d'utilisateur de l'adresse IP source. Si aucun utilisateur n'est identifié, cette zone indique Unknown. • MAC -Indique l'adresse MAC de l'adresse IP source. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown. • Weight - Indique la pondération de l'adresse IP source. La pondération d'une adresse IP est affectée sur l'onglet Assets. Pour plus d'informations, voir Gestion des actifs. • Offenses -Indique le nombre d'infractions associées à cette adresse IP source. • Destination(s) - Indique le nombre d'adresses IP cible associées à cette adresse IP source. • Last Event/Flow - Indique le temps écoulé depuis le dernier événement ou flux. • Events/Flows - Indique le nombre d'événements ou de flux associés à cette adresse IP source.

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Destinations	<p data-bbox="691 338 1453 401">Cliquez sur Destinations pour afficher toutes les adresses IP locales cible pour cette infraction, y compris :</p> <p data-bbox="691 411 1453 569"><i>Remarque : Si les adresses IP cible associées à cette infraction sont distantes, une page séparée s'ouvre pour fournir des informations pour les adresses IP cible distantes. Pour plus d'informations sur les adresses IP cible, voir Affichage des infractions par cible IP.</i></p> <ul data-bbox="691 579 1453 1776" style="list-style-type: none"> <li data-bbox="691 579 1453 705">• Flag - Indique l'action menée sur l'adresse IP cible. Par exemple, si un indicateur s'affiche, l'adresse IP cible est marquée pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires. <li data-bbox="691 716 1453 915">• Destination IP - Indique l'adresse IP de la destination locale. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin, vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>. <li data-bbox="691 926 1453 1104">• Magnitude - Indique l'importance relative de l'adresse IP cible. la barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS de l'actif associé à l'adresse IP cible. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir le Glossaire. <li data-bbox="691 1115 1453 1178">• Location - Indique l'emplacement réseau de l'adresse IP cible. <li data-bbox="691 1188 1453 1251">• Vulnerability - Indique si l'adresse IP cible dispose de vulnérabilités. <li data-bbox="691 1262 1453 1325">• User - Indique le nom d'utilisateur de l'adresse IP cible. Si aucun utilisateur n'est identifié, cette zone indique Unknown. <li data-bbox="691 1335 1453 1398">• MAC - Indique l'adresse MAC de l'adresse IP cible. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown. <li data-bbox="691 1409 1453 1493">• Weight - Indique la pondération de cette adresse IP cible. la pondération d'une adresse IP est affectée sur l'onglet Assets. Pour plus d'informations, voir Gestion des actifs <li data-bbox="691 1503 1453 1566">• Offenses - Indique le nombre d'infractions associées à cette adresse IP cible. <li data-bbox="691 1577 1453 1640">• Source(s) - Indique le nombre d'adresses IP source associées à cette adresse IP cible. <li data-bbox="691 1650 1453 1713">• Last Event/Flow - Indique le temps écoulé depuis le dernier événement ou flux. <li data-bbox="691 1724 1453 1776">• Events/Flows - Indique le nombre d'événements ou de flux associés à cette adresse IP cible.

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Log Sources	<p data-bbox="703 352 1458 411">Cliquez sur Log Sources pour afficher toutes les sources du journal pour cette infraction, y compris :</p> <ul data-bbox="703 426 1458 779" style="list-style-type: none"> <li data-bbox="703 426 1458 453">• Name - Indique le nom de la source du journal. <li data-bbox="703 468 1458 495">• Description - Indique la description de la source du journal. <li data-bbox="703 510 1458 569">• Group - Indique à quel groupe de source de journal la source du journal appartient. <li data-bbox="703 583 1458 642">• Events/Flows - Indique le nombre d'événements associés à cette source de journal. <li data-bbox="703 657 1458 716">• Offenses - Indique le nombre d'infractions associées à cette source de journal pour cette infraction. <li data-bbox="703 730 1458 779">• Total Events/Flows - Indique le nombre total d'événements associés à cette source de journal.
Users	<p data-bbox="703 793 1458 852">Cliquez sur Users pour afficher tous les utilisateurs associés à cette infraction, y compris :</p> <ul data-bbox="703 867 1458 1106" style="list-style-type: none"> <li data-bbox="703 867 1458 894">• Name - Indique le nom de l'utilisateur. <li data-bbox="703 909 1458 968">• Events/Flows - Indique le nombre d'événements ou de flux associés à l'utilisateur pour cette infraction. <li data-bbox="703 982 1458 1041">• Offenses - Indique le nombre des infractions associées à l'utilisateur. <li data-bbox="703 1056 1458 1106">• Total Events/Flows - Indique le nombre total d'événements ou de flux associés à l'utilisateur.

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Categories	<p>Cliquez sur Categories pour afficher des informations de catégorie pour cette infraction, y compris :</p> <p>Remarque : Vous pouvez également étudier davantage les événements relatifs à une catégorie spécifique en cliquant avec le bouton droit sur une catégorie et en sélectionnant Events. Alternativement, vous pouvez mettre en évidence la catégorie et cliquez sur l'icône Events dans la barre d'outils Liste de l'événement des catégories.</p> <ul style="list-style-type: none"> • Name - Indique le nom de la catégorie associée à cette infraction. • Magnitude - Indique l'importance relative de la catégorie. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de la catégorie. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs pour la catégorie et l'ampleur calculée. • Local Destination Count - Indique le nombre d'adresses IP cible locales associées à cette catégorie. • Events/Flows - Indique le nombre d'événements ou de flux associés à cette catégorie. • First Event/Flow - Indique la date et l'heure du premier événement ou flux. • Last Event/Flow - Indique la date et l'heure du dernier événement ou flux. <p>Pour plus d'informations sur les catégories, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>.</p>
Annotations	<p>Cliquez sur Annotations to view pour afficher toutes les annotations pour cette infraction, y compris :</p> <ul style="list-style-type: none"> • Annotation - Indique les détails de cette annotation. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux infractions comme composant de la réponse de la règle. Pour plus d'informations sur les règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>. • Time - Indique la date et l'heure où cette annotation a été créée. • Weight - Indique la pondération de cette annotation.

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Networks	<p>Cliquez sur Networks pour afficher tous les réseaux de destination pour cette infraction, y compris :</p> <ul style="list-style-type: none"> • Flag - Indique l'action menée sur le réseau. Par exemple, si un indicateur s'affiche, le réseau est marqué pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires. • Network - Indique le nom du réseau de destination. • Magnitude - Indique l'importance relative du réseau de destination. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS des actifs associés au réseau de destination. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire. • Source IPs - Indique le nombre d'adresses IP source associées à ce réseau. • Destination IPs - Indique le nombre d'adresses IP cible associées à ce réseau. • Offenses Targeted - Indique le nombre d'infractions ciblées sur ce réseau. • Offenses Launched - Indique le nombre d'infractions lancées par ce réseau. • Events/Flows - Indique le nombre d'événements ou de flux associés à ce réseau.
Rules	<p>Cliquez sur Rules pour afficher toutes les règles qui ont généré cette infraction, y compris :</p> <ul style="list-style-type: none"> • Flag - Indique que la règle a été supprimée étant donné qu'elle a généré pour cette infraction. • Rule Name - Indique le nom de la règle qui a généré cette infraction. • Events/Flows - indique le nombre combiné des événements ou des flux générés pour cette infraction. • First Event/Flow - Indique le temps écoulé depuis que le premier événement ou flux a généré cette règle. • Last Event/Flow - Indique le temps écoulé depuis que le dernier événement ou flux a généré cette règle. <p>Remarque : La règle qui a créé l'infraction est listée en premier.</p> <p>Pour disposer des autorisations appropriées pour modifier une règle, double-cliquez sur la règle pour lancer la page Edit Rules. Pour plus d'informations sur les rôles d'utilisateur, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>.</p> <p>Si la règle a été supprimée, une icône rouge (x) s'affiche à côté de la règle. Si vous double-cliquez sur une règle supprimée, un message s'affiche pour indiquer la règle n'existe plus.</p>

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Events	Cliquez sur Events pour afficher tous les événements pour cette infraction. Lorsque vous cliquez sur Events , les résultats de la recherche d'événement s'affichent. Pour plus d'informations sur la recherche d'événements, voir Etude des événements .
Anomaly	Cliquez sur Anomaly pour afficher les résultats de recherche enregistrée à l'origine de la règle de détection d'anomalie qui a généré cette infraction. <i>Remarque</i> : Ce bouton s'affiche uniquement si l'infraction a été générée par une règle de détection d'anomalie.
Flows	Cliquez sur Flows pour continuer à enquêter sur les flux associés à cette infraction. Lorsque vous cliquez sur Flows , les résultats de la recherche de flux sont affichés. Voir Études flux .

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Connections	<p>Cliquez sur Connections pour continuer à enquêter sur les connexions.</p> <p>Remarque : Cette option n'est disponible que si vous avez acheté et mis sous licence IBM Security QRadar Risk Manager. Pour plus d'informations, voir le guide d'utilisation IBM Security QRadar Risk Manager.</p> <p>Lorsque vous cliquez sur l'icône Connections, la page de recherche de critères de connexion s'affiche dans une nouvelle page, pré-remplie avec les critères de recherche d'événements suivants :</p> <ul style="list-style-type: none"> • Time Range - Récent (Dernière heure) • Column Definition - Indique les colonnes suivantes pour qu'elles soient affichées dans les résultats de recherche : <ul style="list-style-type: none"> - Last Packet Time - Source Type - Source - Destination Type - Destination - Protocol - Destination Port - Flow Application - Flow Source - Flow Count - Flow Source Bytes - Flow Destination Bytes - Log Source - Event Count - Connection Type <p>Vous pouvez personnaliser les paramètres de recherche, si nécessaire. Cliquez sur Search pour afficher les informations de connexion.</p>

Tableau 3-4 Barre d'outils du récapitulatif de l'infraction (suite)

Fonction	Description
Actions	<p>A partir de la zone de liste Actions vous pouvez sélectionner l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Follow up - Sélectionnez cette option pour marquer cette infraction pour un suivi ultérieur. Voir Marquage d'un article pour suivi. • Hide - Sélectionnez cette option pour masquer cette infraction. Pour plus d'informations sur le masquage des infractions, voir Masquage des infractions. • Protect Offense - Sélectionnez cette option pour protéger cette infraction. Pour plus d'informations sur la protection des infractions, voir Protection des infractions. • Close - Sélectionnez cette option pour fermer cette infraction. Pour plus d'informations sur la fermeture des infractions, voir Fermeture d'une infraction. • Email - Sélectionnez cette option pour envoyer le récapitulatif de l'infraction à un ou plusieurs destinataires. Voir Envoi de notification par e-mail. • Add Note - Sélectionnez cette option pour ajouter des notes à l'infraction. Voir Ajout de notes. • Assign - Sélectionnez cette option pour affecter cette infraction à un utilisateur. Voir Affectation des infractions aux utilisateurs.
View Attack Path	<p>Cliquez sur View Attack Path pour continuer à enquêter sur le chemin d'attaque de l'infraction. Lorsque vous cliquez sur l'icône View Attack Path, la page Topologie en cours s'affiche sur une nouvelle page.</p> <p><i>Remarque : Cette option n'est disponible que si vous avez acheté et mis sous licence IBM Security QRadar Risk Manager. Pour plus d'informations, voir le guide d'utilisation IBM Security QRadar Risk Manager.</i></p>
Print	Cliquez sur Print pour imprimer cette infraction.

La page de synthèse de l'infraction fournit les tableaux des informations suivants sur l'infraction sélectionnée :

- [Tableau Offense](#)
- [Tableau récapitulatif de la source d'infraction](#)
- [Tableau des 5 dernières notes](#)
- [Tableau des 5 principales IP source](#)
- [Tableau des 5 principales IP cible](#)
- [Tableau des 5 principales sources de journal](#)
- [Tableau des 5 principaux utilisateurs](#)
- [Tableau des 5 principales catégories](#)

- [Tableau des 10 derniers événements](#)
- [Tableau des 10 derniers événements \(Événements d'anomalie\)](#)
- [Tableau des 10 derniers flux](#)
- [Tableau des 5 principales annotations](#)

REMARQUE

La partie supérieure de la page affiche le trajet de navigation vers l'affichage en cours. Pour renvoyer à une page déjà affichée, cliquez sur le nom de la page sur le trajet de navigation. Cette option est indisponible lors de l'affichage du récapitulatif d'infraction sur une nouvelle page.

REMARQUE

Pour afficher un panneau sur la page de synthèse de façon plus détaillée, cliquez sur l'option barre d'outils associée. Par exemple, si vous souhaitez afficher les détails des adresses IP source, cliquez sur **Sources**.

Offense Table

Le tableau Offense fournit des détails de présentation pour l'infraction. Pour plus d'informations sur la barre d'outils, voir [Tableau 3-4](#).

Tableau 3-5 Paramètres du tableau de l'infraction

Paramètre	Description
Magnitude	Indique l'importance relative de l'infraction. La barre d'ampleur offre une représentation visuelle de toutes les variables corrélées des événements et des flux pour cette infraction. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher les valeurs et l'ampleur calculée. <i>Remarque</i> : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire .

Tableau 3-5 Paramètres du tableau de l'infraction (suite)

Paramètre	Description
Status	<p>Affiche des icônes pour indiquer l'état d'une infraction. Les icônes d'état incluent :</p> <ul style="list-style-type: none"> • Inactive Offense - Indique qu'il s'agit d'une infraction inactive. Une infraction devient inactive au bout de cinq jours après que l'infraction ait reçu le dernier événement. En outre, toutes les infractions deviennent inactives après la mise à niveau de votre logiciel QRadar Network Anomaly Detection. Une infraction inactive ne peut pas redevenir active. Si de nouveaux événements sont détectés pour l'infraction, une nouvelle infraction est créée et l'infraction inactive est conservée jusqu'à ce que la durée de conservation de l'infraction soit écoulée. Vous pouvez effectuer les actions suivantes sur les infractions inactives : protect, flag for follow up, add notes et assign to users. • Hidden Offense - Indique que cette infraction est masquée dans la page All Offenses. Les infractions masquées sont visibles sur la page All Offenses uniquement si vous effectuez une recherche sur les infractions masquées. Pour plus d'informations sur les infractions masquées, voir Masquage des infractions. • User - Indique que l'infraction a été affectée à un utilisateur. Lorsqu'une infraction est affectée à un utilisateur, elle est affichée sur la page My Offenses de cet utilisateur. Pour plus d'informations sur l'affectation des infractions aux utilisateurs Affectation des infractions aux utilisateurs. • Protected - Indique que cette infraction est protégée. La fonction Protect évite que les infractions spécifiées soient retirées de la base de données après que la période de conservation se soit écoulée. Pour plus d'informations sur les infractions protégées, voir Protection des infractions. • Closed Offense - Indique que cette infraction a été fermée. Pour plus d'informations sur la fermeture des infractions, voir Fermeture d'une infraction. <p>Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.</p>
Relevance	Indique l'importance relative de cette infraction.
Severity	Indique la gravité de cette infraction. La gravité précise le niveau de menace que constitue une infraction en relation avec le degré de préparation de l'adresse IP cible pour l'attaque. Cette valeur est directement associée à la catégorie d'événement qui correspond à l'infraction. Par exemple, une attaque Denial of Service (DoS) dispose d'une gravité de 10, ce qui indique une occurrence grave.
Credibility	Indique la crédibilité de cette infraction, telle que déterminée par le classement de crédibilité de dispositifs de source. Par exemple, la crédibilité est augmentée lorsque plusieurs infractions signalent le même événement ou flux.

Tableau 3-5 Paramètres du tableau de l'infraction (suite)

Paramètre	Description
Description	Indique une description de l'infraction.
Source IP(s)	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Cliquez sur le lien pour afficher des détails supplémentaires. Pour plus d'informations sur les adresses IP source, voir Affichage des infractions par source IP .
Destination IP(s)	Indique les adresses IP et le nom de l'actif (si disponible) des destinations locales ou distantes. Cliquez sur le lien pour afficher des détails supplémentaires. Pour plus d'informations sur les adresses IP cible, voir Affichage des infractions par cible IP
Network(s)	Indique le réseau de destination pour cette infraction. Si l'infraction dispose d'un seul réseau de destination, cette zone affiche la feuille de réseau. Cliquez sur le lien pour afficher l'information du réseau. Si l'infraction dispose de plus d'un réseau de destination, le terme Multiple s'affiche. Cliquez sur le lien pour afficher des détails supplémentaires.

Tableau 3-5 Paramètres du tableau de l'infraction (suite)

Paramètre	Description
Offense Type	<p>Indique le type d'infraction. Le type d'infraction est déterminé par la règle qui a créé l'infraction. Par exemple, si le type d'infraction est l'événement source du journal, la règle qui a généré cette infraction est corrélée aux événements en fonction du périphérique qui a détecté l'événement.</p> <p>Les types d'infraction incluent :</p> <ul style="list-style-type: none"> • Source IP • Destination IP • Event Name • User Name • Source MAC Address • Destination MAC Address • Log Source • Host Name • Source Port • Destination Port • Source IPv6 • Destination IPv6 • Source ASN • Destination ASN • Rule • App ID <p>Remarque : Le type d'infraction détermine le type d'information qui s'affiche sur le panneau récapitulatif de la source d'infraction.</p>
Event/Flows Count	<p>Indique le nombre d'événements et de flux qui se sont produits pour cette infraction et le nombre de catégories.</p> <p>Cliquez sur le lien événements afin d'étudier davantage les événements associés à cette infraction. Lorsque vous cliquez sur le lien événements, les résultats de la recherche d'événement s'affichent.</p> <p>Cliquez sur le lien flux afin d'étudier davantage les flux associés à cette infraction. Lorsque vous cliquez sur le lien flux, les résultats de la recherche de flux s'affichent.</p> <p>Remarque : Si le comptage de flux affiche N/A, l'infraction peut avoir une date de début qui précède la date où vous avez effectué une mise à niveau vers IBM Security QRadar Network Anomaly Detection 7.1.0 (MR1), par conséquent, les flux ne peuvent pas être comptés. Vous pouvez, toutefois, cliquer sur le lien N/A pour enquêter sur les flux associés aux résultats de la recherche de flux.</p>

Tableau 3-5 Paramètres du tableau de l'infraction (suite)

Paramètre	Description
Start	Indique la date et l'heure du premier événement ou flux pour cette infraction.
Duration	Indique la quantité de temps écoulée depuis la première détection de cette infraction.
Assigned to	Indique l'utilisateur affecté à cette infraction. Si aucun utilisateur n'est affecté, cette zone indique Not assigned. Cliquez sur Not assigned pour affecter cette infraction à un utilisateur. Pour plus d'informations, voir Affectation des infractions aux utilisateurs .

tableau récapitulatif de la source d'infraction

Le tableau récapitulatif de la source d'infraction indique des informations sur la source de l'infraction. L'information qui s'affiche dans la zone **Offense Source** dépend du type d'infraction. Par exemple, si le type d'infraction est Source Port, la zone **Offense Source** affiche le port source de l'événement qui a créé cette infraction.

REMARQUE

Pour plus d'informations sur les types d'infractions, voir [Offense Type](#). Pour plus d'informations sur les paramètres récapitulatifs de la source d'infraction pour chaque type d'infraction, voir [Options du récapitulatif de la source d'infraction](#).

Tableau des 5 dernières notes

Le tableau des 5 dernières notes indique des informations sur les 5 dernières notes de l'utilisateur de l'infraction. Cliquez sur **Notes** pour afficher des informations supplémentaires. Cliquez sur **Add Notes** pour ajouter une note. Pour plus d'informations sur l'ajout d'une note, voir [Ajout de notes](#).

Tableau 3-6 Paramètres de tableau des 5 dernières notes

Paramètre	Description
Remarques	Indique les notes d'utilisateur pour cette infraction.
Username	Indique l'utilisateur qui a créé cette note.
Date de création	Indique la date et l'heure de création de cette note.

Tableau des 5 principales IP source

Le Tableau des 5 principales IP source indique les cinq principales adresses IP source de cette infraction, organisées en fonction de l'ampleur. Cliquez sur **Sources** pour afficher des informations supplémentaires.

Tableau 3-7 Les 5 sources principales des espaces de présentation de l'image
Paramètres du tableau

Paramètre	Description
Source IP	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau.

Tableau 3-7 Les 5 sources principales des espaces de présentation de l'image
Paramètres du tableau (suite)

Paramètre	Description
Magnitude	Indique l'importance relative de l'adresse IP source. La barre d'ampleur fournit une représentation visuelle de la valeur de risque CVSS de l'actif associé à l'adresse IP source. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir le Glossaire .
Location	Indique l'emplacement réseau de l'adresse IP source.
Vulnerability	Indique si cette adresse IP source dispose de vulnérabilités.
User	Indique le nom d'utilisateur de l'adresse IP source. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
MAC	Indique l'adresse MAC de l'adresse IP source. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown.
Weight	Indique la pondération de l'adresse IP source. La pondération d'une adresse IP est affectée sur l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions pour cette adresse IP source.
Destination(s)	Indique le nombre d'adresses IP cible pour cette adresse IP source.
Last Event/Flow	Indique le temps écoulé depuis que le dernier événement ou flux a été observé pour cette adresse IP source.
Events/Flows	Indique le nombre d'événements ou de flux pour cette adresse IP source.

Tableau des 5 principales IP cible

Le Tableau des 5 principales IP cible indique les cinq principales adresses IP cible de cette infraction, organisées en fonction de l'ampleur. Cliquez sur **Destinations** pour afficher des informations supplémentaires.

Tableau 3-8 Paramètres de tableau des 5 principales cibles de l'espace de présentation de l'image

Paramètre	Description
Destination IP	Indique l'adresse IP ou le nom d'hôte de la cible.
Magnitude	Indique l'importance relative de l'adresse IP cible. La barre d'ampleur fournit une représentation visuelle de la valeur de risque CVSS de l'actif associé à l'adresse IP cible. Déplacez votre souris sur la barre d'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir le Glossaire .
Location	Indique l'emplacement réseau de l'adresse IP cible.
Vulnerability	Indique si l'adresse IP cible dispose de vulnérabilités.

Tableau 3-8 Paramètres de tableau des 5 principales cibles de l'espace de présentation de l'image (suite)

Paramètre	Description
Chained	Indique si l'adresse IP cible est enchaînée. Une adresse IP cible enchaînée est associée à d'autres infractions. Par exemple, une adresse IP cible peut devenir l'adresse IP source pour une autre infraction. Si l'adresse IP cible est enchaînée, cliquez sur Yes pour afficher les infractions enchaînées.
User	Indique le nom d'utilisateur de l'adresse IP cible. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
MAC	Indique l'adresse MAC de l'adresse IP cible. Si aucune adresse MAC n'est identifiée, cette zone indique Inconnu.
Weight	Indique la pondération de l'adresse IP cible. La pondération d'une adresse IP est attribuée à l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions pour cette adresse IP cible.
Source(s)	Indique le nombre des adresses IP source pour cette adresse IP cible.
Last Event/Flow	Indique le temps écoulé depuis que le dernier événement ou flux a été observé pour cette adresse IP cible.
Events/Flows	Indique le nombre d'événements ou de flux pour cette adresse IP cible.

Tableau des 5 principales sources de journal

Le Tableau des 5 principales sources de journal indique les cinq principales sources de journal de cette infraction, organisées en fonction du nombre d'événements par lequel chaque source de journal a contribué à l'infraction. Cliquez sur **Log Sources** pour afficher des informations supplémentaires.

Tableau 3-9 Paramètres de tableau des 5 principales sources de journal

Paramètre	Description
Name	Indique le nom de la source de journal.
Description	Indique la description de la source de journal.
Group	Indique le groupe de source de journal auquel appartient la source de journal.
Events/Flows	Indique le nombre d'événements ou de flux associés à la source de journal pour cette infraction.
Offenses	Indique le nombre d'infractions associés à la source de journal.
Total Events/Flows	Indique le nombre total des événements pour cette source de journal.

Tableau des 5 principaux utilisateurs

Le Tableau des 5 principaux utilisateurs indique les 5 principaux utilisateurs de cette infraction, organisés par le nombre d'infractions par utilisateur. Cliquez sur **Users** pour afficher tous les utilisateurs pour cette infraction.

Tableau 3-10 Paramètres de tableau des 5 principaux utilisateurs

Paramètre	Description
Name	Indique le nom d'utilisateur.
Events/Flows	Indique le nombre d'événements ou de flux associés à l'utilisateur pour cette infraction.
Offenses	Indique le nombre d'infractions associées à l'utilisateur.
Total Events/Flows	Indique le nombre total d'événements ou de flux associés à cet utilisateur.

Tableau des 5 principales catégories

Le Tableau des 5 principales catégories indique les cinq principales globales catégories de cette infraction, organisées en fonction de l'ampleur. Cliquez sur **Categories** pour afficher des informations supplémentaires.

Tableau 3-11 Paramètres de tableau des 5 catégories principales

Paramètre	Description
Name	Indique le nom de la catégorie.
Magnitude	Indique l'importance relative de la catégorie. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de la catégorie. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs pour la catégorie et l'ampleur calculée. <i>Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire.</i>
Local Destination Count	Indique le nombre des adresses IP cible locales associées à cette catégorie.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette catégorie.
First Event/Flow	Indique la date et l'heure de la détection du premier événement pour cette catégorie dans cette infraction.
Last Event/Flow	Indique la date et l'heure de la détection du dernier événement pour cette catégorie dans cette infraction.

Tableau des 10 derniers événements

Le Tableau des 10 derniers événements indique les 10 derniers événements de cette infraction durant la dernière heure, organisés en fonction de l'ampleur. Cliquez sur **Events** pour afficher des informations supplémentaires.

REMARQUE

Si l'infraction sélectionnée a été générée par une règle de détection d'anomalie, un ensemble de paramètres différents s'affichent. Voir [Tableau des 10 derniers événements \(Événements d'anomalie\)](#).

Tableau 3-12 Paramètres de tableau des 10 derniers événements

Paramètre	Description
Event Name	Indique un nom pour cet événement.
Magnitude	Indique l'importance relative de cet événement. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de l'événement. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs pour l'événement et l'ampleur calculée. <i>Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire.</i>
Log Source	Indique la source du journal qui a détecté cet événement.
Category	Indique la catégorie de cet événement.
Destination	Indique l'adresse IP cible de cet événement.
Dst Port	Indique le port de destination de cet événement.
Time	Indique la date et l'heure de la détection du premier événement dans cet événement normalisé. Cette date et heure est spécifiée par le périphérique qui a détecté l'événement.

Tableau des 10 derniers événements (Événements d'anomalie)

Le Tableau des 10 derniers événements (Événements d'anomalie) indique les 10 derniers événements de cette infraction durant la dernière heure. Cliquez sur **Events** pour afficher des informations supplémentaires.

REMARQUE

Ce panneau s'affiche uniquement si l'infraction a été générée par une règle de détection d'anomalie.

Tableau 3-13 Paramètres de tableau des 10 derniers événements(Événements d'anomalie)

Paramètre	Description
Event Name	Indique un nom pour cet événement.
Time	Indique la date et l'heure de la détection du premier événement dans cet événement normalisé. Cette date et heure est spécifiée par le périphérique qui a détecté l'événement.
Anomaly Text	Indique une description du comportement anormal qui a été détecté par la règle de détection d'anomalie.
Anomaly Value	Indique la valeur qui a provoqué la règle de détection d'anomalie pour générer cette infraction.
Anomaly	Sélectionnez cette option pour afficher les résultats de recherche enregistrée qui a provoqué la règle de détection d'anomalie pour générer cet événement.

Tableau des 10 derniers flux

Le Tableau des 10 derniers flux indique les 10 derniers flux de cette infraction durant la dernière heure, organisés en fonction de l'ampleur. Cliquez sur **Flows** pour afficher des informations supplémentaires.

Tableau 3-14 Paramètres de tableau des 10 derniers flux

Paramètre	Description
Application	Indique l'application associée à ce flux.
Source IP	Indique l'adresse IP source de ce flux.
Source Port	Indique le port source de ce flux.
Destination IP	Indique l'adresse IP cible de ce flux.
Destination Port	Indique le port de destination de ce flux.
Total Bytes	Indique le nombre total d'octets pour ce flux.
Last Packet Time	Indique la date et l'heure d'envoi du dernier paquet pour ce flux.

Tableau des 5 principales annotations

Le Tableau des 5 principales annotations indique les 5 principales annotations pour cette infraction. Cliquez sur **Annotations** pour afficher des informations supplémentaires.

Tableau 3-15 Paramètres de tableau des 5 principales annotations

Paramètre	Description
Annotation	Indique les détails pour cette annotation. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux infractions comme composant de la réponse de la règle. Pour plus d'informations sur les règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Time	Indique la date et l'heure de création de cette annotation.
Weight	Indique la pondération de cette annotation.

Options du récapitulatif de la source d'infraction

L'information dans le tableau récapitulatif de la source d'infraction, affichée dans la page récapitulative de l'infraction, dépend du type d'infraction pour l'infraction que vous affichez.

Les types d'infraction incluent :

- **Source IP**
- **Destination IP**
- **Event Name**
- **Username**
- **Source or Destination MAC Address**
- **Log Source**
- **Hostname**

- **Source or Destination Port**
- **Source or Destination IPv6**

- [Source or Destination ASN](#)
- [Rule](#)
- [App ID](#)

Source IP

Si le type d'infraction est Source IP, les informations suivantes s'affichent dans le tableau **Offense Source** :

Tableau 3-16 Paramètres du récapitulatif de l'infraction de la source IP

Paramètre	Description
Source IP	Indique l'adresse IP source associée à l'événement ou au flux qui a créé cette infraction.
Magnitude	Indique l'importance relative de l'adresse IP source. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS de l'actif associé à l'adresse IP source. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire .
User	Indique l'utilisateur associé à cette adresse IP source. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
Host Name	Indique le nom d'hôte associé à l'adresse IP source. Si aucun nom d'hôte n'est identifié, cette zone indique Unknown.
Asset Name	Indique le nom de l'actif, que vous pouvez assigner en utilisant la fonction de profil de l'actif. Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions associées à cette adresse IP source. Cliquez sur le lien pour afficher plus de détails.
Location	Indique l'emplacement réseau de l'adresse IP source. Si l'emplacement est local, vous pouvez cliquer sur le lien pour afficher les réseaux.
Vulnerabilities	Indique le nombre de vulnérabilités identifiées associées à cette adresse IP source. Cette valeur inclut également le nombre de vulnérabilités actives et passives.
MAC	Indique l'adresse MAC de l'adresse IP source lorsque l'infraction a commencé. Si l'adresse MAC est inconnue, cette zone indique Unknown.
Asset Weight	Indique la pondération de l'actif, que vous pouvez affecter en utilisant la fonction de profil de l'actif. Pour plus d'informations, voir Gestion des actifs .
Events/Flows	Indique le nombre d'événements ou de flux associés à l'adresse IP source. Cliquez sur le lien pour afficher plus de détails.

Destination IP

Si le type d'infraction est Destination IP, les informations suivantes s'affichent dans le tableau Offense Source :

Tableau 3-17 Paramètres du récapitulatif de l'infraction IP cible

Paramètre	Description
IP	Indique l'adresse IP cible associée à l'événement ou au flux qui a créé cette infraction.
Magnitude	Indique l'importance relative de l'adresse IP cible. La barre d'ampleur fournit une représentation visuelle de la valeur de risque CVSS de l'actif associé à l'adresse IP cible. Déplacez votre souris sur la barre d'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir le Glossaire .
User	Indique l'utilisateur associé à cette adresse IP cible. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
Host Name	Indique le nom d'hôte associé à l'adresse IP cible. Si aucun nom d'hôte n'est identifié, cette zone indique Unknown.
Asset Name	Indique le nom de l'actif, que vous pouvez assigner en utilisant la fonction de profil de l'actif. Pour plus d'informations, voir Gestion des actifs .
Chained	Indique si l'adresse IP cible est enchaînée. Une adresse IP cible enchaînée est associée à d'autres infractions. Par exemple, une adresse IP cible peut devenir l'adresse IP source pour une autre infraction. Si l'adresse IP cible est enchaînée, cliquez sur Yes pour afficher les infractions enchaînées.
Offenses	Indique le nombre d'infractions associées à cette adresse IP cible. Cliquez sur le lien pour afficher plus de détails.
Location	Indique l'emplacement réseau de l'adresse IP cible. Si l'emplacement est local, vous pouvez cliquer sur le lien pour afficher les réseaux.
Vulnerabilities	Indique le nombre de vulnérabilités identifiées associées à cette adresse IP cible. Cette valeur inclut également le nombre de vulnérabilités actives et passives.
MAC	Indique l'adresse MAC de l'adresse IP cible lorsque l'infraction a commencé. Si l'adresse MAC est inconnue, cette zone indique Unknown.
Asset Weight	Indique la pondération de l'actif, que vous pouvez affecter en utilisant la fonction de profil de l'actif. Pour plus d'informations, voir Gestion des actifs .
Events/Flows	Indique le nombre d'événements ou de flux associés à l'adresse IP cible. Cliquez sur le lien pour afficher plus de détails.

Event Name

Si le type d'infraction est Event Name, les informations suivantes s'affichent dans le tableau Offense Source :

REMARQUE

Les informations affichées pour les infractions Event Name sont dérivées de la carte (QID) d'identificateur QRadar, qui mappe des événements à des identificateurs uniques.

Tableau 3-18 Paramètres du récapitulatif de l'infraction du nom de l'événement

Paramètre	Description
Event Name	Indique le nom de l'événement, comme indiqué dans la carte QID, associé à l'événement ou au flux qui a créé cette infraction. Déplacez votre souris sur le nom de l'événement pour afficher le QID.
High Level Category	Indique la catégorie de haut niveau de l'événement. Pour plus d'informations sur les catégories de haut niveau, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Severity	Indique la gravité de l'événement.
Offenses	Indique le nombre d'infractions associées à ce nom de l'événement. Cliquez sur le lien pour afficher plus de détails.
Low Level Category	Indique la catégorie de bas niveau de l'événement. Pour plus d'informations sur les catégories de bas niveau, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Events/Flows	Indique le nombre d'événements ou de flux associés à ce nom de l'événement. Cliquez sur le lien pour afficher plus de détails.

Username

Si le type d'infraction est Username, les informations suivantes s'affichent dans le tableau Offense Source :

Tableau 3-19 Paramètres du récapitulatif de l'infraction du nom d'utilisateur

Paramètre	Description
Username	Indique le nom d'utilisateur associé à l'événement ou au flux qui a créé cette infraction. Remarque : Si vous survolez le paramètre Username à l'aide du pointeur de votre souris, l'infobulle qui s'affiche fournit le nom d'utilisateur associé aux informations sur le nom d'utilisateur à partir de l'onglet Asset au lieu du nom d'utilisateur associé à l'événement ou au flux ayant créé cette infraction.
Last Known Host	Indique l'hôte en cours auquel est associé l'utilisateur. Si aucun hôte n'est identifié, cette zone indique Unknown. Remarque : Cette zone n'affiche pas les informations historiques.

Tableau 3-19 Paramètres du récapitulatif de l'infraction du nom d'utilisateur (suite)

Paramètre	Description
Last Known MAC	Indique la dernière adresse MAC connue de l'utilisateur. Si aucun code d'authentification de message n'est identifié, cette zone indique Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Last Observed	Indique la dernière date et heure où l'utilisateur a été observé sur le système.
Offenses	Indique le nombre d'infractions associées à cet utilisateur. Cliquez sur le lien pour afficher plus de détails.
Last Known Group	Indique le groupe en cours auquel appartient l'utilisateur. Si aucun groupe n'est actuellement associé au nom d'utilisateur, la valeur de cette zone est Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Last Known Machine	Indique le nom de la machine en cours associé à l'utilisateur. Si aucun nom de machine n'est identifié, cette zone indique Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Last Known IP	Indique l'adresse IP en cours de l'utilisateur. Si aucune adresse IP n'est identifiée, cette zone indique Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Events/Flows	Indique le nombre d'événements ou d'association de flux avec le nom d'utilisateur. Cliquez sur le lien pour afficher plus de détails.

Source or Destination MAC Address

Si le type d'infraction est Source MAC Address ou Destination MAC Address, les informations suivantes s'affichent dans le tableau **Offense Source** :

Tableau 3-20 Paramètres du récapitulatif de l'infraction de l'adresse MAC source ou cible

Paramètre	Description
MAC Address	Indique l'adresse MAC associée à l'événement qui a créé cette infraction. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown.
Last Known Host	Indique l'hôte en cours de l'adresse MAC. Si aucun hôte n'est identifié, cette zone indique Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Last Known Username	Indique l'utilisateur en cours de l'adresse MAC. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>

Tableau 3-20 Paramètres du récapitulatif de l'infraction de l'adresse MAC source ou cible

Paramètre	Description
Last Observed	Indique la dernière date et heure où l'adresse MAC a été observée sur le système.
Offenses	Indique le nombre d'infractions associées à cette adresse MAC. Cliquez sur le lien pour afficher plus de détails.
Last Known IP	Indique l'adresse IP en cours associée à l'adresse MAC. Si aucune adresse IP n'est actuellement associée à l'adresse MAC, la valeur de cette zone est Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Last Known Machine	Indique le nom de la machine en cours associée à l'adresse MAC. Si aucun nom de machine n'est identifié, cette zone indique Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Last Known Group	Indique le groupe en cours associé à l'adresse MAC. Si aucun groupe n'est identifié, cette zone indique Unknown. <i>Remarque : Cette zone n'affiche pas les informations historiques.</i>
Events/Flows	Indique le nombre d'événements associés à cette adresse MAC. Cliquez sur le lien pour afficher plus de détails.

Log Source

Si le type d'infraction est Log Source, les informations suivantes s'affichent dans le tableau Offense Source :

REMARQUE

Les informations affichées pour les infractions sources de journal sont dérivées de la page Log Sources sur l'onglet **Admin**. Vous devez disposer d'une autorisation administrative pour accéder à l'onglet **Admin** et gérer les sources de journal. Pour plus d'informations sur la gestion des sources de journal, voir le *IBM Security QRadar Guide d'utilisation des sources de journal*.

Tableau 3-21 Paramètres du récapitulatif de l'infraction source du journal

Paramètre	Description
Log Source Name	Indique le nom de la source de journal, comme indiqué dans le tableau des sources de journal, associé à l'événement qui a créé cette infraction.
Description	Indique la description de la source de journal.
Last Event/Flow Time	Indique la dernière date et heure où la source de journal a été observée sur le système.
Offenses	Indique le nombre d'infractions associées à cette source de journal. Cliquez sur le lien pour afficher plus de détails.

Tableau 3-21 Paramètres du récapitulatif de l'infraction source du journal (suite)

Paramètre	Description
Log Source Identifier	Indique le nom d'hôte de la source de journal.
Group	Indique à quel groupe la source de journal appartient.
Status	Indique le statut de cette source de journal.
Events/Flows	Indique le nombre d'infractions associées à cette source de journal. Indique le nombre d'événements associés à cette source de journal. Cliquez sur le lien pour afficher plus de détails.

Hostname

Si le type d'infraction est Hostname, les informations suivantes s'affichent dans le tableau Offense Source :

Tableau 3-22 Paramètres du récapitulatif de l'infraction du nom d'hôte

Paramètre	Description
Nom d'hôte	Indique le nom d'hôte associé au flux qui a créé cette infraction.
Last Known MAC	Indique l'adresse MAC associée au nom d'hôte. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown. Remarque : Cette zone n'affiche pas les informations historiques.
Last Known Username	Indique le nom d'utilisateur en cours associé au nom d'hôte. Si aucun utilisateur n'est identifié, cette zone indique Unknown. Remarque : Cette zone n'affiche pas les informations historiques.
Last Observed	Indique la dernière date et heure où le nom d'hôte a été observé sur le système.
Offenses	Indique le nombre d'infractions associées à ce nom d'hôte. Cliquez sur le lien pour afficher plus de détails.
Last Known Machine	Indique le non de machine en cours associé à ce nom d'hôte. Si aucun nom de machine n'est identifié, cette zone indique Unknown. Remarque : Cette zone n'affiche pas les informations historiques.
Last Known IP	Indique l'adresse IP en cours associée au nom d'hôte. Si aucune adresse IP n'est actuellement associée au nom d'hôte, la valeur de cette zone est Unknown. Remarque : Cette zone n'affiche pas les informations historiques.
Last Known Group	Indique le groupe en cours auquel ce nom d'hôte est affecté. Si aucun groupe n'est identifié, cette zone indique Unknown. Remarque : Cette zone n'affiche pas les informations historiques.
Events/Flows	Indique le nombre de flux associés à ce nom d'hôte. Cliquez sur le lien pour afficher plus de détails.

Source or Destination Port

Si le type d'infraction est Source Port ou Destination Port, les informations suivantes s'affichent dans le tableau Offense Source :

Tableau 3-23 Paramètres du récapitulatif du port d'infraction source ou cible.

Paramètre	Description
Port	Indique le port associé à l'événement ou au flux qui a créé cette infraction.

Tableau 3-23 Paramètres du récapitulatif du port d'infraction source ou cible. (suite)

Paramètre	Description
Offenses	Indique le nombre d'infractions associées à ce port. Cliquez sur le lien pour afficher plus de détails.
Events/Flows	Indique le nombre d'événements ou de flux associés à ce port. Cliquez sur le lien pour afficher plus de détails.

Source or Destination IPv6

Si le type d'infraction est Source IPv6 ou Destination IPv6, les informations suivantes s'affichent dans le tableau Offense Source :

Tableau 3-24 Paramètres du récapitulatif de l'infraction IPv6 source ou cible

Paramètre	Description
IPv6	Indique l'adresse IPv6 associée à l'événement ou au flux qui a créé cette infraction.
Offenses	Indique le nombre d'infractions associées à cette adresse IPv6. Cliquez sur le lien pour afficher plus de détails.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette adresse IPv6. Cliquez sur le lien pour afficher plus de détails.

Source or Destination ASN

Si le type d'infraction est Source ASN ou Destination ASN, les informations suivantes s'affichent dans le tableau Offense Source :

Tableau 3-25 Paramètres du récapitulatif de l'infraction de l'avis préalable d'expédition source ou cible

Paramètre	Description
ASN Index	Indique la valeur de l'avis préalable d'expédition associée au flux qui a créé cette infraction.
Offenses	Indique le nombre d'infractions associées à cet avis préalable d'expédition. Cliquez sur le lien pour afficher plus de détails.
Events/Flows	Indique le nombre de flux associés à cet avis préalable d'expédition. Cliquez sur le lien pour afficher plus de détails.

Rule

Si le type d'infraction est Rule, les informations suivantes s'affichent dans le tableau Offense Source :

REMARQUE

L'information affichée pour les infractions de règles est dérivée de l'onglet Rules. Pour plus d'informations sur les règles, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Tableau 3-26 Paramètres du récapitulatif de l'infraction de la règle

Paramètre	Description
Rule Name	Indique le nom de la règle associée à l'événement ou au flux qui a créé cette infraction.
Group(s)	Indique le groupe de règles auquel cette règle appartient.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette règle. Cliquez sur le lien pour afficher plus de détails.
Remarques	Indique les notes de cette règle.
Rule Description	Indique le récapitulatif des paramètres de la règle.
Response	Indique le type de réponse pour la règle.
Rule Type	Indique le type de règle pour l'infraction.
Offenses	Indique le nombre d'infractions associées à cette règle. Cliquez sur le lien pour afficher plus de détails.

App ID

Si le type d'infraction est App ID, les informations suivantes s'affichent dans le tableau Offense Source :

Tableau 3-27 Paramètres du récapitulatif de l'application de division d'identification

Paramètre	Description
Application Name	Indique l'application associée au flux qui a créé cette infraction.
Offenses	Indique le nombre d'infractions associées à cette application. Cliquez sur le lien pour afficher plus de détails.
Events/Flows	Indique le nombre de flux associés à cette application. Cliquez sur le lien pour afficher plus de détails.

Ajout de notes Vous pouvez ajouter des notes à toute infraction sur l'onglet **Offenses**. Les notes peuvent inclure toute information que vous souhaitez capturer pour l'infraction. Par exemple, vous pourriez ajouter une note qui indique une information qui n'est pas automatiquement incluse dans une infraction, comme un numéro de ticket de service clients ou d'information de gestion d'infraction.

Pour ajouter des notes à une infraction :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Naviguez jusqu'à l'infraction à laquelle vous souhaitez ajouter des notes.
- Etape 3** Cliquez deux fois sur l'infraction.
- Etape 4** Sélectionnez l'option **Add Note**.

L'option Add Note est disponible aux emplacements suivants dans un récapitulatif d'infraction :

- **Actions** zone de liste dans la barre d'outils récapitulative d'infraction.
- **Add Note** icône dans le panneau des 5 dernières notes.

Étape 5 Entrez la note que vous souhaitez inclure pour cette infraction. Vous pouvez entrer jusqu'à 1996 caractères.

REMARQUE

Le texte de la note ne recherche pas automatiquement de texte et n'est pas modifiable. Le texte s'affiche exactement sur l'onglet tel qu'il a été entré. Par exemple, si vous entrez le texte sans insérer des retours chariots, le texte de la note s'affiche sur une seule ligne dans le récapitulatif Notes et la colonne Note contient une barre de défilement.

Etape 6 Cliquez sur **Add Note**.

Une note s'affiche dans le panneau Last 5 Notes du récapitulatif d'infraction. Une icône **Notes** s'affiche dans la colonne d'indicateurs de la liste des infractions. Si vous déplacez votre souris sur l'indicateur de notes, la note pour cette infraction s'affiche.

Suppression des infractions de l'onglet Offenses

Vous pouvez supprimer une infraction de l'onglet **Offenses** en utilisant les options suivantes :

- **Masquage des infractions**
- **Affichage des infractions masquées**
- **Fermeture d'une infraction**
- **Fermeture des infractions listées**

Vous pouvez masquer ou fermer une infraction de toute liste des infractions (par exemple, All Offenses) ou les pages Offense Summary. Les procédures ci-dessous fournissent des instructions sur le masquage et la fermeture des infractions à partir de la page All Offenses.

Masquage des infractions

Après avoir masqué une infraction, l'infraction ne s'affiche plus dans aucune liste (par exemple, All Offenses) dans l'onglet **Offenses**; Cependant, si vous effectuez une recherche qui inclut les infractions masquées, l'élément s'affiche dans les résultats de recherche. Pour masquer une infraction :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Sélectionnez l'infraction que vous souhaitez masquer.

REMARQUE

Pour masquer plusieurs infractions, maintenez la touche de contrôle enfoncée pendant que vous sélectionnez chaque infraction que vous souhaitez masquer.

Etape 4 Dans la zone de liste **Actions**, sélectionnez **Hide**.

Etape 5 Cliquez sur **OK**.

La page All Offenses affiche toutes les infractions, à l'exception des infractions masquées.

REMARQUE

Si vous consultez les résultats d'une recherche configurée pour exclure les infractions masquées, les comptages d'infractions qui s'affichent dans le volet By Category de l'onglet **Offenses** peuvent être erronés. Si vous voulez voir le compte total dans le volet By Category, décochez la case **Hidden Offenses** dans le volet Excludes de votre page de recherche des infractions.

Affichage des infractions masquées

Les infractions masquées ne sont pas visibles sur l'onglet **Offenses**, cependant, vous pouvez afficher les infractions masquées si vous souhaitez les afficher à nouveau. Pour afficher les infractions masquées :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **All Offenses**.
- Etape 3** Utilisez la fonction de recherche pour afficher les infractions masquées :
 - a Dans la zone de liste **Search**, sélectionnez **New Search**.
 - b Dans la liste **Exclude option** sur le panneau Search Parameters, décochez la case **Hidden Offenses**.
 - c Cliquez sur **Search**.

La page All Offenses page s'affiche, incluant toutes les infractions. L'infraction est spécifiée comme masquée par l'icône **Hidden** dans la colonne d'indicateur. Les infractions masquées sont encore configurées comme masquées, par conséquent, la prochaine fois que vous affichez toutes les infractions sans que les paramètres de recherche soient appliqués, vous ne verrez pas les infractions masquées.

- Etape 4** Localisez et sélectionnez l'infraction masquée que vous souhaitez afficher.

- Etape 5** A partir de la zone de liste **Actions**, sélectionnez **Show**.

Désormais l'infraction masquée n'est plus configurée comme masquée.

Fermeture d'une infraction

Après avoir fermé (supprimé) une infraction, l'infraction ne s'affiche plus dans aucune liste (par exemple, All Offenses) sur l'onglet **Offenses**. L'infraction fermée est supprimée de la base de données après que la durée de conservation de l'infraction est écoulée. La valeur par défaut de la durée de conservation de l'infraction est 3 jours. Si des événements supplémentaires se produisent pour cette infraction, une nouvelle infraction est créée. Si vous effectuez une recherche qui inclut les infractions fermées, l'article est affiché dans les résultats de la recherche tant qu'il n'a pas été retiré de la base de données.

Pour fermer une infraction :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **All Offenses**.
- Etape 3** Sélectionnez l'infraction que vous souhaitez fermer.

REMARQUE

Pour fermer plusieurs infractions, maintenez la touche de contrôle enfoncée pendant que vous sélectionnez chaque infraction que vous souhaitez fermer.

- Etape 4** Dans la zone de liste **Actions**, sélectionnez **Close**.
- Etape 5** Dans la zone de liste **Reason for Closing**, sélectionnez une cause. La valeur par défaut de la cause est **non-issue**.

Etape 6 Dans la zone de liste **Reason for Closing**, sélectionnez une cause.

Si vous disposez des droits d'administrateur, vous pouvez ajouter des causes personnalisées dans la zone de liste **Reason for Closing** :

- a Cliquez sur l'icône **Edit Custom Reasons**.
- b Dans la zone **Reason**, entrez une raison. La saisie doit contenir entre 5 et 60 caractères.
- c Cliquez sur **OK**.

Etape 7 Facultatif. Dans la zone **Notes**, entrez une note. Elle s'affiche sur la page des détails de l'infraction.

Etape 8 Cliquez sur **OK**.

REMARQUE

Après avoir fermé une infraction, les comptages qui s'affichent sur le panneau By Category de l'onglet **Offenses** peuvent nécessiter plusieurs minutes afin de répercuter l'infraction fermée.

Fermeture des infractions listées

Les infractions qui s'affichent sur la page de synthèse incluent soit toutes les infractions ou, si une recherche est appliquée, un sous-ensemble des infractions. Vous pouvez fermer (supprimer) toutes les infractions listées de l'onglet **Offenses**. Après l'écoulement de la période de conservation de l'infraction, les infractions fermées sont supprimées de la base de données. Si des événements supplémentaires se produisent pour cette infraction, une nouvelle infraction est créée. Si vous effectuez une recherche qui inclut les infractions fermées, l'article est affiché dans les résultats de la recherche tant qu'il n'a pas été retiré de la base de données.

Pour fermer les infractions listées :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Dans la zone de liste **Actions**, sélectionnez **Close Listed**.

Etape 4 Dans la zone de liste **Reason for Closing**, sélectionnez une cause. La valeur par défaut de la cause est **non-issue**.

Si vous disposez des droits d'administrateur, vous pouvez ajouter des causes personnalisées dans la zone de liste **Reason for Closing** :

- a Cliquez sur l'icône **Edit Custom Reasons**.
- b Dans la zone **Reason**, entrez une raison. La saisie doit contenir entre 5 et 60 caractères.
- c Cliquez sur **OK**.

Etape 5 Facultatif. Dans la zone **Notes**, entrez une note. Elle s'affiche sur la page des détails de l'infraction.

Etape 6 Cliquez sur **OK**.

Les infractions fermées ne sont plus listées.

REMARQUE

Après avoir fermé les infractions, les comptages qui s'affichent sur le panneau By Category de l'onglet **Offenses** peuvent prendre plusieurs minutes afin de répercuter les infractions fermées.

Protection des infractions

Les infractions sont conservées pendant une durée de conservation configurable. La valeur par défaut de la durée de conservation est 3 jours. Cependant, les utilisateurs Admin peuvent personnaliser la durée de conservation. Vous pourriez disposer d'infractions que vous souhaitez conserver quelle que soit la durée de conservation. Vous pouvez utiliser la fonction Protect pour éviter que ces infractions soient retirées de la base de données lorsque la durée de conservation est écoulée. Pour plus d'informations sur la durée de conservation de l'infraction, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.



ATTENTION

Lorsque le modèle de données SIM est réinitialisé en utilisant l'option **Hard Clean**, toutes les infractions, y compris les infractions protégées, sont supprimées de la base de données et du disque. Vous devez disposer de privilèges administratifs afin de réinitialiser le modèle de données SIM. Pour plus d'informations, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Cette section comprend les rubriques suivantes :

- [Protection des infractions](#)
- [Protection des infractions listées](#)
- [Déprotection des infractions](#)
- [Déprotection des infractions listées](#)

Protection des infractions

Pour protéger les infractions :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **All Offenses**.
- Etape 3** Sélectionnez l'infraction que vous souhaitez protéger.

REMARQUE

Pour protéger plusieurs infractions, maintenez la touche de contrôle enfoncée pendant que vous sélectionnez chaque infraction que vous souhaitez protéger.

- Etape 4** A partir de la zone de liste **Actions**, sélectionnez **Protect**.
- Etape 5** Cliquez sur **OK**.

L'infraction protégée est indiquée par une icône **Protected** dans la colonne d'indicateur.

Protection des infractions listées

Pour protéger les infractions listées :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **All Offenses**.
- Etape 3** A partir de la zone de liste **Actions**, sélectionnez **Protect Listed**.
- Etape 4** Cliquez sur **OK**.

Les infractions protégées sont indiquées par une icône **Protected** dans la colonne Flag.

Déprotection des infractions

Pour déprotéger les infractions :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **All Offenses**.
- Etape 3** Sélectionnez l'infraction que vous souhaitez déprotéger.

REMARQUE

Pour déprotéger plusieurs infractions, maintenez la touche de contrôle enfoncée pendant que vous sélectionnez chaque infraction que vous souhaitez déprotéger.

REMARQUE

Vous pouvez utiliser la fonction de recherche pour afficher uniquement les infractions protégées. Si vous décochez la case **Protected** et vous vous assurez que toutes les autres options sont sélectionnées dans la liste **Excludes option** sur le panneau Search Parameters, seules les infractions protégées s'affichent.

- Etape 4** A partir de la zone de liste **Actions**, sélectionnez **Unprotect**.
- Etape 5** Cliquez sur **OK**.

L'infraction non protégée ne s'affiche plus dans l'icône **Protected** dans la colonne d'indicateur.

Déprotection des infractions listées

Pour déprotéger les infractions listées :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **All Offenses**.

REMARQUE

Vous pouvez utiliser la fonction de recherche pour afficher uniquement les infractions protégées. Si vous décochez la case protégée et vous vous assurez que toutes les autres options sont sélectionnées dans la liste **Excludes option** sur le panneau Search Parameters, seules les infractions protégées s'affichent.

- Etape 3** A partir de la zone de liste **Actions**, sélectionnez **Unprotect Listed**.
- Etape 4** Cliquez sur **OK**.

Les infractions non protégées n'affichent plus l'icône **Protected** dans la colonne Flag.

Exportation des infractions

Vous pouvez exporter des infractions au format Extensible Markup Language (XML) ou Comma Separated Values (CSV). L'exportation des infractions vous autorise à ré-utiliser ou à stocker vos données sur les infractions. Par exemple, vous pouvez exporter des infractions pour créer des rapports non basés sur QRadar Network Anomaly Detection. Vous pouvez également exporter des infractions comme stratégie secondaire de conservation à long terme. Le service clients peut vous demander d'exporter des infractions pour des fins d'identification et de résolution des problèmes.

Le fichier résultant XML ou CSV contient les paramètres spécifiés dans le panneau Column Definition de vos paramètres de recherche. La durée nécessaire pour exporter vos données dépend du nombre de paramètres spécifiés.

Pour exporter des infractions :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de navigation, cliquez sur **All Offenses**.

Etape 3 Sélectionnez l'infraction que vous souhaitez exporter.

Etape 4 Sélectionnez une des options suivantes :

- Si vous souhaitez exporter les infractions au format XML, sélectionnez **Actions > Export to XML** dans la zone de liste **Actions**.
- Si vous souhaitez exporter les infractions au format CSV, sélectionnez **Actions > Export to CSV** dans la zone de liste **Actions**

Etape 5 Choisissez l'une des opérations suivantes :

- Si vous souhaitez ouvrir la liste pour l'affichage immédiat, sélectionnez l'option **Open with** et sélectionnez une application dans la zone de liste.
- Si vous souhaitez enregistrer la liste, sélectionnez l'option **Save to Disk**.

Etape 6 Cliquez sur **OK**.

Affectation des infractions aux utilisateurs

En utilisant l'onglet **Offenses**, vous pouvez affecter des infractions aux utilisateurs QRadar Network Anomaly Detection pour investigation. Lorsqu'une infraction est affectée à un utilisateur, elle est affichée sur la page My Offenses de cet utilisateur. Vous devez disposer de privilèges appropriés pour affecter des infractions aux utilisateurs. Pour plus d'informations sur les rôles d'utilisation, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Vous pouvez attribuer des infractions aux utilisateurs soit à partir de l'onglet **Offenses** ou des pages Offense Summary. La procédure ci-dessous donne des instructions sur l'affectation des infractions à partir de l'onglet **Offenses**.

Pour affecter une infraction à un utilisateur :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **All Offenses**.
- Etape 3** Sélectionnez l'infraction que vous souhaitez affecter.

REMARQUE

Pour affecter plusieurs infractions, maintenez la touche de contrôle enfoncée pendant que vous sélectionnez chaque infraction que vous souhaitez affecter.

- Etape 4** A partir de la zone de liste **Actions**, sélectionnez **Assign**.
- Etape 5** A partir de la zone de liste **Username**, sélectionnez l'utilisateur auquel vous souhaitez affecter cette infraction.

REMARQUE

La zone de liste **Username** affiche uniquement les utilisateurs qui disposent des privilèges de l'onglet **Offenses**.

- Etape 6** Cliquez sur **Save**.

L'infraction est attribuée à l'utilisateur sélectionné. L'icône **User** s'affiche dans la colonne d'indicateur de l'onglet **Offenses** pour indiquer que cette infraction est affectée. L'utilisateur désigné peut également voir cette infraction dans sa page My Offenses.

Envoi de notification par e-mail

Vous pouvez envoyer un e-mail contenant un récapitulatif d'infraction à n'importe quelle adresse e-mail valide. Le corps du message électronique contient les informations suivantes (si disponible) :

- Adresse IP source
- Nom d'utilisateur source, nom d'hôte ou nom de l'actif.
- Nombre total des sources
- Les cinq principales sources de l'ampleur
- Réseaux sources
- Adresse IP cible
- Nom d'utilisateur cible, nom d'hôte ou nom de l'actif.
- Nombre total des cibles
- Les cinq principales cibles de l'ampleur
- Réseaux cible
- Nombre total des événements
- Les règles qui ont causé le déclenchement de l'infraction ou de la règle d'événement
- Description complète de l'infraction ou de la règle d'événement
- Division d'identification de l'infraction

- Les cinq principales catégories
- Heure de début de l'infraction ou heure de l'événement généré
- Les cinq principales annotations
- Lien vers l'infraction dans l'interface utilisateur QRadar Network Anomaly Detection
- Contribution aux règles CRE

Pour envoyer une notification par e-mail :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Naviguez jusqu'à l'infraction pour laquelle vous souhaitez envoyer une notification par courrier électronique

Etape 3 Cliquez deux fois sur l'infraction.

Etape 4 Dans la zone de liste **Actions**, sélectionnez **Email**.

Etape 5 Entrez des valeurs pour les paramètres suivants :

Tableau 3-28 Paramètres des préférences de notification

Item	Description
To	Entrez l'adresse e-mail de l'utilisateur que vous souhaitez notifier si un changement se produit dans l'infraction sélectionnée. Séparez les nombreuses adresses e-mail avec une virgule.
From	Tapez l'adresse e-mail d'origine configurée par défaut. La valeur configurée par défaut est root@localhost.com.
Email Subject	Entrez l'objet par défaut pour l'e-mail. La valeur configurée par défaut est Offense ID.
Email Message	Entrez le message standard que vous souhaitez pour accompagner la notification e-mail.

Etape 6 Cliquez sur **Send**.

Un e-mail est immédiatement envoyé aux destinataires de l'e-mail.

Marquage d'un article pour suivi En utilisant l'onglet **Offenses**, vous pouvez marquer une infraction, une adresse IP source, une adresse IP cible et un réseau pour suivi. Ceci vous permet de contrôler un article particulier pour une investigation complémentaire.

Pour marquer un article pour suivi :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Naviguez jusqu'à l'infraction que vous souhaitez marquer pour suivi.

Etape 3 Cliquez deux fois sur l'infraction que vous souhaitez marquer pour suivi.

Etape 4 A partir de la zone de liste **Actions**, sélectionnez **Follow up**.

L'infraction affiche désormais un indicateur dans la colonne **Flags**, indiquant que l'infraction est marquée pour suivi.

REMARQUE

Si vous ne voyez pas votre infraction marquée sur la liste d'infractions, vous pouvez trier la liste pour afficher en premier toutes les infractions marquées. Pour trier une liste d'infraction par infraction marquée, cliquez deux fois sur l'en-tête de colonne **Flags**.

Affichage des infractions par catégorie

La page By Category details vous fournit une vue d'ensemble des infractions fondées sur la catégorie de haut niveau.

REMARQUE

Par défaut, la page By Category details est organisée en fonction du comptage d'infraction. Si vous changez l'affichage, cliquez sur **Save Layout** pour enregistrer l'affichage actuel comme votre vue par défaut. La prochaine fois que vous vous connectez à l'onglet **Offenses**, l'agencement enregistré s'affiche.

Pour afficher les infractions par catégorie :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Sur le menu de navigation, cliquez sur **By Category**.

La page des détails By Category affiche les catégories de haut niveau. Les comptages pour chaque catégorie sont accumulés à partir des valeurs dans les catégories de bas niveau.

REMARQUE

Les catégories de bas niveau sur les infractions associées sont affichées avec une flèche. Vous pouvez cliquer sur la flèche pour afficher les catégories de bas niveau. Si vous souhaitez afficher toutes les catégories, cliquez sur **Show Inactive Categories**.

REMARQUE

Les zones de comptages, telles que **Event/Flow Count** et **Source Count**, ne considèrent pas les autorisations réseau de l'utilisateur.

Etape 3 Pour afficher plus d'informations sur la catégorie de bas niveau pour une catégorie particulière, cliquez sur la flèche à côté du nom de la catégorie.

Etape 4 Pour afficher des informations détaillées sur l'infraction, cliquez deux fois sur n'importe quelle catégorie de bas niveau pour afficher la liste des infractions associées.

Pour plus d'informations sur la gestion des infractions, voir [Gestion des infractions](#).

Affichage des infractions par source IP

Vous pouvez afficher les infractions organisées par adresse IP source. Une adresse IP source indique l'hôte qui a généré les infractions à la suite d'une tentative d'attaque sur votre système. Toutes les adresses IP source sont listées en premier en fonction de la plus grande ampleur. La liste des infractions affiche uniquement les adresses IP source des infractions actives.

Pour afficher les infractions par adresse IP source :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Cliquez sur **By Source IP**.

La page de détails By Source IP fournit les informations suivantes :

Tableau 3-29 Paramètres de la page By Source IP Details Page Parameters

Paramètre	Description
View Offenses	Sélectionnez une option dans cette zone de liste pour filtrer les infractions que vous souhaitez afficher sur cette page. Vous pouvez consulter toutes les infractions ou filtrer les infractions en fonction d'un intervalle. A partir de la zone de liste, vous pouvez sélectionner l'intervalle que vous souhaitez filtrer.
Current Search Parameters	La partie supérieure du tableau affiche les détails des paramètres de recherche appliqués aux résultats de la recherche. Pour supprimer ces paramètres de recherche, cliquez sur Clear Filter . <i>Remarque : Ce paramètre s'affiche uniquement après l'application d'un filtre.</i>
Flag	Indique l'action menée sur l'adresse IP source. Par exemple si un indicateur s'affiche, l'infraction est l'adresse IP source pour le suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Source IP	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau.
Magnitude	Indique l'importance relative de l'adresse IP source. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS de l'actif associé à l'adresse IP source. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire .
Location	Indique le réseau, le continent ou le pays où l'adresse IP source est localisée. Les pays sont représentés par indicateur.
Vulnerability	Indique si cette adresse IP source dispose de vulnérabilités.
User	Indique l'utilisateur associé à cette adresse IP source. Si aucun utilisateur n'est identifié, cette zone indique Inconnu.
MAC	Indique l'adresse MAC associée à cette adresse IP source. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown.
Weight	Indique la pondération de cette adresse IP source. La pondération d'une adresse IP est affectée sur l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions associées à cette adresse IP source.
Destination(s)	Indique le nombre des adresses IP cible associées à cette adresse IP source.
Last Event/Flow	Indique le temps écoulé depuis que le dernier événement ou flux a été observé sur le système pour cette adresse IP source.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette adresse IP source.

Etape 3 Cliquez deux fois sur l'adresse IP source que vous souhaitez afficher.

REMARQUE

Si vous souhaitez afficher l'adresse IP source sur une nouvelle page, maintenez la touche de contrôle pendant que vous cliquez deux fois sur l'adresse IP source.

REMARQUE

La partie supérieure de la page affiche le trajet de navigation vers l'affichage en cours. Si vous souhaitez renvoyer à une page déjà affichée, cliquez sur le nom de la page sur le trajet de navigation.

La page Source Details fournit les informations suivantes :

Tableau 3-30 Source Détails de paramètres de page

Paramètre	Description
Magnitude	Indique l'importance relative de l'adresse IP source. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS de l'actif associé à l'adresse IP source. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire .
IP	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau.
Location	Indique l'emplacement de l'adresse IP source. Les pays sont représentés par leurs indicateurs.
Offense(s)	Indique les noms des infractions associées à cette adresse IP source. Pour afficher des informations supplémentaires à propos de l'infraction, cliquez sur le nom ou le terme qui s'affiche. Si de multiples infractions existent, le terme Multiple s'affiche.
Local Destination(s)	Indique la destination locale des adresses IP associées à l'adresse IP source. Pour afficher des informations supplémentaires sur les adresses IP cible, cliquez sur l'adresse IP ou sur le terme qui s'affiche. Si plusieurs adresses IP cible existent, le terme Multiple s'affiche.
Events/Flows	Indique le nombre total d'événements ou de flux associés à cette adresse IP source.
First event/flow seen on	Indique la date et l'heure où cette adresse IP source a généré le premier événement ou flux.
Last event/flow seen on	Indique la date et l'heure du dernier événement ou flux générés associés à cette adresse IP source.

La barre d'outils source fournit les fonctions suivantes :

Tableau 3-31 Barre d'outils Source

Fonction	Description
Destinations	Cliquez sur Destinations pour afficher la liste des adresses locales IP cible pour cette adresse IP source.

Tableau 3-31 Barre d'outils Source (suite)

Fonction	Description
Offenses	Cliquez sur Offenses pour afficher une liste d'infractions associées à l'adresse IP source.
Remarques	Cliquez sur Notes pour afficher toutes les notes pour cette adresse IP source. Pour plus d'informations à propos des notes, voir Ajout de notes .
Actions	A partir de la zone de liste Actions vous pouvez sélectionner l'une des actions suivantes : <ul style="list-style-type: none"> • Follow up - Sélectionnez cette option pour marquer cette infraction pour un suivi ultérieur. Voir Marquage d'un article pour suivi. • Add Notes - Sélectionnez cette option afin d'ajouter des notes pour cette adresse IP cible. Voir Ajout de notes. • Print - Sélectionnez cette option pour imprimer cette infraction.

Etape 4 Pour afficher une liste des adresses IP cible locales pour l'adresse IP source, cliquez sur **Destinations** dans la page de la barre d'outils source.

La liste des destinations locales fournit les informations suivantes :

Tableau 3-32 Par Source IP - Liste des destinations locales

Paramètre	Description
Flag	Indique l'action menée sur l'adresse IP cible. Par exemple, si un indicateur est affiché, l'adresse IP cible est marquée pour le suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Destination IP	Indique l'adresse IP de la destination. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>
Magnitude	Indique l'importance relative de cette adresse IP cible. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de l'adresse IP cible. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire .
Location	Indique l'emplacement de l'adresse IP cible.
Vulnerability	Indique si cette adresse IP cible dispose de vulnérabilités.
User	Indique le nom d'utilisateur de l'adresse IP cible. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
MAC	Indique l'adresse MAC de l'adresse IP cible. Si aucune adresse MAC n'est identifiée, cette zone indique Inconnu.

Tableau 3-32 Par Source IP - Liste des destinations locales (suite)

Paramètre	Description
Weight	Indique la pondération de cette adresse IP cible. La pondération d'une adresse IP est attribuée à l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions associées à cette adresse IP cible.
Source(s)	Indique le nombre d'adresses IP source associées à cette adresse IP cible.
Last Event/Flow	Indique le temps écoulé depuis le dernier événement ou flux.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette adresse IP cible.

La liste de la barre d'outils des destinations locales fournit les fonctions suivantes :

Tableau 3-33 Par Source IP - Barre d'outils de la liste des destinations locales

Fonction	Description
Offenses	Cliquez sur Offenses pour afficher une liste des infractions pour cette adresse IP cible.
Sources	Cliquez sur Sources pour afficher une liste d'adresses IP source associées à cette adresse IP cible. Pour plus d'informations, voir Tableau 3-29 .
Search	<p>Cliquez sur Search pour filtrer les IP cible pour cette adresse IP source. Pour filtrer les cibles :</p> <ol style="list-style-type: none"> 1 Cliquez sur Search. 2 Entrez des valeurs pour les paramètres suivants : <ul style="list-style-type: none"> Destination Network - Dans la zone de liste, sélectionnez le réseau que vous souhaitez filtrer. Magnitude - Dans la zone de liste, sélectionnez si vous souhaitez filtrer l'ampleur par Égale à, Inférieure à, ou Supérieure à la valeur configurée. Sort by - Dans la zone de liste, sélectionnez la façon dont vous voulez trier les résultats du filtre. 3 Cliquez sur Search. <p>Pour plus d'informations sur les résultats, voir le tableau Tableau 3-32.</p>

Etape 5 Pour afficher une liste des infractions associées à cette adresse IP source, cliquez sur **Offenses** dans la barre d'outils de la page source.

Tableau 3-34 Par Source IP - Liste des infractions

Paramètre	Description
Flag	<p>Indique les mesures prises sur l'infraction. Les actions sont représentées par les icônes suivantes :</p> <ul style="list-style-type: none"> • Flag - Indique que l'infraction est marquée pour suivi. Ceci vous permet de contrôler un article particulier pour une investigation complémentaire. Pour plus d'informations sur le marquage d'une infraction pour suivi, voir Marquage d'un article pour suivi. • User - Indique que l'infraction a été affectée à un utilisateur. Lorsqu'une infraction est affectée à un utilisateur, elle est affichée sur la page My Offenses de cet utilisateur. Pour plus d'informations sur l'affectation des infractions aux utilisateurs, voir Affectation des infractions aux utilisateurs. • Notes - Indique qu'un utilisateur a ajouté des notes à l'infraction. Les notes peuvent inclure toute information que vous souhaitez capturer pour l'infraction. Par exemple, vous pourriez ajouter une note qui indique une information qui n'est pas automatiquement incluse dans une infraction, comme un numéro de ticket de service clients ou d'information de gestion d'infraction. Pour plus d'informations à propos des notes, voir Ajout de notes. • Protected - Indique que cette infraction est protégée. La fonction Protect évite que les infractions spécifiées soient retirées de la base de données après que la période de conservation se soit écoulée. Pour plus d'informations sur les infractions protégées, voir Protection des infractions. • Inactive Offense - Indique qu'il s'agit d'une infraction inactive. Une infraction devient inactive au bout de cinq jours après que l'infraction a reçu le dernier événement. En outre, toutes les infractions deviennent inactives après la mise à niveau de votre logiciel QRadar Network Anomaly Detection. <p>Une infraction inactive ne peut pas redevenir active. Si de nouveaux événements sont détectés pour l'infraction, une nouvelle infraction est créée et l'infraction inactive est conservée jusqu'à ce que la durée de conservation de l'infraction soit écoulée. Vous pouvez effectuer les actions suivantes sur les infractions inactives: protéger, indiquer pour suivi, ajouter des notes, et affecter aux utilisateurs.</p> <p>Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.</p>
ID	Indique l'identificateur QRadar Network Anomaly Detection pour cette infraction.
Description	Indique la description de cette infraction.
Offense Type	Indique le type d'infraction. Le type d'infraction est déterminé par la règle qui a créé l'infraction. Par exemple, si le type d'infraction est l'événement source de journal, la règle qui a généré cette infraction est corrélée aux événements en fonction du périphérique qui a détecté l'événement.

Tableau 3-34 Par Source IP - Liste des infractions (suite)

Paramètre	Description
Offense Source	Indique des informations sur la source de l'infraction. L'information qui s'affiche dans la zone Offense Source dépend du type d'infraction. Par exemple, si le type d'infraction est Source Port, la zone Offense Source affiche le port source de l'événement qui a créé cette infraction.
Magnitude	Indique l'importance relative de l'infraction. la barre d'ampleur offre une représentation visuelle de toutes les variables corrélées des événements et des flux. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. <i>Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire.</i>
Source IPs	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Destination IPs	Indique les adresses IP et les noms de l'actif (si disponibles) de la destination associée à cette infraction. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Users	Indique les utilisateurs associés à cette infraction. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
Log Sources	Indique les sources de journal associées à cette infraction.
Events	Indique le nombre d'événements associés à cette infraction.
Flows	Indique le nombre de flux associés à cette infraction.
Start Date	Indique la date et l'heure de la première occurrence de cette infraction.
Last Event/Flow	Indique le temps écoulé depuis le dernier événement ou flux.

La liste de la barre d'outils des infractions fournit les fonctions suivantes :

Tableau 3-35 Par Source IP - Barre d'outils de la liste des infractions

Fonction	Description
Sources	Cliquez sur Sources pour afficher une liste d'adresses IP source pour l'infraction sélectionnée. Pour plus d'informations, voir Affichage des infractions par source IP .
Destinations	Cliquez sur Destinations pour voir toutes les adresses IP cible pour l'infraction sélectionnée. Pour plus d'informations, voir Affichage des infractions par cible IP .

Tableau 3-35 Par Source IP - Barre d'outils de la liste des infractions (suite)

Fonction	Description
Categories	<p data-bbox="638 352 1469 411">Cliquez sur Categories pour afficher les informations de catégorie pour l'infraction sélectionnée.</p> <ul data-bbox="638 426 1469 898" style="list-style-type: none"> <li data-bbox="638 426 1469 453">• Name - Indique le nom de la catégorie associée à l'infraction. <li data-bbox="638 468 1469 663">• Magnitude - Indique l'importance relative de la catégorie. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de la catégorie. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs pour la catégorie et l'ampleur calculée. Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire. <li data-bbox="638 678 1469 737">• Local Destination Count - Indique le nombre d'adresses IP cible associées à cette catégorie. <li data-bbox="638 751 1469 810">• Events/Flows - Indique le nombre d'événements ou de flux associés à cette catégorie. <li data-bbox="638 825 1469 852">• First Event/Flow - Indique la date du premier événement ou flux. <li data-bbox="638 867 1469 894">• Last Event/Flow - Indique la date du dernier événement ou flux. <p data-bbox="638 909 1469 999">Remarque : Vous pouvez également étudier davantage les événements associés à une catégorie spécifique en cliquant sur le bouton droit et en sélectionnant Events.</p> <p data-bbox="638 1014 1469 1073">Pour plus d'informations sur les catégories, voir Affichage des infractions par catégorie.</p>
Annotations	<p data-bbox="638 1094 1469 1152">Cliquez sur Annotations pour afficher toutes les annotations pour l'infraction sélectionnée, y compris :</p> <ul data-bbox="638 1167 1469 1421" style="list-style-type: none"> <li data-bbox="638 1167 1469 1335">• Annotation - Indique les détails de cette annotation. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux infractions comme composant de la réponse de la règle. Pour plus d'informations sur les règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>. <li data-bbox="638 1350 1469 1377">• Time - Indique la date et l'heure de cette annotation. <li data-bbox="638 1392 1469 1419">• Weight - Indique la pondération de cette annotation.

Tableau 3-35 Par Source IP - Barre d'outils de la liste des infractions (suite)

Fonction	Description
Networks	<p data-bbox="626 338 1456 401">Cliquez sur Networks pour afficher tous les réseaux de destination pour l'infraction sélectionnée, y compris :</p> <ul data-bbox="626 411 1456 1087" style="list-style-type: none"> <li data-bbox="626 411 1456 506">• Flag - Indique l'action menée sur le réseau. Par exemple, si un indicateur s'affiche, le réseau est marqué pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires. <li data-bbox="626 516 1456 548">• Network - Indique le nom du réseau de destination. <li data-bbox="626 558 1456 726">• Magnitude - Indique l'importance relative du réseau de destination. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS des actifs associés au réseau de destination. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire. <li data-bbox="626 737 1456 800">• Source IPs - Indique le nombre d'adresses IP source associées à ce réseau. <li data-bbox="626 810 1456 873">• Destination IPs - Indique le nombre d'adresses IP cible associées à ce réseau. <li data-bbox="626 884 1456 947">• Offenses Targeted - Indique le nombre d'infractions ciblées sur ce réseau. <li data-bbox="626 957 1456 1020">• Offenses Launched - Indique le nombre d'infractions lancées par ce réseau. <li data-bbox="626 1031 1456 1087">• Events/Flows - Indique le nombre d'événements ou de flux associés à ce réseau.
Actions	<p data-bbox="626 1098 1456 1161">A partir de la zone de liste Actions, vous pouvez sélectionner l'une des actions suivantes :</p> <ul data-bbox="626 1171 1456 1568" style="list-style-type: none"> <li data-bbox="626 1171 1456 1266">• Hide - Sélectionnez cette option pour masquer cette infraction. Pour plus d'informations sur le masquage des infractions, voir Masquage des infractions. <li data-bbox="626 1276 1456 1371">• Show - Sélectionnez cette option pour afficher toutes les infractions masquées. Pour plus d'informations sur l'affichage des infractions, voir Affichage des infractions masquées. <li data-bbox="626 1381 1456 1476">• Close - Sélectionnez cette option pour fermer une infraction. Pour plus d'informations sur la fermeture des infractions, voir Fermeture d'une infraction. <li data-bbox="626 1486 1456 1568">• Close Listed - Sélectionnez cette option pour fermer l'infraction listée. Pour plus d'informations sur la fermeture des infractions listées, voir Fermeture des infractions listées.

Affichage des infractions par cible IP

Vous pouvez afficher une liste des adresses IP cible locales pour des infractions générées dans votre déploiement. Toutes les adresses IP cible sont listées en premier en fonction de la plus grande ampleur.

Pour afficher les infractions par adresse IP cible :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Cliquez sur **By Destination IP**.

La page de détails By Destination IP fournit les informations suivantes :

Tableau 3-36 Par paramètres de page de détails de destination d'adresse IP

Paramètre	Description
View Offenses	Sélectionnez une option dans cette zone de liste pour filtrer les infractions que vous souhaitez afficher sur cette page. Vous pouvez consulter toutes les infractions ou filtrer les infractions en fonction d'un intervalle. A partir de la zone de liste, vous pouvez sélectionner l'intervalle que vous souhaitez filtrer.
Current Search Parameters	La partie supérieure du tableau affiche les détails des paramètres de recherche appliqués aux résultats de la recherche. Pour supprimer ces paramètres de recherche, cliquez sur Clear Filter . <i>Remarque : Ce paramètre s'affiche uniquement après avoir appliqué un filtre.</i>
Flag	Indique les mesures prises sur l'adresse IP cible. Par exemple, si un indicateur est affiché, l'adresse IP cible est marquée pour le suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Destination IP	Indique l'adresse IP de la destination. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Magnitude	Indique l'importance relative de l'adresse IP cible. La barre d'ampleur fournit une représentation visuelle de la valeur de risque CVSS de l'actif associé à l'adresse IP cible. Déplacez votre souris sur la barre d'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire .
Location	Indique l'emplacement de l'adresse IP cible.
Vulnerability	Indique si l'adresse IP cible dispose de vulnérabilités.
User	Indique le nom d'utilisateur pour cette adresse IP cible. Si aucun utilisateur n'est identifié, cette zone indique Inconnu.
MAC	Indique l'adresse MAC pour cette adresse IP cible. Si aucune adresse MAC n'est identifiée, cette zone indique Inconnu.
Weight	Indique la pondération de l'adresse IP cible. La pondération d'une adresse IP est attribuée à l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions associées à cette adresse IP cible.
Source(s)	Indique le nombre d'adresses IP source associées à cette adresse IP cible.
Last Event/Flow	Indique le temps écoulé depuis le dernier événement ou flux.

Tableau 3-36 Par paramètres de page de détails de destination d'adresse IP (suite)

Paramètre	Description
Events/Flows	Indique le nombre d'événements ou de flux associés à cette adresse IP cible.

Etape 3 Cliquez deux fois sur l'adresse IP cible que vous souhaitez afficher.

REMARQUE

Si vous souhaitez afficher les détails sur une nouvelle page, maintenez la touche de contrôle pendant que vous cliquez deux fois sur l'adresse IP cible que vous souhaitez afficher.

REMARQUE

La partie supérieure de la page affiche le trajet de navigation vers l'affichage en cours. Si vous souhaitez renvoyer à une page déjà affichée, cliquez sur le nom de la page sur le trajet de navigation.

La page de destination fournit les informations suivantes :

Tableau 3-37 Page de destination

Paramètre	Description
Magnitude	Indique l'importance relative des attaques contre l'adresse IP cible. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de l'adresse IP cible. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre d'ampleur pour afficher des valeurs et l'ampleur calculée. <i>Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir le Glossaire.</i>
IP/DNS Name	Indique l'adresse IP de la destination. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Offense(s)	Indique le nom de l'infraction. Vous pouvez cliquer sur le nom pour voir les détails de l'infraction. Si plusieurs infractions sont associées à cette adresse IP cible, cette zone indique Multiple et le nombre d'infractions.
Source(s)	Indique les adresses IP source de l'infraction associée à cette adresse IP cible. Pour afficher des informations supplémentaires sur les adresses IP source, cliquez sur l'adresse IP, le nom de l'actif, ou un terme qui est affiché. Si une adresse IP source est spécifiée, une adresse IP et un nom de l'actif sont affichés (si disponible). Vous pouvez cliquer sur l'adresse IP ou le nom de l'actif pour voir les détails de l'adresse IP source. Si plusieurs adresses IP source existent, cette zone indique Multiple et le nombre d'adresses IP source.

Tableau 3-37 Page de destination (suite)

Paramètre	Description
Event/Flow Count	Indique le nombre total d'événements ou de flux générés associés à cette adresse IP cible.

La barre d'outils de destination fournit les fonctions suivantes :

Tableau 3-38 Cible Barre d'outils

Fonction	Description
Offenses	Cliquez sur Offenses pour afficher la liste des infractions associées à cette adresse IP cible. Voir Etape 4 .
Sources	Cliquez sur Sources pour afficher une liste d'adresses IP source associées à cette adresse IP cible. Voir Etape 5 .
Remarques	Cliquez sur Notes pour afficher toutes les notes pour cette adresse IP cible. Pour plus d'informations à propos des notes, voir Ajout de notes .
Actions	A partir de la zone de liste Actions vous pouvez sélectionner l'une des actions suivantes : <ul style="list-style-type: none"> • Follow up - Sélectionnez cette option pour marquer cette adresse IP cible pour un suivi ultérieur. Voir Marquage d'un article pour suivi. • Notes - Sélectionnez cette option afin d'ajouter des notes pour cette adresse IP cible. Voir Ajout de notes. • Print - Sélectionnez cette option pour imprimer cette adresse IP cible.

Etape 4 Pour afficher une liste d'infractions associées à cette adresse IP cible, cliquez sur **Offenses** sur la barre d'outils de la page de destination.

La liste des infractions fournit les informations suivantes :

Tableau 3-39 Par cible IP - Liste des infractions

Paramètre	Description
Flag	<p>Indique les mesures prises sur l'infraction. Les actions sont représentées par les icônes suivantes :</p> <ul style="list-style-type: none"> • Flag - Indique que l'infraction est marquée pour suivi. Ceci vous permet de contrôler un article particulier pour une investigation complémentaire. Pour plus d'informations sur le marquage d'une infraction pour suivi, voir Marquage d'un article pour suivi. • User - Indique que l'infraction a été affectée à un utilisateur. Lorsqu'une infraction est affectée à un utilisateur, elle est affichée sur la page My Offenses de cet utilisateur. Pour plus d'informations sur l'affectation des infractions aux utilisateurs, voir Affectation des infractions aux utilisateurs. • Notes - Indique qu'un utilisateur a ajouté des notes à l'infraction. Les notes peuvent inclure toute information que vous souhaitez capturer pour l'infraction. Par exemple, vous pourriez ajouter une note qui indique une information qui n'est pas automatiquement incluse dans une infraction, comme un numéro de ticket de service clients ou d'information de gestion d'infraction. Pour plus d'informations sur l'ajout des notes, voir Ajout de notes. • Protected - Indique que cette infraction est protégée. La fonction Protect évite que les infractions spécifiées soient retirées de la base de données après que la période de conservation se soit écoulée. Pour plus d'informations sur les infractions protégées, voir Protection des infractions. • Inactive Offense - Indique qu'il s'agit d'une infraction inactive. Une infraction devient inactive au bout de cinq jours après que l'infraction ait reçu le dernier événement. En outre, toutes les infractions deviennent inactives après la mise à niveau de votre logiciel QRadar Network Anomaly Detection. <p>Une infraction inactive ne peut pas redevenir active. Si de nouveaux événements sont détectés pour l'infraction, une nouvelle infraction est créée et l'infraction inactive est conservée jusqu'à ce que la durée de conservation de l'infraction soit écoulée. Vous pouvez effectuer les actions suivantes sur les infractions inactives: protéger, indiquer pour suivi, ajouter des notes, et affecter aux utilisateurs.</p> <p>Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.</p>
ID	Indique l'identificateur QRadar pour cette infraction.
Description	Indique la description de cette infraction.
Offense Type	Indique le type d'infraction. Le type d'infraction est déterminé par la règle qui a créé l'infraction. Par exemple, si le type d'infraction est l'événement source du journal, la règle qui a généré cette infraction est corrélée aux événements en fonction du périphérique qui a détecté l'événement.

Tableau 3-39 Par cible IP - Liste des infractions (suite)

Paramètre	Description
Offense Source	Indique des informations sur la source de l'infraction. L'information qui s'affiche dans la zone Offense Source dépend du type d'infraction. Par exemple, si le type d'infraction est Source Port, la zone Offense Source affiche le port source de l'événement qui a créé cette infraction.
Magnitude	Indique l'importance relative de l'infraction. La barre d'ampleur offre une représentation visuelle de toutes les variables corrélées des événements et des flux pour cette infraction. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. <i>Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir the Glossaire.</i>
Source IPs	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Destination IPs	Indique les adresses IP et les noms de l'actif (si disponibles) de la destination associée à cette infraction. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Users	Indique les utilisateurs associés à cette infraction. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
Log Sources	Indique les sources de journal associées à cette infraction.
Events	Indique le nombre d'événements associés à cette infraction.
Flows	Indique le nombre de flux associés à cette infraction.
Start Date	Indique la date et l'heure de la première occurrence de cette infraction.
Last Event/Flow	Indique la date et l'heure de la détection de cet événement pour cette infraction.

La liste de la barre d'outils des infractions fournit les fonctions suivantes :

Tableau 3-40 Par cible IP - Barre d'outils de la liste des infractions

Fonction	Description
Sources	Cliquez sur Sources pour afficher une liste d'adresses IP source pour l'infraction sélectionnée. Pour plus d'informations, voir Affichage des infractions par source IP .

Tableau 3-40 Par cible IP - Barre d'outils de la liste des infractions (suite)

Fonction	Description
Destinations	Cliquez sur Destinations pour afficher les adresses IP cible locales ou distantes pour cette infraction. Pour plus d'informations sur les adresses IP cible, voir Affichage des infractions par cible IP .
Categories	<p>Cliquez sur Categories pour afficher des informations de catégorie pour cette infraction, y compris :</p> <p>Remarque : Vous pouvez également étudier davantage les événements relatifs à une catégorie spécifique en cliquant avec le bouton droit sur une catégorie et en sélectionnant Events.</p> <ul style="list-style-type: none"> • Name - Indique le nom de la catégorie associée à cette infraction. • Magnitude - Indique l'importance relative de la catégorie. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de la catégorie. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs pour la catégorie et l'ampleur calculée. Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire. • Local Destination Count - Indique le nombre d'adresses IP cible associées à cette catégorie. • Events/Flows - Indique le nombre d'événements ou de flux associés à cette catégorie. • First Event/Flow - Indique la date du premier événement ou flux. • Last Event/Flow - Indique la date du dernier événement ou flux. <p>Pour plus d'informations sur les catégories, voir Affichage des infractions par catégorie.</p>
Annotations	<p>Cliquez sur Annotations pour afficher toutes les notes explicatives pour cette infraction, y compris :</p> <ul style="list-style-type: none"> • Annotation - Indique les détails de cette annotation. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux infractions comme composant de la réponse de la règle. Pour plus d'informations sur les règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>. • Time - Indique la date et l'heure de cette annotation. • Weight - Indique la pondération de cette annotation.

Tableau 3-40 Par cible IP - Barre d'outils de la liste des infractions (suite)

Fonction	Description
Networks	<p>Cliquez sur Networks pour afficher tous les réseaux de destination pour cette infraction, y compris :</p> <ul style="list-style-type: none"> • Flag - Indique l'action menée sur le réseau. Par exemple, si un indicateur s'affiche, le réseau est marqué pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires. • Network - Indique le nom du réseau de destination. • Magnitude - Indique l'importance relative du réseau de destination. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS des actifs associés au réseau de destination. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire. • Source IPs - Indique le nombre d'adresses IP source associées à ce réseau. • Destination IPs - Indique le nombre d'adresses IP cible associées à ce réseau. • Offenses Targeted - Indique le nombre d'infractions ciblées sur ce réseau. • Offenses Launched - Indique le nombre d'infractions lancées par ce réseau. • Events/Flows - Indique le nombre d'événements ou de flux associés à ce réseau.
Actions	<p>A partir de la zone de liste Actions vous pouvez sélectionner l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Hide - Sélectionnez cette option pour masquer cette infraction. Pour plus d'informations sur le masquage des infractions, voir Masquage des infractions. • Show - Sélectionnez cette option pour afficher toutes les infractions masquées. Pour plus d'informations sur l'affichage des infractions, voir Affichage des infractions masquées. • Close - Sélectionnez cette option pour fermer une infraction. Pour plus d'informations sur la fermeture des infractions, voir Fermeture d'une infraction. • Close Listed - Sélectionnez cette option pour fermer l'infraction listée. Pour plus d'informations sur la fermeture des infractions listées, voir Fermeture des infractions listées.

Etape 5 Pour afficher une liste d'adresses IP source associées à cette adresse IP cible, cliquez sur **Sources** sur la barre d'outils de la page de destination.

La liste de sources fournit les informations suivantes :

Tableau 3-41 Par cible IP - Liste des sources

Paramètre	Description
Flag	Indique l'action menée sur l'adresse IP source. Par exemple, si un indicateur s'affiche, l'adresse IP source est marquée pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Source IP	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Magnitude	Indique l'importance relative de cette adresse IP source. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de l'adresse IP source. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire .
Location	Indique l'emplacement de l'adresse IP source.
Vulnerability	Indique si cette adresse IP source dispose de vulnérabilités.
User	Indique le nom d'utilisateur de l'adresse IP source. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
MAC	Indique l'adresse MAC de l'adresse IP source. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown.
Weight	Indique la pondération de cette adresse IP source. La pondération d'une adresse IP est affectée sur l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions associées à cette adresse IP source.
Destination(s)	Indique le nombre des adresses IP cible associées à cette adresse IP source.
Last Event/Flow	Indique le temps écoulé depuis le dernier événement ou flux.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette adresse IP source.

La liste de la barre d'outils des sources fournit les fonctions suivantes :

Tableau 3-42 Par cible IP - Barre d'outils de la liste des sources

Fonction	Description
Destinations	Cliquez sur Destinations pour afficher des adresses IP cible locales ou distantes pour cette adresse IP source. Pour plus d'informations sur les adresses IP cible, voir Affichage des infractions par cible IP .

Tableau 3-42 Par cible IP - Barre d'outils de la liste des sources (suite)

Fonction	Description
Offenses	Cliquez sur Offenses pour afficher une liste d'infractions pour cette adresse IP source. Pour plus d'informations, voir Gestion des infractions .

Affichage des infractions par réseau

Vous pouvez afficher la liste des infractions regroupées par réseau. Tous les réseaux sont listés en premier en fonction de la plus grande ampleur.

Pour afficher les infractions par réseau :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Sur le menu de navigation, cliquez sur **By Network**.

La page By Network fournit les informations suivantes :

Tableau 3-43 Paramètres de page des détails par réseau

Paramètre	Description
Flag	Indique l'action menée sur le réseau. Par exemple, si un indicateur s'affiche, le réseau est marqué pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Name	Indique le nom du réseau.
Magnitude	Indique l'importance relative du réseau. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées du réseau. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. <i>Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire.</i>
Source IPs	Indique le nombre d'adresses IP source associées à ce réseau.
Destination IPs	Indique le nombre d'adresses IP cible associées à ce réseau.
Offenses Targeted	Indique le nombre d'infractions visées par ce réseau.
Offenses Launched	Indique le nombre d'infractions originaires de ce réseau.
Events/Flows	Indique le nombre d'événements ou de flux associés à ce réseau.

Etape 3 Cliquez deux fois sur le réseau que vous souhaitez afficher.

REMARQUE

Si vous souhaitez afficher les détails sur une nouvelle page, maintenez la touche de contrôle pendant que vous cliquez deux fois sur le réseau que vous souhaitez afficher.

REMARQUE

La partie supérieure de la page affiche le trajet de navigation vers l'affichage en cours. Si vous souhaitez renvoyer à une page déjà affichée, cliquez sur le nom de la page sur le trajet de navigation.

La page de réseau fournit les informations suivantes :

Tableau 3-44 Paramètres de page de réseau

Paramètre	Description
Magnitude	Indique l'importance relative du réseau. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées du réseau. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. <i>Remarque</i> : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire .
Network	Indique l'adresse IP ou le nom du réseau.
Offense(s) Launched	Indique les infractions lancées à partir du réseau. Si plusieurs infractions sont responsables, cette zone indique Multiple et le nombre d'infractions.
Offense(s) Targeted	Indique les infractions visées par le réseau. Si plusieurs infractions sont responsables, cette zone indique Multiple et le nombre d'infractions.
Source(s)	Indique les adresses IP source associées à ce réseau. Pour afficher des informations supplémentaires sur les adresses IP source, cliquez sur l'adresse IP, le nom de l'actif, ou un terme qui est affiché. Si plusieurs adresses IP source existent, cette zone indique Multiple et le nombre d'adresses IP source. Cliquez sur Multiple (n) pour afficher un tableau d'adresses IP sources dans le bas de la page.
Event/Flow Count	Indique le nombre total d'événements ou de flux générés pour ce réseau.

La barre d'outils de réseau fournit les fonctions suivantes :

Tableau 3-45 Barre d'outils de la page de réseau

Fonction	Description
Sources	Cliquez sur Sources pour afficher une liste d'adresses IP source associées à ce réseau. Voir Etape 4 .
Destinations	Cliquez sur Destinations pour afficher une liste d'adresses IP cible associées à ce réseau. Voir Etape 5 .
Offenses	Cliquez sur Offenses pour afficher la liste des infractions associées à ce réseau. Voir Etape 6 .
Remarques	Cliquez sur Notes pour afficher toutes les notes pour ce réseau. Pour plus d'informations sur les notes, voir Ajout de notes .

Tableau 3-45 Barre d'outils de la page de réseau (suite)

Fonction	Description
Actions	<p>A partir de la zone de liste Actions vous pouvez sélectionner l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Follow up - Sélectionnez cette option pour marquer ce réseau pour un suivi ultérieur. Voir Marquage d'un article pour suivi. • Add Note - Sélectionnez cette option pour ajouter des notes au réseau. Voir Ajout de notes. • Print - Sélectionnez cette option pour imprimer cette liste des infractions de réseau.

Etape 4 Pour afficher une liste d'adresses IP source associées à ce réseau, cliquez sur **Sources** sur la barre d'outils de la page réseau.

La liste de sources fournit les informations suivantes :

Tableau 3-46 Par réseau - Liste des sources

Paramètre	Description
Flag	Indique l'action menée sur l'adresse IP source. Par exemple, si un indicateur s'affiche, l'adresse IP source est marquée pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Source IP	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Magnitude	Indique l'importance relative de cette adresse IP source. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de l'adresse IP source. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire .
Location	Indique l'emplacement de l'adresse IP source.
Vulnerability	Indique si cette adresse IP source dispose de vulnérabilités.
User	Indique le nom d'utilisateur de l'adresse IP source. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
MAC	Indique l'adresse MAC de l'adresse IP source. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown.
Weight	Indique la pondération de cette adresse IP source. La pondération d'une adresse IP est affectée sur l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions associées à cette adresse IP source.

Tableau 3-46 Par réseau - Liste des sources (suite)

Paramètre	Description
Destination(s)	Indique le nombre des adresses IP cible associées à cette adresse IP source.
Last Event/Flow	Indique le temps écoulé depuis le dernier événement ou flux.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette adresse IP source.

La liste de la barre d'outils des sources fournit les fonctions suivantes :

Tableau 3-47 Par réseau - Barre d'outils de la liste des sources

Fonction	Description
Destinations	Cliquez sur Destinations pour afficher les adresses IP cible locales ou distantes. Pour plus d'informations sur les adresses IP cible, voir Affichage des infractions par cible IP .
Offenses	Cliquez sur Offenses pour afficher les infractions associées à cette adresse IP source. Pour plus d'informations sur les infractions, voir Gestion des infractions .

Etape 5 Pour afficher une liste des adresses IP cible associées à ce réseau, cliquez sur **Destinations** sur la barre d'outils de la page réseau.

La liste des destinations locales fournit les informations suivantes :

Tableau 3-48 Par réseau - Paramètres de la liste des destinations locales

Paramètre	Description
Flag	Indique les mesures prises sur l'adresse IP cible. Par exemple, si un indicateur est affiché, l'adresse IP cible est marquée pour le suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Destination IP	Indique l'adresse IP de la destination. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Magnitude	Indique l'importance relative de cette adresse IP cible. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de l'adresse IP cible. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire .
Location	Indique l'emplacement de l'adresse IP cible.
Vulnerability	Indique si cette adresse IP cible dispose de vulnérabilités.
User	Indique le nom d'utilisateur de l'adresse IP cible. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
MAC	Indique l'adresse MAC de l'adresse IP cible. Si aucune adresse MAC n'est identifiée, cette zone indique Inconnu.
Weight	Indique la pondération de cette adresse IP cible. La pondération d'une adresse IP est attribuée à l'onglet Assets . Pour plus d'informations, voir Gestion des actifs .
Offenses	Indique le nombre d'infractions associées à cette adresse IP cible.
Source(s)	Indique le nombre d'adresses IP source associées à cette adresse IP cible.

Tableau 3-48 Par réseau - Paramètres de la liste des destinations locales (suite)

Paramètre	Description
Last Event/Flow	Indique le temps écoulé depuis le dernier événement ou flux.
Events/Flows	Indique le nombre d'événements ou de flux associés à cette adresse IP cible.

La liste de la barre d'outils des destinations locales fournit les fonctions suivantes :

Tableau 3-49 Barre d'outils de la liste des destinations locales

Fonction	Description
Offenses	Cliquez sur Offenses pour afficher une liste des infractions pour cette adresse IP cible. Voir Etape 6 .
Sources	Cliquez sur Sources pour afficher une liste d'adresses IP source. Pour plus d'informations, voir Affichage des infractions par source IP .
Search	<p>Cliquez sur Search pour rechercher les adresses IP cible de ce réseau. Pour rechercher des adresses IP cible :</p> <ol style="list-style-type: none"> 1 Cliquez sur Search. 2 Entrez des valeurs pour les paramètres : <ul style="list-style-type: none"> Destination Network - Dans la zone de liste, sélectionnez le réseau que vous souhaitez rechercher. Magnitude - Dans la zone de liste, sélectionnez si vous souhaitez rechercher l'ampleur Égale à, Inférieure à, ou supérieure à la valeur configurée. Sort by - Dans la zone de liste et les options, sélectionnez comment vous souhaitez trier les résultats de la recherche. 3 Cliquez sur Search.

Etape 6 Pour afficher une liste des infractions associées à ce réseau, cliquez sur **Offenses** sur la barre d'outils de la page réseau.

La liste des infractions fournit les informations suivantes :

Tableau 3-50 Par réseau - Paramètres de la liste des infractions

Paramètre	Description
Flag	<p>Indique les mesures prises sur l'infraction. Les actions sont représentées par les icônes suivantes :</p> <ul style="list-style-type: none"> • Flag - Indique que l'infraction est marquée pour suivi. Ceci vous permet de contrôler un article particulier pour une investigation complémentaire. Pour plus d'informations sur le marquage d'une infraction pour suivi, voir Marquage d'un article pour suivi. • User - Indique que l'infraction a été affectée à un utilisateur. Lorsqu'une infraction est affectée à un utilisateur, elle est affichée sur la page My Offenses de cet utilisateur. Pour plus d'informations sur l'affectation des infractions aux utilisateurs, voir Affectation des infractions aux utilisateurs. • Notes - Indique qu'un utilisateur a ajouté des notes à l'infraction. Les notes peuvent inclure toute information que vous souhaitez capturer pour l'infraction. Par exemple, vous pourriez ajouter une note qui indique une information qui n'est pas automatiquement incluse dans une infraction, comme un numéro de ticket de service clients ou d'information de gestion d'infraction. Pour plus d'informations sur l'ajout des notes, voir Ajout de notes. • Protected - Indique que cette infraction est protégée. La fonction Protect évite que les infractions spécifiées soient retirées de la base de données après que la période de conservation se soit écoulée. Pour plus d'informations sur les infractions protégées, voir, Protection des infractions. • Inactive Offense - Indique qu'il s'agit d'une infraction inactive. Une infraction devient inactive au bout de cinq jours après que l'infraction ait reçu le dernier événement. En outre, toutes les infractions deviennent inactives après la mise à niveau de votre logiciel QRadar Network Anomaly Detection. Une infraction inactive ne peut pas redevenir active. Si de nouveaux événements sont détectés pour l'infraction, une nouvelle infraction est créée et l'infraction inactive est conservée jusqu'à ce que la durée de conservation de l'infraction soit écoulée. Vous pouvez effectuer les actions suivantes sur les infractions inactives: protéger, indiquer pour suivi, ajouter des notes, et affecter aux utilisateurs. <p>Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.</p>
ID	Indique l'identificateur QRadar pour cette infraction.
Description	Indique la description de cette infraction.
Offense Type	Indique le type d'infraction. Le type d'infraction est déterminé par la règle qui a créé l'infraction. Par exemple, si le type d'infraction est l'événement source du journal, la règle qui a généré cette infraction est corrélée aux événements en fonction du périphérique qui a détecté l'événement.

Tableau 3-50 Par réseau - Paramètres de la liste des infractions (suite)

Paramètre	Description
Offense Source	Indique des informations sur la source de l'infraction. L'information qui s'affiche dans la zone Offense Source dépend du type d'infraction. Par exemple, si le type d'infraction est Source Port, la zone Offense Source affiche le port source de l'événement qui a créé cette infraction.
Magnitude	Indique l'importance relative de l'infraction. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de l'infraction, de la source, de la destination ou du réseau. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. <i>Remarque : Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire.</i>
Source IPs	Indique l'adresse IP ou le nom d'hôte du périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Destination IPs	Indique les adresses IP et les noms de l'actif (si disponibles) de l'adresse IP cible associée à cette infraction. Si les consultations du serveur de noms de domaine sont activées sur l'onglet Admin , vous pouvez afficher le nom du serveur de noms de domaine en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Users	Indique les utilisateurs associés à cette infraction. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
Log Sources	Indique les sources de journal associées à cette infraction.
Events	Indique le nombre d'événements associés à cette infraction.
Flows	Indique le nombre de flux associés à cette infraction.
Start Date	Indique la date et l'heure de la première occurrence de cette infraction.
Last Event/Flow	Indique la date et l'heure où cet événement ou flux a été détecté pour cette infraction.

La liste de la barre d'outils des infractions fournit les fonctions suivantes :

Tableau 3-51 Par réseau - Barre d'outils de la liste des infractions

Fonction	Description
Sources	Cliquez sur Sources pour afficher une liste d'adresses IP source pour l'infraction sélectionnée. Pour plus d'informations, voir Affichage des infractions par source IP .

Tableau 3-51 Par réseau - Barre d'outils de la liste des infractions (suite)

Fonction	Description
Destinations	Cliquez sur Destinations pour afficher les adresses IP cible locales ou distantes pour l'infraction sélectionnée. Pour plus d'informations sur les adresses IP cible, voir Affichage des infractions par cible IP .
Categories	<p>Cliquez sur Categories pour afficher des informations de catégorie pour l'infraction sélectionnée, y compris :</p> <p>Remarque : <i>Vous pouvez également étudier davantage les événements relatifs à une catégorie spécifique en cliquant avec le bouton droit sur une catégorie et en sélectionnant Events.</i></p> <ul style="list-style-type: none"> • Name - Indique le nom de la catégorie associée à cette infraction. • Magnitude - Indique l'importance relative de la catégorie. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées de la catégorie. Les variables incluent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs pour la catégorie et l'ampleur calculée. Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir Glossaire. • Local Destination Count - Indique le nombre d'adresses IP cible associées à cette catégorie. • Events/Flows - Indique le nombre d'événements ou de flux associés à cette catégorie. • First Event/Flow - Indique le temps écoulé depuis le premier événement ou flux. • Last Event/Flow - Indique le temps écoulé depuis le dernier événement ou flux. <p>Pour plus d'informations sur les catégories, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>.</p>
Annotations	<p>Cliquez sur Annotations pour afficher toutes les notes explicatives pour l'infraction sélectionnée, y compris :</p> <ul style="list-style-type: none"> • Annotation - Indique les détails de cette annotation. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux infractions comme composant de la réponse de la règle. Pour plus d'informations sur les règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>. • Time - Indique la date et l'heure de cette annotation. • Weight - Indique la pondération de cette annotation.

Tableau 3-51 Par réseau - Barre d'outils de la liste des infractions (suite)

Fonction	Description
Networks	<p data-bbox="638 352 1430 411">Cliquez sur Networks pour afficher tous les réseaux de destination pour cette infraction, y compris :</p> <ul data-bbox="638 426 1469 1102" style="list-style-type: none"> <li data-bbox="638 426 1469 512">• Flag - Indique l'action menée sur le réseau. Par exemple, si un indicateur s'affiche, le réseau est marqué pour suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires. <li data-bbox="638 527 1279 554">• Network - Indique le nom du réseau de destination. <li data-bbox="638 569 1469 741">• Magnitude - Indique l'importance relative du réseau de destination. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS des actifs associés au réseau de destination. Déplacez votre souris sur la barre de l'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir Glossaire. <li data-bbox="638 756 1446 814">• Source IPs - Indique le nombre d'adresses IP source associées à ce réseau. <li data-bbox="638 829 1373 888">• IP de destination - Indique le nombre d'adresses IP source associées à ce réseau. <li data-bbox="638 903 1458 961">• Offenses Targeted - Indique le nombre d'infractions ciblées sur ce réseau. <li data-bbox="638 976 1446 1035">• Offenses Launched - Indique le nombre d'infractions lancées par ce réseau. <li data-bbox="638 1050 1373 1102">• Events/Flows - Indique le nombre d'événements ou de flux associés à ce réseau.
Actions	<p data-bbox="638 1117 1469 1176">A partir de la zone de liste Actions vous pouvez sélectionner l'une des actions suivantes :</p> <ul data-bbox="638 1190 1469 1579" style="list-style-type: none"> <li data-bbox="638 1190 1469 1276">• Hide - Sélectionnez cette option pour masquer cette infraction. Pour plus d'informations sur le masquage des infractions, voir Masquage des infractions. <li data-bbox="638 1291 1469 1377">• Show - Sélectionnez cette option pour afficher toutes les infractions masquées. Pour plus d'informations sur l'affichage des infractions masquées, voir Affichage des infractions masquées. <li data-bbox="638 1392 1469 1478">• Close - Sélectionnez cette option pour fermer une infraction. Pour plus d'informations sur la fermeture des infractions, voir Fermeture d'une infraction. <li data-bbox="638 1493 1469 1579">• Close Listed - Sélectionnez cette option pour fermer l'infraction listée. Pour plus d'informations sur la fermeture des infractions listées, voir Fermeture des infractions listées.

4

ENQUÊTE D'ÉVÉNEMENTS

A l'aide de l'onglet **Log Activity**, vous pouvez surveiller et enquêter sur l'activité de journal (événements) en temps réel ou effectuer des recherches avancées.

Cette section comprend les rubriques suivantes :

- [Présentation de l'onglet Activity](#)
- [Utilisation de l'onglet Log Activity](#)
- [Affichage des événements](#)
- [Affichage des violations associées](#)
- [Modification d'un mappage d'événement](#)
- [Utilisation de la fonction Custom Event Properties](#)
- [Réglage des faux positifs](#)
- [Gestion des données PCAP](#)
- [Exportation des événements](#)

Présentation de l'onglet Activity

Vous devez avoir le droit d'afficher l'onglet **Log Activity**. Pour plus d'informations sur les permissions et l'affectation de rôles, voir le *Guide d'administration IBM Security QRadar Network Anomaly Detection*.

Un événement est un enregistrement d'une source de journal, par exemple un périphérique pare-feu ou un routeur, qui décrit une action sur un réseau ou un hôte. L'onglet **Log Activity** spécifie les événements qui sont associés aux violations. Vous pouvez utiliser l'onglet **Log Activity** afin de :

- Rechercher les événements (voir [Recherche de données](#))
- Enregistrer et gérer les résultats et les critères de recherche
- Afficher les événements en temps réel (en continu)
- Afficher les informations d'événements regroupés par diverses options
- Créer, afficher et enquêter sur les graphiques de série temporelle
- Afficher et gérer les données de Capture de paquets (PCAP)
- Associer ou mapper un événement inconnu à une catégorie de haut et de bas niveau (ou QRadar Identifiant (QID))

- Ajustez les événements faux positifs à partir de la génération des violations
- Exporter les événements au format Extensible Markup Language (XML) ou Comma-Separated Value (CSV)

QRadar Network Anomaly Detection normalise les événements à afficher sur l'onglet **Log Activity**. La normalisation implique l'analyse des données de l'événement brut et la préparation des données pour afficher des informations lisibles sur l'onglet. Lorsque QRadar Network Anomaly Detection normalise les événements, le système normalise également les noms. Par conséquent, le nom qui s'affiche sur l'onglet **Log Activity** peut ne pas correspondre au nom qui s'affiche dans l'événement.

Utilisation de l'onglet Log Activity

Si vous avez configuré les critères de recherche par défaut, les résultats de cette recherche sont affichés automatiquement lorsque vous accédez à l'onglet **Log Activity**. Pour plus d'informations sur l'enregistrement du critère, voir [Sauvegarde des critères de recherche](#).

Cette section comprend les rubriques suivantes :

- [Utilisation de la barre d'outils](#)
- [Utilisation des options du menu contextuel](#)
- [Utilisation de la barre d'état](#)

Utilisation de la barre d'outils

A l'aide de la barre d'outils, vous pouvez accéder aux options suivantes :

Tableau 4-1 Options de la barre d'outils de l'onglet Log Activity

Option	Description
Search	<p>Cliquez sur Search pour effectuer des recherches avancées sur les événements. Les options incluent :</p> <ul style="list-style-type: none"> • New Search - Sélectionnez cette option pour créer une nouvelle recherche d'événement. • Edit Search - Sélectionnez cette option pour sélectionner et modifier une recherche d'événement. • Manage Search Results - Sélectionnez cette option pour afficher et gérer les résultats de la recherche. Voir Gestion des résultats de recherche <p>Pour plus d'informations sur la fonctionnalité de recherche, voir Recherche de données.</p>
Quick Searches	<p>Dans cette zone de liste, vous pouvez exécuter des recherches précédemment enregistrées. Les options sont uniquement affichées dans la zone de liste Quick Searches lorsque vous avez enregistré les critères de recherche qui spécifient l'option Include in my Quick Searches.</p>
Add Filter	<p>Cliquez sur Add Filter pour ajouter un filtre pour les résultats de la recherche actuelle.</p>

Tableau 4-1 Options de la barre d'outils de l'onglet Log Activity (suite)

Option	Description
Save Criteria	Cliquez sur Save Criteria pour enregistrer les critères de la recherche actuelle.
Save Results	Cliquez sur Save Results pour enregistrer les résultats de la recherche actuelle. Cette option s'affiche uniquement à la fin d'une recherche. En mode de transmission en continu, cette option est désactivée.
Cancel	Cliquez sur Cancel pour annuler une recherche en cours. En mode de transmission en continu cette option est désactivée.
False Positive	Cliquez sur False Positive pour ouvrir la fenêtre False Positive Tuning, qui vous permet d'accorder les événements qui sont connus pour être des faux positifs de la création des violations. Pour plus d'informations sur les faux positifs, voir Glossaire . En mode de transmission en continu, cette option est désactivée. Pour plus d'informations sur le réglage des faux positifs, voir Réglage des faux positifs .

Tableau 4-1 Options de la barre d'outils de l'onglet Log Activity (suite)

Option	Description
Rules	<p data-bbox="680 338 1360 396">Cliquez sur Rules pour configurer les règles d'événement personnalisé. Les options incluent :</p> <ul data-bbox="680 411 1456 527" style="list-style-type: none"> <li data-bbox="680 411 1456 527">• Rules - Sélectionnez cette option pour créer une règle. Lorsque vous sélectionnez l'option Rule, l'Assistant des règles s'affiche, prérempli avec les options appropriées pour la création d'une règle d'événement. <p data-bbox="680 541 1456 695">Remarque : Pour activer les options de règle de détection des anomalies (<i>Add Threshold Rule, Add Behavioral Rule et Add Anomaly Rule</i>), vous devez enregistrer les critères de recherche regroupés parce que les critères de recherche enregistrés spécifient les paramètres requis.</p> <ul data-bbox="680 709 1456 972" style="list-style-type: none"> <li data-bbox="680 709 1456 972">• Add Threshold Rule - Sélectionnez cette option pour créer une règle de seuil. Une règle de seuil teste le trafic d'événement de l'activité qui excède un seuil configuré. Les seuils peuvent être basés sur des données recueillies par QRadar Network Anomaly Detection. Par exemple, si vous créez une règle de seuil indiquant que pas plus de 220 clients peuvent se connecter au serveur entre 08 et 17 heures, les règles génèrent une alerte lorsque le 221^{ème} client tente de se connecter. <p data-bbox="711 987 1390 1073">Lorsque vous sélectionnez l'option Add Threshold Rule, l'Assistant des règles s'affiche, prérempli avec les options appropriées pour la création d'une règle de seuil.</p> <ul data-bbox="680 1087 1456 1409" style="list-style-type: none"> <li data-bbox="680 1087 1456 1409">• Add Behavioral Rule - Sélectionnez cette option pour créer une règle comportementale. Une règle comportementale teste le trafic d'événement pour une activité anormale, telle que l'existence d'un trafic nouveau ou inconnu, qui est un trafic qui cesse soudainement ou un changement en pourcentage de la quantité de temps où un objet est actif. Par exemple, vous pouvez créer une règle comportementale pour comparer le volume moyen du trafic pour les 5 dernières minutes par rapport au volume moyen du trafic au cours de la dernière heure. S'il existe plus d'un changement de 40%, la règle génère une réponse. <p data-bbox="711 1423 1403 1509">Lorsque vous sélectionnez l'option Add Behavioral Rule, l'Assistant des règles s'affiche, prérempli avec les options appropriées pour la création d'une règle comportementale.</p>

Tableau 4-1 Options de la barre d'outils de l'onglet Log Activity (suite)

Option	Description
	<ul style="list-style-type: none"> • Add Anomaly Rule - Sélectionnez cette option pour créer une règle d'anomalie. Une règle d'anomalie teste le trafic d'événement pour une activité anormale, telle que l'existence d'un trafic nouveau ou inconnu, qui est un trafic qui cesse soudainement ou un changement en pourcentage de la quantité de temps où un objet est actif. Par exemple, si une zone de votre réseau qui ne communique jamais avec l'Asie commence à communiquer avec des hôtes dans ce pays, une règle d'anomalie génère une alerte. <p>Lorsque vous sélectionnez l'option Add Anomaly Rule, l'Assistant des règles s'affiche, prérempli avec les options appropriées pour la création d'une règle d'anomalie.</p> <p>Pour plus d'informations sur les règles, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i>.</p>
Actions	<p>Cliquez sur Actions pour effectuer les actions suivantes :</p> <ul style="list-style-type: none"> • Show All - Sélectionnez cette option pour supprimer tous les filtres sur les critères de recherche et afficher tous les événements non filtrés. • Print - Sélectionnez cette option pour imprimer les événements affichés sur la page. • Export to XML > Visible Columns - Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles dans l'onglet Log Activity. Il s'agit de l'option recommandée. Voir Exportation des événements. • Export to XML > Full Export (All Columns) - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour terminer. Voir Exportation des événements. • Export to CSV > Visible Columns - Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles dans l'onglet Log Activity. Il s'agit de l'option recommandée. Voir Exportation des événements. • Export to CSV > Full Export (All Columns) - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour terminer. Voir Exportation des événements. • Delete - Sélectionnez cette option pour supprimer un résultat de la recherche. Voir Suppression d'une recherche. • Notify - Sélectionnez cette option pour spécifier que vous souhaitez recevoir une notification par courriel à l'issue de la recherche sélectionnée. Cette option est activée uniquement pour les recherches en cours. <p>Remarque : Les options Print, Export to XML et Export to CSV sont désactivées en mode de transmission en continu et lors de l'affichage des résultats de la recherche partielle.</p>

Tableau 4-1 Options de la barre d'outils de l'onglet Log Activity (suite)

Option	Description
Quick Filter	<p>Entrez vos critères de recherche dans la zone Quick Filter et cliquez sur l'icône Quick Filter ou appuyez sur la touche Enter sur le clavier. Tous les événements qui correspondent à vos critères de recherche sont affichés dans la liste des événements. Une recherche de texte est exécutée sur le contenu d'événement pour déterminer lequel correspond à vos critères spécifiés.</p> <p>Remarque : Lorsque vous cliquez sur la zone Quick Filter, une info-bulle s'affiche, fournissant des informations sur la syntaxe à utiliser pour les critères de recherche. Pour plus d'informations sur la syntaxe, voir Utilisation de la syntaxe Quick Filter.</p>

Utilisation de la syntaxe Quick Filter

La fonction Quick Filter permet de rechercher des contenus d'événement à l'aide d'une chaîne de recherche de texte. La fonction Quick Filter est disponible dans les emplacements suivants sur l'interface utilisateur :

- **Log Activity toolbar** - Sur la barre d'outils, la zone **Quick Filter** vous permet de saisir une chaîne de recherche de texte et cliquer sur l'icône **Quick Filter** pour appliquer votre filtre rapide à la liste affichée des événements.
- **Add Filter dialog box** - A partir de la boîte de dialogue **Add Filter**, accessible en cliquant sur l'icône **Add Filter** sur l'onglet **Log Activity**, vous pouvez sélectionner **Quick Filter** en tant que votre paramètre filtre et taper une ligne de recherche de texte. Cela vous permet d'appliquer votre filtre rapide à la liste affichée des événements ou des flux. Pour plus d'informations sur la boîte de dialogue Add Filter, voir [Performing a Sub-Search](#).
- **Event and Flow search pages** - A partir des pages de recherche de flux et d'événements, vous pouvez ajouter un filtre rapide à votre liste de filtres à inclure dans vos critères de recherche. Pour plus d'informations sur la configuration du critère de recherche, voir [Effectuer une sous-recherche](#).

Lorsque vous affichez des événements en temps réel (en continu) ou en mode dernière plage, vous pouvez taper uniquement des mots simples ou des phrases dans la zone **Quick Filter**. Lorsque vous affichez des événements à l'aide d'une plage de temps, suivez les instructions de syntaxe ci-dessous pour taper vos critères de recherche de texte :

- Les termes de recherche peuvent inclure n'importe quel texte brut que vous vous attendez à trouver dans le contenu. Par exemple, `Firewall`
- Incluez plusieurs termes entre guillemets doubles pour indiquer que vous souhaitez rechercher l'expression exacte. Pour exemple, `"Firewall deny"`
- Les termes de recherche peuvent inclure des caractères génériques et des caractères simples ou multiples. Le terme de recherche ne peut pas commencer par un caractère générique. Par exemple, `F?rwall` ou `F??ew*`

- Conditions de groupe à l'aide d'expressions logiques, telles que AND, OR, et NOT. La syntaxe est sensible à la casse et les opérateurs doivent être en majuscules pour être reconnus comme des expressions logiques et non comme termes de recherche. Par exemple : (%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)
Lors de la création d'un critère de recherche qui comprend l'expression logique NOT, vous devez inclure au moins un autre type d'expression logique ; dans le cas contraire, votre filtre ne retournera aucun résultat. Par exemple : (%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)
- Les caractères suivants doivent être précédés d'une barre oblique inverse pour indiquer que le personnage fait partie de votre terme de recherche : + - & | ! () { } [] ^ " ~ * ? : \. Par exemple : "%PIX\ -5\ -304001"

Utilisation des options du menu contextuel

Sur l'onglet **Log Activity**, vous pouvez cliquer avec le bouton droit de la souris sur un événement pour accéder aux informations supplémentaires de filtre d'événement.

Les options du menu contextuel sont :

Tableau 4-2 Options du menu contextuel

Option	Description
Filter on	Sélectionnez cette option pour filtrer sur l'événement sélectionné, selon le paramètre sélectionné à cet événement.
False Positive	Sélectionnez cette option afin d'ouvrir la fenêtre False Positive Tuning, qui vous permet d'ajuster les événements connus pour être des faux positifs à partir de la création des violations. En mode de transmission en continu, cette option est désactivée. Voir Réglage des faux positifs .
More options:	Sélectionnez cette option pour examiner une adresse IP ou un nom d'utilisateur. Pour plus d'informations sur l'examen de l'adresse IP, voir Etude des adresses IP . Pour plus d'informations sur l'examen du nom d'utilisateur, voir Etude des noms d'utilisateur . Remarque : Cette option n'est pas affichée en mode de transmission en continu.

Utilisation de la barre d'état

Lors de la diffusion en flux des événements, la barre d'état affiche le nombre moyen des résultats reçus par seconde. C'est le nombre des résultats de que la console a reçu avec succès de Event Processors. Si ce nombre est supérieur à 40 résultats par seconde, seulement 40 résultats s'affichent. Le reste s'accumule dans la mémoire tampon du résultat. Pour afficher les informations d'état supplémentaires, déplacez le pointeur de votre souris sur la barre d'état.

Lorsque QRadar Network Anomaly Detection n'est pas une diffusion en flux des événements, la barre d'état affiche le nombre des résultats de la recherche

actuellement affichés dans l'onglet et le temps requis pour traiter les résultats de la recherche.

Affichage des événements

Par défaut, l'onglet **Log Activity** affiche les événements en mode diffusion en flux, vous permettant d'afficher des événements en temps réel. Pour plus d'informations sur le mode de diffusion en flux, voir [Affichage des événements en continu](#). Vous pouvez spécifier une plage de temps différente pour filtrer les événements à l'aide de la zone de liste **View**.

Vous pouvez afficher les événements à l'aide des options suivantes :

- [Affichage des événements en continu](#)
- [Affichage des événements normalisés](#)
- [Affichage de données d'événements brutes](#)
- [Affichage des événements groupés](#)

Affichage des événements en continu

Mode de transmission en continu vous permet d'afficher les données d'événement entrant dans votre système. Ce mode vous donne une vue en temps réel de votre activité actuelle en affichant les dernière 50 événements.

Si vous appliquez des filtres sur l'onglet **Log Activity** ou dans vos critères de recherche avant d'activer le mode de transmission en continu, les filtres sont maintenus dans le mode de diffusion en continu. Toutefois, le mode de diffusion en continu ne supporte pas les recherches qui incluent des événements groupés. Si vous activez le mode de diffusion en continu sur les événements groupés ou les critères de recherche groupés, l'onglet **Log Activity** affiche les événements normalisés. Voir [Affichage des événements normalisés](#).

Pour afficher les événements en diffusion continu :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez déjà sauvegardé un critère de recherche pour qu'il soit un critère par défaut, les résultats de ce critère de recherche s'affichent.

Etape 2 A partir de zone de liste **View**, sélectionnez **Real Time (diffusion en flux)**.

Les événements en continu sont affichés. Pour plus d'informations sur les options de la barre d'outils, voir [Tableau 4-1](#). Pour plus d'informations sur les paramètres affichés en mode continu, voir [Tableau 4-4](#).

- ▶ Pour sélectionner un enregistrement de l'événement, cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.

Lorsque la diffusion en continu est mise en pause, les derniers 1 000 événements sont affichés.

- ▶ Pour redémarrer le mode de transmission en continu, cliquez sur l'icône **Play**.

Afficher les événements normalisés

Pour afficher les événements normalisés :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats enregistrés pour cette recherche sont affichés.

Etape 2 Depuis la zone de liste **Display**, sélectionnez **Default (Normalized)**.

Etape 3 A partir de la zone de liste **View**, sélectionnez le laps de temps que vous souhaitez afficher.

REMARQUE

Si vous avez sélectionné un cadre de temps à afficher, un graphique de séries temporelles s'affiche. Pour plus d'informations sur l'utilisation des graphiques de série temporelle, voir [Gestion des graphiques de séries temporelles](#).

L'onglet **Log Activity** affiche les paramètres suivants :

Tableau 4-3 Log Activity Tab - Default (Normalized)

Paramètre	Description
Current Filters	La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche. Pour effacer les valeurs de filtre, cliquez sur Clear Filter . <i>Remarque : Ce paramètre ne s'affiche qu'après avoir appliqué un filtre.</i>
View	Dans cette zone de liste, vous pouvez sélectionner la plage de temps que vous souhaitez filtrer.

Tableau 4-3 Log Activity Tab - Default (Normalized) (suite)

Paramètre	Description
Current Statistics	<p>Lorsqu'elles ne sont pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours sont affichées, notamment :</p> <p>Remarque : Cliquez sur la flèche à côté Current Statistics pour afficher ou masquer les statistiques</p> <ul style="list-style-type: none"> • Total Results - Indique le nombre total des résultats correspondant à vos critères de recherche. • Data Files Searched - Indique le nombre total des fichiers de données recherchés au cours de la plage de temps spécifié. • Compressed Data Files Searched - Indique le nombre total de fichiers de données compressées recherchés au cours de la plage de temps spécifiée. • Index File Count - Indique le nombre total de fichiers d'index recherchés au cours de la plage de temps spécifiée. • Duration - Indique la durée de la recherche. <p>Remarque : Les statistiques actuelles sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les événements, vous serez peut-être invité à fournir des informations statistiques actuelles.</p>
Charts	<p>Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'option de regroupement et l'intervalle de temps. Cliquez sur Hide Charts si vous souhaitez retirer les graphiques de votre écran.</p> <p>Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur les graphiques de configuration, voir Configuration des graphiques.</p> <p>Remarque : Si vous utilisez Mozilla Firefox comme navigateur et qu'un bloqueur de publicités est installé, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer le bloqueur de publicités. Pour plus d'informations, voir la documentation de votre navigateur.</p>
Offenses icon	<p>Cliquez sur l'icône Offenses pour afficher les détails de la violation associée à cet événement. Pour plus d'informations, voir Affichage des violations associées.</p>
Event Name	<p>Indique le nom normalisé de l'événement.</p>
Log Source	<p>Indique la source du journal qui a envoyé l'événement à QRadar Network Anomaly Detection. S'il existe plusieurs sources de journal associées à cet événement, cette zone définit le terme Multiple et le nombre de sources du journal.</p>

Tableau 4-3 Log Activity Tab - Default (Normalized) (suite)

Paramètre	Description
Event Count	Indique le nombre total des événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs événements du même type pour la même source et l'adresse IP de destination sont détectés dans un court laps de temps.
Time	Indique la date et le moment où QRadar Network Anomaly Detection a reçu l'événement.
Low Level Category	Indique la catégorie de bas niveau associée à cet événement. Pour plus d'informations sur les catégories d'événements, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Source IP	Indique l'adresse IP source de l'événement.
Source Port	Indique le port source de l'événement.
Destination IP	Indique l'adresse IP cible de l'événement.
Destination Port	Indique le port de destination de l'événement.
Username	Indique le nom d'utilisateur associé à cet événement. Les noms d'utilisateurs sont souvent disponibles dans les événements d'authentification associés. Pour tous les autres types d'événements où le nom d'utilisateur n'est pas disponible, cette zone spécifie N/A.
Magnitude	Indique l'ampleur de cet événement. Les variables comprennent la crédibilité, la pertinence et la gravité. Pointez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'amplitude calculée. Pour plus d'informations sur la crédibilité, la pertinence et la gravité, voir Glossaire .

Etape 4 Cliquez deux fois sur l'événement que vous souhaitez afficher plus en détail.

REMARQUE

Si vous affichez des événements en mode de transmission continu, vous devez mettre en pause ce mode avant de cliquer deux fois sur un événement.

Les résultats de détails d'événements fournissent les informations suivantes :

Tableau 4-4 Détails d'événement

Paramètre	Description
Event Information	
Event Name	Indique le nom normalisé de l'événement.
Low Level Category	Indique la catégorie de bas niveau de cet événement. Pour plus d'informations sur les catégories, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Event Description	Indique une description de l'événement, si disponible.
Magnitude	Indique l'ampleur de cet événement. Pour plus d'informations sur l'ampleur, voir Glossaire .

Tableau 4-4 Détails d'événement (suite)

Paramètre	Description
Relevance	Indique l'importance de cet événement. Pour plus d'informations sur la pertinence, voir Glossaire .
Severity	Indique la gravité de cet événement. Pour plus d'informations sur la gravité, voir le Glossaire .
Credibility	Indique la crédibilité de cet événement. Pour plus d'informations sur la crédibilité, voir le Glossaire .
Username	Indique le nom d'utilisateur associé à cet événement, si disponible.
Start Time	Indique l'heure à laquelle l'événement a été reçu de la source du journal.
Storage Time	Indique l'heure à laquelle l'événement a été stocké dans la base de données QRadar Network Anomaly Detection.
Log Source Time	Indique l'heure du système telle que rapportée par la source du journal à l'événement du contenu.
<p>Anomaly Detection Information - Ce panneau s'affiche uniquement si cet événement a été généré par une règle de détection des anomalies. Pour plus d'informations sur les règles de détection des anomalies, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i>. Cliquez sur l'icône Anomaly pour afficher les résultats de la recherche sauvegardée qui a entraîné la règle de détection des anomalies afin de générer cet événement.</p>	
Rule Description	Indique la règle de détection des anomalies qui a généré cet événement.
Anomaly Description	Indique une description du comportement anormal qui a été détecté par la règle de détection des anomalies.
Anomaly Alert Value	Indique la valeur d'alerte d'anomalie.
Informations sur la source et destination	
Source IP	Indique l'adresse IP source de l'événement.
Destination IP	Indique l'adresse IP cible de l'événement.
Source Asset Name	Indique le nom d'actif de la source de l'événement défini par l'utilisateur. Pour plus d'informations sur les actifs, voir Gestion des actifs .
Destination Asset Name	Indique le nom de l'actif de la destination de l'événement défini par l'utilisateur. Pour plus d'informations sur les actifs, voir Gestion des actifs .
Source Port	Indique le port source de cet événement.
Destination Port	Indique le port de destination de cet événement.
Pre NAT Source IP	Pour un pare-feu ou un autre périphérique capable de traduire des adresses réseau (NAT), ce paramètre définit l'adresse IP source avant l'application des valeurs NAT. NAT traduit l'adresse IP dans un réseau à une adresse IP différente sur un autre réseau.

Tableau 4-4 Détails d'événement (suite)

Paramètre	Description
Pre NAT Destination IP	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP cible avant l'application des valeurs NAT.
Pre NAT Source Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port source avant l'application des valeurs NAT.
Pre NAT Destination Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port de destination avant l'application des valeurs NAT.
Post NAT Source IP	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP source avant l'application des valeurs NAT.
Post NAT Destination IP	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP cible avant l'application des valeurs NAT.
Post NAT Source Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port source avant l'application des valeurs NAT.
Post NAT Destination Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port de destination avant l'application des valeurs NAT.
IPv6 Source	Indique l'adresse IPv6 source de l'événement.
IPv6 Destination	Indique l'adresse IPv6 de destination de l'événement.
Source MAC	Indique l'adresse MAC source de l'événement.
Destination MAC	Indique l'adresse MAC de destination de l'événement.
Information sur Payload	
Payload	Indique le contenu payload de l'événement. Cette zone fournit trois onglets pour afficher le contenu : <ul style="list-style-type: none"> • Universal Transformation Format (UTF) - Cliquez sur UTF. • Hexidecimal - Cliquez sur HEX. • Base64 - Cliquez sur Base64.
Informations supplémentaires	
Protocol	Indique le protocole associé à cet événement.
QID	Indique le QID de cet événement. Chaque événement possède un QID unique. Pour plus d'informations sur le mappage d'un QID, voir Modification d'un mappage d'événement .
Log Source	Indique la source du journal qui a envoyé l'événement à QRadar Network Anomaly Detection. S'il existe plusieurs sources de journal associées à cet événement, cette zone spécifie le terme Multiple et le nombre de sources du journal.

Tableau 4-4 Détails d'événement (suite)

Paramètre	Description
Event Count	Indique le nombre total des événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs du même type d'événement pour la même source et adresse IP cible sont détectés dans une période de temps courte.
Custom Rules	Indique les règles personnalisées qui correspondent à cet événement. Pour plus d'informations sur les règles, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Custom Rules Partially Matched	Indique les règles personnalisées qui correspondent partiellement à cet événement. Pour plus d'informations sur les règles, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Annotations	Indique l'annotation pour cet événement. Les annotations sont des descriptions texte que les règles peuvent ajouter automatiquement aux événements au sein d'une réponse de règle. Pour plus d'informations sur les règles, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
<p>Identity Information - QRadar Network Anomaly Detection collecte les informations d'identité, le cas échéant, des messages du journal source. Les informations d'identité fournissent des détails supplémentaires au sujet des actifs sur votre réseau. Les sources du journal génèrent seulement des informations d'identité si le message envoyé à QRadar Network Anomaly Detection contient une adresse IP et au moins un des éléments suivants : nom d'utilisateur ou adresse MAC. Toutes les sources du journal ne génèrent pas des informations d'identité. Pour plus d'informations sur l'identité et les actifs, voir Gestion des actifs.</p>	
Identity Username	Indique le nom d'utilisateur de l'actif associé à cet événement.
Identity IP	Indique l'adresse IP de l'actif associée à cet événement.
Identity Net Bios Name	Indique le nom du système d'entrée/sortie de la base du réseau (Net Bios) de l'actif associé à cet événement.
Identity Extended Field	Indique des informations supplémentaires sur l'élément associé à cet événement. Le contenu de cette zone est un texte défini par l'utilisateur et repose sur les périphériques sur votre réseau qui sont disponibles pour fournir des informations d'identité. On peut citer : l'emplacement physique des noms de ports, des politiques pertinentes, des commutateurs de réseau et des noms de port.
Has Identity (Flag)	Indique True si QRadar Network Anomaly Detection a collecté des informations identifiées pour l'actif associé à cet événement. Pour plus d'informations sur les périphériques qui envoient les informations d'identité, voir le <i>Guide de configuration DSM IBM Security QRadar</i> .
Identity Host Name	Indique le nom d'hôte de l'actif associé à cet événement.
Identity MAC	Indique l'adresse MAC de l'actif associée à cet événement.

Tableau 4-4 Détails d'événement (suite)

Paramètre	Description
Identity Group Name	Indique le nom du groupe de l'actif associé à cet événement.

La barre d'outils des détails des événements fournit les fonctions suivantes :

Tableau 4-5 Barre d'outils des détails d'événement

Fonction	Description
Return to Events List	Cliquez sur Return to Event List pour revenir à la liste des événements.
Offense	Cliquez sur Offense pour afficher les violations associées à cet événement.
Anomaly	Cliquez sur Anomaly pour afficher les résultats de recherche enregistrée qui a provoqué la règle de détection des anomalies pour générer cet événement. <i>Remarque : Cette icône s'affiche uniquement si cet événement a été généré par une règle de détection des anomalies.</i>
Map Event	Cliquez sur Map Event pour éditer le mappage d'événement. Pour plus d'informations, voir Modification d'un mappage d'événement .
False Positive	Cliquez sur False Positive pour ajuster QRadar Network Anomaly Detection à empêcher les événements du faux positif de générer les violations.
Extract Property	Cliquez sur Extract Property pour créer une propriété d'événement personnalisé à partir de l'événement sélectionné. Pour plus d'informations, voir Utilisation de la fonction Custom Event Properties .
Previous	Cliquez sur Previous pour afficher l'événement précédent dans la liste d'événement.
Next	Cliquez sur Next pour afficher l'événement suivant dans la liste d'événement.
PCAP Data	<i>Remarque : Cette option ne s'affiche que si votre QRadar Network Anomaly Detection Console est configuré pour s'intégrer avec Juniper JunOS Platform DSM. Pour plus d'informations sur la gestion des données PCAP, voir Gestion des données PCAP.</i>

A partir de la zone de liste **PCAP Data**, sélectionnez l'une des options suivantes :

- **View PCAP Information** - Sélectionnez cette option pour afficher les informations PCAP. Pour plus d'informations, voir [Affichage des informations PCAP](#).
- **Download PCAP File** - Sélectionnez cette option pour télécharger le fichier PCAP pour votre système de bureau. Pour plus d'informations, voir [Téléchargement du fichier PCAP pour votre système de bureau](#).

Tableau 4-5 Barre d'outils des détails d'événement (suite)

Fonction	Description
Print	Cliquez sur Print pour imprimer les détails d'événement.

Affichage de données d'événements brutes

Pour afficher les données d'événements brutes :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 A partir de la zone de liste **Display**, sélectionnez **Raw Events**.

Etape 3 A partir de la zone de liste **View**, sélectionnez le laps de temps que vous souhaitez afficher.

Les résultats de l'onglet **Log Activity** fournissent les données d'événements brutes suivantes :

Tableau 4-6 Paramètres d'événement brut

Paramètre	Description
Current Filters	La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche. Pour effacer les valeurs de filtre, cliquez sur Clear Filter . <i>Remarque : Ce paramètre ne s'affiche qu'après avoir appliqué un filtre.</i>
View	A partir de la zone de liste, sélectionnez la plage de temps que vous souhaitez filtrer.

Tableau 4-6 Paramètres d'événement brut (suite)

Paramètre	Description
Current Statistics	<p>Lorsqu'elles ne sont pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours sont affichées, notamment :</p> <p>Remarque : Cliquez sur la flèche à côté de Current Statistics pour afficher ou masquer les statistiques.</p> <ul style="list-style-type: none"> • Total Results - Indique le nombre total des résultats correspondant à vos critères de recherche. • Data Files Searched - Indique le nombre total des fichiers de données recherchés au cours de la plage de temps spécifié. • Compressed Data Files Searched - Indique le nombre total de fichiers de données compressées recherchés au cours de la plage de temps spécifiée. • Index File Count - Indique le nombre total de fichiers d'index recherchés au cours de la plage de temps spécifiée. • Duration - Indique la durée de la recherche. <p>Remarque : Les statistiques actuelles sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service clients pour identifier et résoudre les événements, on pourrait vous demander de fournir des informations statistiques actuelles.</p>
Charts	<p>Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'option de regroupement et l'intervalle de temps. Cliquez sur Hide Charts si vous souhaitez retirer les graphiques de votre écran.</p> <p>Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir Configuration des graphiques.</p> <p>Remarque : Si vous utilisez Mozilla Firefox comme navigateur et qu'un bloqueur de publicités est installé, les graphiques ne s'affichent pas. Pour afficher des graphiques, vous devez supprimer le bloqueur de publicités. Pour plus d'informations, voir la documentation de votre navigateur.</p>
Offenses icon	<p>Cliquez sur cette icône pour afficher les détails de violation associée à cet événement. Pour plus d'informations, voir Affichage des violations associées.</p>
Start Time	<p>Indique l'heure du premier événement telle que rapportée à QRadar Network Anomaly Detection par la source du journal.</p>
Log Source	<p>Indique la source du journal qui est à l'origine de cet événement. S'il existe plusieurs sources de journal associées à cet événement, cette zone spécifie le terme Multiple et le nombre de sources du journal.</p>

Tableau 4-6 Paramètres d'événement brut (suite)

Paramètre	Description
Payload	Indique les informations de contenu d'événement original au format UTF-8.

Etape 4 Cliquez deux fois sur l'événement que vous souhaitez afficher plus en détails.

Pour plus d'informations sur la page de détails des événements, voir [Tableau 4-4](#).
 Pour plus d'informations sur la barre de détails des événements, voir [Tableau 4-5](#).

Affichage des événements groupés

A l'aide de l'onglet **Log Activity**, vous pouvez afficher les événements groupés par diverses options. A partir de la zone de liste **Display**, vous pouvez sélectionner le paramètre par lequel vous souhaitez grouper les événements.

REMARQUE

La zone de liste **Display** n'est pas affichée dans le mode de transmission en continu parce que le mode de transmission en continu ne supporte pas les événements groupés. Si vous entrez en mode de transmission continu à l'aide des critères de recherche non groupés, cette option s'affiche.

Pour afficher les événements groupés :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 A partir de la zone de liste **View**, sélectionnez le cadre de temps que vous souhaitez afficher.

Etape 3 Depuis la zone de liste **Display**, choisissez l'une des options suivantes :

Tableau 4-7 Grouped Events Options

Option de groupe	Description
Low Level Category	Affiche une liste résumée des événements regroupés par la catégorie bas niveau de l'événement. Pour plus d'informations sur les catégories, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Event Name	Affiche une liste résumée des événements regroupés par le nom normalisé de l'événement.
Destination IP	Affiche une liste résumée des événements regroupés par l'adresse IP cible de l'événement.
Destination Port	Affiche une liste résumée des événements regroupés par l'adresse du port de destination de l'événement.
Source IP	Affiche une liste résumée des événements regroupés par l'adresse IP source de l'événement.
Custom Rule	Affiche une liste résumée des événements regroupés par la règle personnalisée associée.

Tableau 4-7 Grouped Events Options (suite)

Option de groupe	Description
Username	Affiche une liste résumée des événements regroupés par le nom d'utilisateur associé à l'événement.
Log Source	Affiche une liste résumée des événements regroupés par les sources de journal qui envoient l'événement QRadar Network Anomaly Detection.
High Level Category	Affiche une liste résumée des événements regroupés par la catégorie de haut niveau de l'événement. Pour plus d'informations sur les catégories, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Network	Affiche une liste résumée des événements regroupés par le réseau associé à l'événement.
Source Port	Affiche une liste résumée des événements regroupés par l'adresse source du port de l'événement.

L'agencement de colonne des données dépend de l'option de groupe choisie. Chaque ligne dans la table d'événements représente un groupe d'événements. L'onglet **Log Activity** fournit les informations suivantes lors de l'affichage groupé des événements :

Tableau 4-8 Paramètres d'événement groupés

Paramètre	Description
Grouping By	Indique le paramètre groupé sur la recherche.
Current Filters	La partie supérieure de la table affiche les détails du filtre appliqué aux résultats de la recherche. Pour effacer les valeurs de filtre, cliquez sur Clear Filter .
View	A partir de la zone de liste, sélectionnez la plage de temps que vous souhaitez filtrer.

Tableau 4-8 Paramètres d'événement groupés (suite)

Paramètre	Description
Current Statistics	<p>Lorsqu'elles ne s'ont pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours sont affichées, notamment :</p> <p>Remarque : Cliquez sur la flèche à côté Current Statistics pour afficher ou masquer les statistiques.</p> <ul style="list-style-type: none"> • Total Results - Indique le nombre total des résultats correspondant à vos critères de recherche. • Data Files Searched - Indique le nombre total des fichiers de données recherchés au cours de la plage de temps spécifié. • Compressed Data Files Searched - Indique le nombre total de fichiers de données compressées recherchés au cours de la plage de temps spécifiée. • Index File Count - Indique le nombre total de fichiers d'index cherchés au cours de la plage de temps spécifiée. • Duration - Indique la durée de la recherche. <p>Remarque : Les statistiques actuelles sont utiles pour l'identification et résolution des problèmes. Lorsque vous contactez le service clients pour identifier et résoudre les événements, on pourrait vous demander de fournir des informations statistiques actuelles.</p>
Charts	<p>Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'option de regroupement et l'intervalle de temps. Cliquez sur Hide Charts si vous souhaitez supprimer le graphique de votre affichage.</p> <p>Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir Configuration des graphiques.</p> <p>Remarque : Si vous utilisez Mozilla Firefox comme navigateur et qu'un bloqueur de publicités est installé, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer le bloqueur de publicités. Pour plus d'informations, voir la documentation de votre navigateur.</p>
Source IP (Unique Count)	Indique l'adresse IP de source associé à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone définit le terme Multiple et le nombre d'adresses IP.
Destination IP (Unique Count)	Indique l'adresse IP cible associée à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone définit le terme Multiple et le nombre d'adresses IP.
Destination Port (Unique Count)	Indique les ports de destination associés à cet événement. S'il existe plusieurs ports associés à cet événement, cette zone définit le terme Multiple et le nombre de ports.
Event Name	Indique le nom normalisé de l'événement.

Tableau 4-8 Paramètres d'événement groupés (suite)

Paramètre	Description
Log Source (Unique Count)	Indique les sources du journal qui a transmis l'événement à QRadar Network Anomaly Detection. S'il existe plusieurs sources de journal associées à cet événement, cette zone définit le terme Multiple et le nombre de sources du journal.
High Level Category (Unique Count)	Indique la catégorie de haut niveau de cet événement. S'il existe plusieurs catégories associées à cet événement, cette zone définit le terme Multiple et le nombre de catégories. Pour plus d'informations sur les catégories, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Low Level Category (Unique Count)	Indique la catégorie de bas niveau de cet événement. S'il existe plusieurs catégories associées à cet événement, cette zone définit le terme Multiple et le nombre de catégories. Pour plus d'informations sur les catégories, voir le <i>Guide d'administration IBM Security QRadar Network Anomaly Detection</i> .
Protocol (Unique Count)	Indique l'ID du protocole associé à cet événement. S'il existe plusieurs protocoles associés à cet événement, cette zone définit l'expression Multiple et le numéro des ID du protocole.
Username (Unique Count)	Indique le nom d'utilisateur associé à cet événement, si disponible. S'il existe plusieurs noms d'utilisateur associés à cet événement, cette zone définit le terme Multiple et le nombre de noms d'utilisateurs.
Magnitude (Maximum)	Indique l'ampleur maximale calculée pour les événements groupés. Les variables utilisées pour calculer la magnitude incluent la crédibilité, la pertinence et la gravité. Pour plus d'informations sur la crédibilité, la pertinence et la gravité, voir Glossaire .
Event Count (Sum)	Indique le nombre total des événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs du même type d'événement pour la même source et adresse IP cible sont détectés dans une période de temps courte.
Count	Indique le nombre total d'événements normalisés dans ce groupe d'événements.

Etape 4 Cliquez deux fois sur le groupe d'événement que vous souhaitez étudier.

La liste de la page Events affiche les événements appartenant au groupe sélectionné.

REMARQUE

La page List of Events ne conserve pas les configurations de graphique que vous avez peut-être définies sur l'onglet **Log Activity**.

Pour plus d'informations sur les paramètres List of Events, voir [Tableau 4-3](#).

Etape 5 Cliquez deux fois sur l'événement que vous souhaitez étudier

Pour plus d'informations sur la page de détails des événements, voir [Tableau 4-4](#).
 Pour plus d'informations sur la barre d'outils de détails des événements, voir [Tableau 4-5](#).

Affichage des violations associées

Si un événement correspond à un rôle, une violation peut être générée sur l'onglet **Offenses**. A partir de l'onglet **Log Activity**, vous pouvez afficher la violation associée avec l'événement en cliquant sur l'icône **Offense** pour l'événement que vous souhaitez étudier. Pour plus d'informations sur les règles, voir le *Guide d'administration IBM Security QRadar Network Anomaly Detection*. Pour plus d'informations sur la gestion des infractions, voir [Violations ou infractions](#).

Pour afficher une violation associée :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

REMARQUE

Si vous affichez des événements en mode de transmission en continu, vous devez mettre en pause le mode avant que vous étudiez un événement.

Etape 2 Cliquez sur l'icône **Offense** à côté de l'événement que vous souhaitez étudier.

REMARQUE

Si le Magistrate n'a pas encore enregistré l'infraction avec l'événement sélectionné sur le disque ou que l'infraction a été purgée de la base de données, un message d'information s'affiche.

Pour plus d'informations sur la gestion des infractions, voir [Violations ou infractions](#).

Modification d'un mappage d'événement

À des fins de normalisation, QRadar Network Anomaly Detection mappe automatiquement les événements de sources de journal aux catégories de concentration de haut et bas niveau. Pour plus d'informations sur les catégories d'événements, voir le *Guide d'administration IBM Security QRadar Network Anomaly Detection*.

À l'aide de la fonction Map Event, vous pouvez manuellement mapper un événement normalisé ou brut à une catégorie de haut et bas niveau (ou QID). Cette action manuelle permet à QRadar Network Anomaly Detection pour mapper les événements de source de journal inconnus à des événements connus QRadar Network Anomaly Detection afin qu'ils puissent être classés et traités de façon adéquate.

Lorsque QRadar Network Anomaly Detection reçoit des événements de sources de journal que le système ne parvient pas à catégoriser, QRadar Network Anomaly

Detection catégorise ces événements comme étant inconnus. Ces événements se produisent pour plusieurs raisons, notamment :

- **User-defined Events** - Certaines sources de journal comme Snort, vous permettent de créer des événements définis par l'utilisateur.
- **New Events or Older Events** - Les sources du journal du vendeur peuvent mettre à jour leurs logiciels avec des versions de maintenance pour prendre en charge de nouveaux événements que QRadar Network Anomaly Detection ne prend pas en charge.

REMARQUE

La fonction Map Event est désactivée pour les événements lorsque la catégorie de haut niveau est SIM Audit ou le type de source de journal est Simple Object Access Protocol (SOAP).

Pour modifier le mappage de l'événement :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

REMARQUE

Si vous affichez des événements en mode de transmission en continu, vous devez mettre en pause le mode avant que vous mappez un événement.

Etape 2 Pour tout événement normalisé ou brut, cliquez deux fois sur l'événement que vous souhaitez mapper.

Pour plus d'informations sur l'affichage d'événements personnalisés, voir [Affichage des événements normalisés](#). Pour plus d'informations sur l'affichage des événements bruts, voir [Affichage de données d'événements brutes](#).

Etape 3 Cliquez sur **Map Event**.

Etape 4 Si vous connaissez le QID que vous souhaitez mapper à cet événement, entrez le QID dans la zone **Enter QID**. Allez à [Etape 6](#).

Etape 5 Si vous ne connaissez pas le QID à associer à cet événement, recherchez un QID particulier :

- a Sélectionnez l'une des options suivantes :
 - Pour rechercher un QID par catégorie, sélectionnez la catégorie de haut niveau de la zone de liste **High-Level Category**.
 - Pour rechercher un QID par catégorie, sélectionnez la catégorie de bas niveau de la zone de liste **Low-Level Category**.
 - Pour rechercher un QID par type de source de journal, sélectionnez un type de source de journal de la zone de liste **Log Source Type**.
 - Pour rechercher un QID par nom, entrez le nom dans la zone **QID/Name**.
- b Cliquez sur **Search**.
Une liste des QID s'affiche.
- c Sélectionnez le QID que vous souhaitez associer à cet événement.

Etape 6 Cliquez sur **OK**.

Utilisation de la fonction Custom Event Properties

La fonction Custom Event Properties vous permet de rechercher, d'afficher et de rapporter les informations que contiennent les journaux et qu'en général, QRadar Network Anomaly Detection ne normalise et n'affiche pas.

REMARQUE

Pour créer des propriétés d'événement personnalisé, vous devez avoir l'autorisation de la propriété d'événement définie par l'utilisateur. Vérifiez auprès de votre administrateur pour vous assurer que vous disposez des autorisations appropriées. Pour plus d'informations sur les autorisations, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Vous pouvez créer des propriétés d'événement personnalisé depuis deux endroits sur l'onglet **Log Activity** :

- **Event details** - Sélectionnez un événement depuis l'onglet **Log Activity** pour créer une propriété de type événement personnalisé dérivé de son contenu.
- **Search page** - Vous pouvez créer et modifier une propriété de type événement personnalisé dans la page de recherche. Lorsque vous créez une nouvelle propriété d'événement personnalisé dans la page de recherche, la propriété d'événement n'est pas dérivée d'un événement particulier ; par conséquent, la fenêtre Event Property Definition n'est pas préremplie. Vous pouvez copier et coller le contenu des informations à partir d'une autre source. Pour plus d'informations, voir [Recherche d'événements ou de flux](#).

REMARQUE

Si vous disposez des autorisations Administrative, vous pouvez également créer et modifier les propriétés d'événement personnalisé de l'onglet **Admin**.

Cette section comprend les rubriques suivantes :

- [Création des propriétés d'événements personnalisés](#)
- [Modifier une propriété d'événement personnalisé](#)
- [Copie d'une propriété d'événement personnalisé](#)
- [Suppression d'une propriété d'événement personnalisé](#)

Creating Custom Event Properties

À l'aide de la fonction Custom Event Properties, vous pouvez créer deux types de propriétés d'événement personnalisé :

- **Regex** - À l'aide des instructions de l'expression régulière (Regex), vous pouvez extraire les données non normalisées du contenu d'événement.

Par exemple, QRadar Network Anomaly Detection rapports sur tous les utilisateurs qui font des modifications d'autorisations utilisateur sur un serveur Oracle. QRadar Network Anomaly Detection fournit une liste d'utilisateurs et le nombre de fois où ils ont apporté une modification à l'autorisation d'un autre compte. Cependant, en règle générale QRadar Network Anomaly Detection ne peut pas afficher le compte utilisateur courant ou l'autorisation qui a été modifiée. Vous pouvez créer une propriété de type événement personnalisé

pour extraire ces informations à partir des journaux et utiliser ensuite la propriété d'événement pour les recherches d'événements et rapports.

L'utilisation de cette fonctionnalité requiert une connaissance avancée des expressions régulières (regex). L'expression régulière définit la zone que vous voulez quelle soit la propriété d'événement personnalisé. Après avoir entré une instruction d'expression régulière, vous pouvez la valider par rapport au contenu. Lorsque vous définissez des modèles d'expressions régulières, optez pour des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez faire référence aux tutoriels d'expression régulière disponibles sur le Web.

Une propriété de type événement personnalisé peut être associée à plusieurs expressions régulières. Lorsqu'un événement est analysé, chaque modèle d'expression régulière est testé sur l'événement jusqu'à ce qu'un modèle d'expression régulière corresponde au contenu. Le premier modèle d'expression régulière correspondant au contenu d'événement détermine les données à extraire.

- **Calculated** - À l'aide des propriétés d'événement personnalisé basées sur le calcul, vous pouvez effectuer des calculs sur les propriétés d'événement numériques existantes pour produire une propriété calculée. Par exemple, vous pouvez créer une propriété qui affiche un pourcentage en divisant une propriété numérique par une autre.

Cette section comprend les rubriques suivantes :

- [Création d'une propriété d'événement personnalisé axée sur les Regex](#)
- [Création d'une propriété d'événement personnalisé basée sur le calcul](#)

Création d'une propriété d'événement personnalisé axée sur les Regex

Une propriété d'événement personnalisé basée sur l'expression régulière fait correspondre des contenus d'événement à une expression régulière.

Pour créer une propriété d'événement personnalisé basée sur les expressions régulières :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Cliquez deux fois sur l'événement sur lequel vous souhaitez baser la propriété d'événement personnalisé.

REMARQUE

Si vous affichez des événements en mode de transmission continu, vous devez mettre en pause ce mode avant de cliquer deux fois sur un événement.

Etape 3 Cliquez sur **Extract Property**.

REMARQUE

Si vous disposez des autorisations d'administration, vous pouvez accéder à la fenêtre Custom Event Properties sur l'onglet **Admin**. Cliquez sur **Admin > Data Sources > Custom Event Properties**. Pour plus d'informations, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Etape 4 Dans le panneau Property Type, sélectionnez l'option **Regex Based**.

Etape 5 Configurer les paramètres de propriété de l'événement personnalisé :

Tableau 4-9 Paramètres de la fenêtre de propriétés d'événement personnalisées

Paramètre	Description
Test Field	Indique le contenu qui a été extrait de l'événement non normalisé.
Property Definition	
Existing Property	Pour sélectionner une propriété existante, sélectionnez cette option et puis sélectionnez un nom de propriété enregistré précédemment dans la zone de liste.
New Property	Pour créer une nouvelle propriété, sélectionnez cette option et entrez un nom unique pour cette propriété de l'événement personnalisé. Le nouveau nom de propriété ne peut pas être le nom d'une propriété de type événement normalisé, comme Username, Source IP ou Destination IP.
Optimize parsing for rules, reports, and searches	<p>Pour analyser et stocker la propriété la première fois que QRadar Network Anomaly Detection reçoit l'événement, sélectionnez la case à cocher. Lorsque vous cochez la case, la propriété ne nécessite pas d'analyse supplémentaire pour les rapports, la recherche ou les essais de règle.</p> <p>Si vous désactivez cette case à cocher, la propriété est analysée à chaque fois qu'un rapport sur la recherche ou test de la règle est exécuté.</p> <p>Cette option est désactivée par défaut.</p>
Field Type	<p>Dans la zone de liste, sélectionnez le type de zone. Le type de zone détermine comment la propriété d'événement personnalisé s'affiche dans QRadar Network Anomaly Detection et les options disponibles pour l'agrégation. Les options du type de zone sont :</p> <ul style="list-style-type: none"> • Alpha-Numeric • Numeric • IP • Port <p>L'option par défaut est Alpha-Numeric.</p>
Description	Entrez une description de cette description d'événement personnalisé.
Property Expression Definition	

Tableau 4-9 Paramètres de la fenêtre de propriétés d'événement personnalisées (suite)

Paramètre	Description
Log Source Type	Dans la zone de liste, sélectionnez le type de source de journal auquel s'applique cette propriété d'événement personnalisé.
Log Source	Dans la zone de liste, sélectionnez la source du journal à laquelle s'applique cette propriété d'événement personnalisé. S'il existe plusieurs sources de journal associées à cet événement, cette zone spécifie le terme Multiple et le nombre de sources du journal.
Event Name	<p>Pour spécifier un nom d'événement auquel s'applique cette propriété d'événement personnalisé, sélectionnez cette option.</p> <p>Cliquez sur Browse pour accéder au navigateur de l'événement, puis sélectionnez le QRadar Identifier (QID) pour le nom d'événement que vous souhaitez appliquer à cette propriété d'événement personnalisé.</p> <p>Cette option est désactivée par défaut.</p>
Category	<p>Pour spécifier une catégorie de bas niveau à laquelle s'applique cette propriété d'événement personnalisé, sélectionnez cette option.</p> <p>Pour sélectionner une catégorie de bas niveau :</p> <ol style="list-style-type: none"> 1 A partir de la zone de liste High Level Category, sélectionnez la catégorie de bas niveau. Les mises à jour de la liste Low Level Category pour inclure uniquement les catégories de niveau inférieur associées à la catégorie sélectionnée de haut niveau. 2 A partir de la zone de liste Low Level Category, sélectionnez la catégorie de bas niveau à laquelle s'applique cette propriété d'événement personnalisé.

Tableau 4-9 Paramètres de la fenêtre de propriétés d'événement personnalisées (suite)

Paramètre	Description
RegEx	<p>Entrez l'expression régulière à utiliser pour extraire les données du contenu. Les expressions régulières sont sensibles à la casse.</p> <p>Exemple des expressions régulières :</p> <ul style="list-style-type: none"> • courrier électronique : <code>(.+@[^\.\.]*\.[a-z]{2,})\$</code> • Adresse URL : <code>(http\:\/\/[a-zA-Z0-9\-\.\.]+\.[a-zA-Z]{2,3}(/\s*)?\$)</code> • Nom de domaine : <code>(http[s]?:\/\/(.*?)["/?:])</code> • Nombre en virgule flottante : <code>([-+]?\d*\.\d*\$)</code> • Entier : <code>([-+]?\d*\$)</code> • Adresse IP : <code>(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)</code> <p>Par exemple : pour faire correspondre un journal se présente comme suit : SEVERITY=43 Construire l'Expression régulière comme suit : SEVERITY=([-+]?\d*\$)</p> <p>Remarque : Les groupes de capture doivent être placés entre parenthèses.</p>
Capture Group	<p>Entrez le groupe de capture à utiliser si l'expression régulière contient plus d'un groupe de capture.</p> <p>Les groupes de capture traitent les caractères multiples en tant qu'unité unique. Dans un groupe de capture, les caractères sont regroupés entre parenthèses.</p>
Test	<p>Cliquez sur Test pour tester l'expression régulière contre le contenu.</p>
Enabled	<p>Sélectionnez cette case à cocher pour activer cette propriété d'événement personnalisé. Si vous désactivez la case à cocher, cette propriété d'événement personnalisé ne s'affiche pas dans les filtres de recherche d'événements ou les listes de colonnes et la propriété d'événement ne sont pas analysées du contenu.</p> <p>La valeur par défaut est activée.</p>

Etape 6 Cliquez sur **Test** pour tester les expressions régulières par rapport au contenu.

Etape 7 Cliquez sur **Save**.

La propriété d'événement personnalisé apparaît maintenant en tant qu'une option dans la liste des colonnes disponibles sur la page de recherche.

REMARQUE

Les propriétés d'événement personnalisé ne sont pas automatiquement intégrées dans les listes des événements. Pour inclure une propriété d'événement

personnalisé dans une liste d'événements, vous devez sélectionner la propriété de l'événement personnalisé dans la liste des colonnes disponibles lors de la création d'une recherche.

Création d'une propriété d'événement personnalisé basée sur le calcul

Pour créer une propriété d'événement personnalisé basée sur le calcul :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez précédemment enregistré une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Cliquez deux fois sur l'événement sur lequel vous souhaitez baser la propriété d'événement personnalisé.

REMARQUE

Si vous affichez des événements en mode de transmission continu, vous devez mettre en pause ce mode avant de cliquer deux fois sur un événement.

Etape 3 Cliquez sur **Extract Property**.

REMARQUE

Si vous disposez des autorisations d'administration, vous pouvez accéder à la fenêtre Custom Event Properties sur l'onglet **Admin**. Cliquez sur **Admin > Data Sources > Custom Event Properties**. Pour plus d'informations, voir *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Etape 4 Dans le panneau Property Type, sélectionnez l'option **Calculation Based**.

Etape 5 Configurer les paramètres de propriété de l'événement personnalisé :

Tableau 4-10 Paramètres de la fenêtre des propriétés d'événement personnalisées

Paramètre	Description
Property Definition	
Property Name	Entrez un nom unique pour cette propriété de l'événement personnalisé. Le nouveau nom de propriété ne peut pas être le nom d'une propriété de type événement normalisé, comme Username, Source IP ou Destination IP.
Description	Entrez une description de cette propriété d'événement personnalisé.
Property Calculation Definition	
Property 1	Dans la zone de liste, sélectionnez la première propriété que vous souhaitez utiliser dans votre calcul. Les options incluent toutes les propriétés des événements numériques normalisés et personnalisés. Vous pouvez également définir une valeur numérique spécifique. A partir de la zone de liste Property 1 , sélectionnez l'option User Defined . Le paramètre Numeric Property s'affiche. Entrez une valeur numérique spécifique.

Tableau 4-10 Paramètres de la fenêtre des propriétés d'événement personnalisées (suite)

Paramètre	Description
Operator	Dans la zone de liste, sélectionnez l'opérateur que vous souhaitez appliquer aux propriétés sélectionnées dans le calcul. Les options incluent : <ul style="list-style-type: none"> • Add • Subtract • Multiply • Divide
Property 2	Dans la zone de liste, sélectionnez la seconde propriété que vous souhaitez utiliser dans votre calcul. Les options incluent toutes les propriétés des événements numériques normalisés et personnalisés. Vous pouvez également définir une valeur numérique spécifique. A partir de la zone de liste Property 1 , sélectionnez l'option User Defined . Le paramètre Numeric Property s'affiche. Entrez une valeur numérique spécifique.
Enabled	Sélectionnez cette case à cocher pour activer cette propriété d'événement personnalisé. Si vous désactivez la case à cocher, cette propriété d'événement personnalisé ne s'affiche pas dans les filtres de recherche d'événements ou les listes de colonnes et la propriété d'événement ne sont pas analysées du contenu. La valeur par défaut est activée.

Etape 6 Cliquez sur **Save**.

La propriété d'événement personnalisé apparaît maintenant en tant qu'une option dans la liste des colonnes disponibles sur la page de recherche.

REMARQUE

Les propriétés d'événement personnalisé ne sont pas automatiquement intégrées dans les listes des événements. Pour inclure une propriété d'événement personnalisé dans une liste d'événements, vous devez sélectionner la propriété de l'événement personnalisé dans la liste des colonnes disponibles lors de la création d'une recherche.

Modifier une propriété d'événement personnalisé

Pour modifier une propriété d'événement personnalisé :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Dans la zone de liste **Search**, sélectionnez **Edit Search**.

Etape 3 Cliquez sur **Manage Custom Properties**.

La fenêtre Custom Event Properties fournit les informations suivantes :

Tableau 4-11 Gérer les colonnes de la fenêtre des propriétés d'événement personnalisé

Colonne	Description
Property Name	Indique un nom unique pour cette propriété de l'événement personnalisé.
Type	Indique le type de cette propriété de l'événement personnalisé. Les options incluent : <ul style="list-style-type: none"> • Regex - Une propriété d'événement personnalisé basée sur une expression régulière correspond à une propriété de type événement personnalisé axé sur l'expression régulière. Voir Création des propriétés d'événements personnalisés • Calculated - Une propriété de type événement personnalisé basée sur le calcul effectuée un calcul sur les propriétés de l'événement. Voir Création d'une propriété d'événement personnalisé basée sur le calcul.
Property Description	Indique une description pour cette propriété d'événement personnalisé.
Log Source Type	Indique le nom du type de source de journal auquel s'applique cette propriété d'événement personnalisé.
Log Source	Indique la source du journal à laquelle s'applique cette propriété d'événement personnalisé. S'il existe plusieurs sources de journal associées à cet événement, cette zone définit le terme Multiple et le nombre de sources du journal.
Expression	Indique l'expression de cette propriété d'événement personnalisé. L'expression dépend du type de propriété d'événement personnalisé : <ul style="list-style-type: none"> • Pour une propriété de type événement personnalisé basée sur les expressions régulières, ce paramètre définit l'expression régulière à utiliser pour extraire les données du contenu. • Pour une propriété de type événement personnalisé basée sur le calcul, ce paramètre spécifie le calcul que vous souhaitez utiliser pour créer une valeur de propriété d'événement personnalisé.
Username	Indique le nom de l'utilisateur qui a créé cette propriété d'événement personnalisé.
Enabled	Indique si cette propriété d'événement personnalisé est activée. Cette zone spécifie True ou False.
Creation Date	Indique la date de création de cette propriété de type événement personnalisé.
Modification Date	Indique la dernière modification de cette propriété d'événement personnalisé.

La barre d'outils Custom Event Property fournit les fonctions suivantes :

Tableau 4-12 Options de la barre d'outils de la propriété d'événement personnalisé

Option	Description
Add	Cliquez sur Add pour ajouter une nouvelle propriété d'événement personnalisé. Voir Création des propriétés d'événements personnalisés .
Edit	Cliquez sur Edit pour modifier la propriété sélectionnée de l'événement personnalisé.
Copy	Cliquez sur Copy pour copier les propriétés sélectionnées de l'événement personnalisé.

Tableau 4-12 Options de la barre d'outils de la propriété d'événement personnalisé (suite)

Delete	Cliquez sur Delete pour supprimer les propriétés sélectionnées de l'événement personnalisé.
Enable/Disable	Cliquez sur Enable/Disable pour activer ou désactiver les propriétés sélectionnées de l'événement personnalisé pour l'analyse et la visualisation dans le cas des filtres de recherche ou de la colonne de liste.

Etape 4 Sélectionnez la propriété d'événement personnalisé que vous souhaitez éditer et cliquez sur **Edit**.

REMARQUE

Vous pouvez également cliquer deux fois sur la propriété d'événement personnalisé que vous souhaitez modifier.

Etape 5 Modifiez les paramètres nécessaires. Voir [Tableau 4-9](#).

Etape 6 Si vous avez modifié l'expression régulière, cliquez sur **Test** pour tester l'expression régulière par rapport au contenu.

Etape 7 Cliquez sur **Save**.

La propriété d'événement personnalisé modifiée est maintenant mise à jour dans la liste des colonnes disponibles sur la page de recherche.

REMARQUE

Les propriétés d'événement personnalisé ne sont pas automatiquement intégrées dans les listes des événements. Pour inclure une propriété d'événement personnalisé dans une liste d'événements, vous devez sélectionner la propriété de l'événement personnalisé dans la liste des colonnes disponibles lors de la création d'une recherche.

Copie d'une propriété d'événement personnalisé

Pour copier une propriété d'événement personnalisé :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Dans la zone de liste **Search**, sélectionnez **Edit Search**.

Etape 3 Cliquez sur **Manage Custom Properties**.

Etape 4 Sélectionnez la propriété d'événement personnalisé que vous souhaitez copier, puis cliquez sur **Copy**.

Etape 5 Sélectionnez l'option **New Property** et entrez le nom d'une nouvelle propriété.

Etape 6 Modifiez les paramètres nécessaires. Voir [Paramètres de la fenêtre de propriétés d'événement personnalisées](#).

Etape 7 Si vous avez modifié l'expression régulière, cliquez sur **Test** pour tester l'expression régulière par rapport au contenu.

Etape 8 Cliquez sur **Save**.

La propriété d'événement personnalisé copiée est maintenant disponible dans la liste des colonnes disponibles sur la page de recherche.

REMARQUE

Les propriétés d'événement personnalisé ne sont pas automatiquement intégrées dans les listes des événements. Pour inclure une propriété d'événement personnalisé dans une liste d'événements, vous devez sélectionner la propriété de l'événement personnalisé dans la liste des colonnes disponibles lors de la création d'une recherche.

Suppression d'une propriété d'événement personnalisé

Vous pouvez supprimer toute propriété personnalisée, à condition que la propriété personnalisée ne soit pas associée à une autre. Si vous tentez de supprimer une propriété personnalisée associée à une autre, un message d'erreur s'affiche, indiquant le nom de la propriété personnalisée associée.

Pour supprimer une propriété d'événement personnalisé :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats enregistrés pour cette recherche s'affichent.

Etape 2 Dans la zone de liste **Search**, sélectionnez **Edit Search**.**Etape 3** Cliquez sur **Manage Custom Properties**.**Etape 4** Sélectionnez la propriété d'événement personnalisé que vous souhaitez supprimer et cliquez sur **Delete**.**Etape 5** Cliquez sur **Oui**.

La propriété d'événement personnalisé supprimée n'apparaît plus dans les détails de l'événement.

Réglage des faux positifs

Vous pouvez utiliser la fonction False Positive Tuning pour régler les événements de faux positifs à partir des infractions créées. Vous devez disposer des droits appropriés pour créer des règles personnalisées afin de régler les faux positifs. Pour plus d'informations sur les rôles, voir le *Guide d'administration IBM Security QRadar Network Anomaly Detection*. Pour plus d'informations sur les faux positifs, voir [Glossaire](#).

Pour régler un événement de faux positifs :

Etape 1 Cliquez sur l'onglet **Log Activity**.**Etape 2** Sélectionnez l'événement que vous souhaitez régler.**Etape 3** Cliquez sur **False Positive**.**REMARQUE**

Si vous affichez des événements en mode transmission continu, vous devez suspendre ledit mode avant de cliquer sur **False Positive**.

La fenêtre False Positive s'affiche avec des informations dérivées de l'événement sélectionné.

Etape 4 Sélectionnez l'une des options suivantes **Event/Flow Property** :

- Les Event/Flow avec un QID caractéristique de <Event>
- Toutes les Event/Flow avec une catégorie de bas niveau du <Event>
- Toutes les Event/Flow avec une catégorie de haut niveau du <Event>

Etape 5 Sélectionnez l'une des options de **Traffic Direction** :

- <Source IP Address> to <Destination/// IP Address>
- <Source IP Address> to Any Destination
- Any Source to <Destination IP Address>
- Any Source to any Destination

Etape 6 Cliquez sur **Tune**.

REMARQUE

Vous pouvez ajuster les événements du faux positif depuis la page de résumé ou de détails.

Gestion des données PCAP

Si votre QRadar Network Anomaly Detection Console est configurée pour s'intégrer à Juniper JunOS Platform DSM, QRadar Network Anomaly Detection peut recevoir, traiter et stocker les données Packet Capture (PCAP) d'une source de journal Juniper SRX-Series Services Gateway. Pour plus d'informations sur Juniper JunOS Platform DSM, voir le *IBM Security QRadar Guide de configuration DSM*.

Avant que vous ne puissiez afficher les données PCAP sur l'onglet **Log Activity**, la source du journal Juniper SRX-Series Services Gateway doit être configurée avec le protocole PCAP Syslog Combination. Pour plus d'informations sur la configuration des protocoles de la source du journal, voir le *IBM Security QRadar Guide d'utilisation des sources de journal*.

Cette section comprend les rubriques suivantes :

- [Affichage de la colonne PCAP Data](#)
- [Affichage des informations PCAP](#)
- [Téléchargement du fichier PCAP pour votre système de bureau](#)

Affichage de la colonne PCAP Data

La colonne PCAP Data n'est pas affichée par défaut sur l'onglet **Log Activity**. Lorsque vous créez un critère de recherche, vous devez sélectionner la colonne **PCAP Data** dans le panneau Column Definition. Vous pouvez également grouper vos résultats de recherche d'événement à l'aide de la colonne **PCAP Data**. Pour plus d'informations sur la recherche et l'affichage d'événements, voir [Enquête d'événements](#).

Pour afficher la colonne **PCAP Data** dans les résultats de la recherche d'événement :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Etape 2 Dans la zone de liste **Search**, sélectionnez **New Search**.

Etape 3 Facultatif. Configurez votre critère de recherche caractéristique :

REMARQUE

Si vous effectuez cette étape, les résultats de la recherche affichent seulement les événements qui possèdent des données PCAP disponibles.

a Dans la première zone de liste, sélectionnez **PCAP data**.

b Dans la seconde zone de liste, sélectionnez **Equals**.

c Dans la troisième zone de liste, sélectionnez **True**.

d Cliquez sur **Add Filter**.

Etape 4 Configurez vos définitions de colonne :

a Depuis la liste **Available Columns** dans le panneau Column Definition, cliquez sur **PCAP Data**.

b Cliquez sur l'icône **Add Column** sur l'ensemble inférieur des icônes pour déplacer la colonne **PCAP Data** à la liste **Columns**.

c Facultatif. Cliquez sur l'icône **Add Column** dans le haut de l'ensemble des icônes pour déplacer la colonne **PCAP Data** d'une liste **Group By**.

Etape 5 Cliquez sur **Filter**.

REMARQUE

Vous pouvez configurer votre recherche d'événement à l'aide des paramètres supplémentaires, toutefois, cette procédure ne montre que les critères de recherche requis pour afficher la colonne de données PCAP. Pour plus d'informations sur la recherche d'événements, voir [Recherche d'événements ou de flux](#).

Les résultats de la recherche d'événements sont affichés, y compris la colonne **PCAP Data**. Si les données PCAP sont disponibles pour un événement, une icône est affichée dans la colonne **PCAP Data**. En utilisant l'icône **PCAP**, vous pouvez afficher les données PCAP ou télécharger le fichier PCAP pour votre système de bureau.

Etape 6 Cliquez deux fois sur l'événement que vous souhaitez étudier.

REMARQUE

Si vous affichez des événements en mode de transmission continu, vous devez mettre en pause ce mode avant de cliquer deux fois sur un événement.

A partir de l'option de la barre d'outils **PCAP Data**, vous affichez les informations PCAP ou téléchargez le fichier PCAP sur votre système de bureau.

Pour plus d'informations sur l'affichage et le téléchargement des données PCAP, voir les sections suivantes :

- [Affichage des informations PCAP](#)
- [Téléchargement du fichier PCAP pour votre système de bureau](#)

Affichage des informations PCAP

Vous pouvez consulter une version lisible des données dans le fichier PCAP. Pour afficher les informations PCAP :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Etape 2 Effectuez ou sélectionnez une recherche qui affiche la colonne **PCAP Data**. Voir [Affichage de la colonne PCAP Data](#).

Les résultats de recherche d'événement sont affichés.

Etape 3 Choisissez l'une des opérations suivantes :

- Cliquez avec le bouton droit de la souris sur l'icône **PCAP** de l'événement que vous souhaitez étudier, puis sélectionnez **More Options > View PCAP Information**.
- Cliquez deux fois sur l'événement que vous souhaitez étudier, puis sélectionnez **PCAP Data > View PCAP Information** à partir de la barre d'outils des détails d'événement.

REMARQUE

Si vous affichez les événements en mode transmission continu, vous devez mettre en pause ce mode avant de cliquer deux fois sur un événement.

REMARQUE

Avant que les données PCAP ne puissent être affichées, QRadar Network Anomaly Detection doit récupérer le fichier PCAP pour l'afficher sur l'interface. Si le processus de téléchargement prend un certain temps, la fenêtre de téléchargement PCAP Packet Information s'affiche. Dans la plupart des cas, le processus de téléchargement est rapide et cette fenêtre ne s'affiche pas.

Après que le fichier est récupéré, une fenêtre contextuelle s'affiche, fournissant une version lisible du fichier PCAP. Vous pouvez lire les informations affichées dans la fenêtre ou télécharger les informations sur votre système de bureau

Etape 4 Si vous voulez télécharger les informations sur votre système de bureau, choisissez l'une des options suivantes :

- Cliquez sur **Download PCAP File** pour télécharger le fichier PCAP d'origine pour être utilisé dans une application externe.
- Cliquez sur **Download PCAP Text** pour télécharger le plan d'action en format.TXT.

Etape 5 Sélectionnez l'une des options suivantes :

- Si vous souhaitez ouvrir le fichier pour l'affichage immédiat, sélectionnez l'option **Open with** et sélectionnez une application dans la zone de liste.
- Si vous souhaitez enregistrer la liste, sélectionnez l'option **Save File**.

Etape 6 Cliquez sur **OK**.

Téléchargement du fichier PCAP pour votre système de bureau Vous pouvez télécharger le fichier PCAP pour votre système de bureau pour le stockage ou pour une utilisation dans d'autres applications. Pour télécharger le fichier PCAP pour votre système de bureau :

Etape 1 Cliquez sur l'onglet **Log Activity**.

Etape 2 Effectuez ou sélectionnez une recherche qui affiche la colonne **PCAP Data**. Voir [Affichage de la colonne PCAP Data](#).

Les résultats de recherche d'événement sont affichés.

Etape 3 Pour l'événement que vous souhaitez étudier, choisissez une des méthodes suivantes :

- Cliquez sur l'icône **PCAP**.
- Cliquez avec le bouton droit de la souris sur l'icône **PCAP** puis sélectionnez **More Options > Download PCAP File**.
- Cliquez deux fois sur l'événement que vous souhaitez étudier, puis sélectionnez **PCAP Data > Download PCAP File** depuis la barre d'outils des détails des événements.

REMARQUE

Si vous affichez les événements en mode transmission continu, vous devez mettre en pause ce mode avant que vous cliquez deux fois sur un événement.

Etape 4 Choisissez l'une des options suivantes :

- Si vous souhaitez ouvrir le fichier pour l'affichage immédiat, sélectionnez l'option **Open with** et sélectionnez une application dans la zone de liste.
- Si vous souhaitez enregistrer la liste, sélectionnez l'option **Save File**.

Etape 5 Cliquez sur **OK**.

Exportation des événements

Vous pouvez exporter des événements en format Extensible Markup Language (XML) ou Comma Separated Values (CSV). La longueur du temps nécessaire pour exporter vos données dépend du nombre de paramètres spécifié.

Pour exporter des événements :

Etape 1 Cliquez sur l'onglet **Log Activity**.

REMARQUE

Si vous affichez des événements en mode de transmission en continu vous devez mettre en pause le mode avant d'exporter des informations d'événement.

Etape 2 A partir de la zone de liste **Actions**, sélectionnez l'une des options suivantes :

- **Export to XML > Visible Columns** -Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles sur l'onglet **Log Activity**. Il s'agit de l'option recommandée.
- **Export to XML > Full Export (All Columns)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour terminer.
- **Export to CSV > Visible Columns** - Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles sur l'onglet **Log Activity**. Il s'agit de l'option recommandée.
- **Export to CSV > Full Export (All Columns)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour terminer.

Etape 3 Si vous souhaitez reprendre vos activités, cliquez sur **Notify When Done**.

Vous recevez une notification une fois l'exportation est terminée. Si vous n'avez pas sélectionné l'icône **Notify When Done**, la fenêtre d'état s'affiche.

5

ETUDE DES FLUX

A l'aide de l'onglet **Network Activity**, vous pouvez surveiller et enquêter sur l'activité du réseau (flux) en temps réel ou effectuer des recherches avancées.

Cette section comprend les rubriques suivantes :

- [L'onglet Using the Network Activity](#)
- [Affichage des flux](#)
- [Affichage des violations associées](#)
- [Utilisation des propriétés de flux personnalisé](#)
- [Réglage des faux Positifs](#)
- [Exportation des flux](#)

Présentation de l'onglet Network Activity

Vous devez avoir le droit d'afficher l'onglet **Network Activity**. Pour plus d'informations sur les autorisations et l'affectation de rôles, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

L'onglet **Network Activity** vous permet de contrôler visuellement et d'étudier les données de flux en temps réel, ou d'effectuer des recherches avancées pour filtrer les flux affichés. Un flux est une session de communication entre deux hôtes. Vous pouvez afficher les informations des flux afin de déterminer comment le trafic est communiqué et ce qui est communiqué (si l'option de capture de contenu est activée). Les informations sur le flux peuvent également comprendre certains détails tels que les protocoles, les valeurs ASN ou les valeurs IFIndex (Interface Index). Vous pouvez utiliser l'onglet **Network Activity** pour :

- Chercher des flux. Voir [Recherche de données](#).
- Sauvegarder et gérer les critères et les résultats de recherche
- Afficher les flux en temps réel (diffusion en flux)
- Afficher les informations liées au flux groupés par divers options
- Créer, afficher et étudier les graphiques de séries temporelles
- Ajustez les flux faux positifs à partir de la génération des violations
- Exporter les flux en format XML ou CSV

L'onglet Using the Network Activity

Si vous avez déjà configuré une recherche sauvegardée en tant que recherche par défaut, les résultats de cette recherche sont automatiquement affichés lorsque vous accédez à l'onglet **Network Activity**. Pour plus d'informations sur l'enregistrement du critère de recherche, voir [Sauvegarde des critères de recherche](#).

Cette section comprend les rubriques suivantes :

- [Utilisation de la barre d'outils](#)
- [Utilisation des options du menu contextuel](#)
- [Utilisation de la barre d'état](#)

Utilisation de la barre d'outils

La barre d'outils fournit les options suivantes :

Tableau 5-1 Les options de la barre d'outils de l'onglet Network Activity

Option	Description
Search	<p>Cliquez sur Search pour effectuer des recherches avancées sur les flux. Les options comprennent :</p> <ul style="list-style-type: none"> • New Search - Sélectionnez cette option pour créer une nouvelle recherche de flux. • Edit Search - Sélectionnez cette option afin de sélectionner et éditer la recherche de flux. • Manage Search Results - Sélectionnez cette option afin d'afficher et gérer les résultats de recherche. Voir Gestion des résultats de recherche. <p>Pour plus d'informations sur la fonctionnalité de recherche, voir Recherche de données.</p>
Quick Searches	<p>A partir de cette zone de liste, vous pouvez exécuter les recherches sauvegardées. Les options ne sont affichées dans la zone de liste Quick Searches qu'après avoir sauvegardé les critères de recherche qui indiquent l'option Include in my Quick Searches.</p>
Add Filter	<p>Cliquez sur Add Filter afin d'ajouter un filtre aux résultats de recherche en cours.</p>
Save Criteria	<p>Cliquez sur Save Criteria afin de sauvegarder le critère de recherche suivant.</p>
Save Results	<p>Cliquez sur Save Results afin de sauvegarder les résultats de recherche en cours. Cette option n'est affichée que lorsqu'une recherche est complétée. En mode de transmission en continu cette option est désactivée.</p>
Cancel	<p>Cliquez sur Cancel pour annuler une recherche en progression. En mode de transmission en continu, cette option est désactivée.</p>

Tableau 5-1 Les options de la barre d'outils de l'onglet Network Activity (suite)

Option	Description
False Positive	<p>Cliquez sur False Positive afin d'ouvrir la fenêtre d'optimisation des faux positifs, qui vous permet d'ajuster les flux connus en tant que faux positifs à partir de la création des violations. Pour plus d'informations sur les faux positifs, voir le Glossaire.</p> <p>En mode de transmission en continu, cette option est désactivée. Voir Exportation des flux.</p>

Tableau 5-1 Les options de la barre d'outils de l'onglet Network Activity (suite)

Option	Description
Rules	<p data-bbox="678 338 1317 401">Cliquez sur Rules afin de configurer les règles de flux personnalisées. Les options comprennent :</p> <ul data-bbox="678 411 1456 527" style="list-style-type: none"> <li data-bbox="678 411 1456 527">• Rules - Sélectionnez cette option afin de créer une règle. Lorsque vous sélectionnez l'option Rules, l'assistant des règles s'affiche, déjà rempli avec les options appropriées pour la création d'une règle de flux. <p data-bbox="678 537 1456 695">Remarque : Afin d'activer les options de la règle de détection des anomalies (ajoutez la règle de seuil, ajoutez une règle comportementale et ajoutez une règle d'anomalie), vous devez ajouter un critère de recherche agrégé parce que le critère de recherche sauvegardé indique les paramètres nécessaires</p> <ul data-bbox="678 705 1456 947" style="list-style-type: none"> <li data-bbox="678 705 1456 947">• Add Threshold Rule - Sélectionnez cette option pour créer une règle de seuil. Une règle de seuil teste le trafic de flux pour une activité qui dépasse un seuil configuré. Un seuil peut être basé sur n'importe quelles données collectées par QRadar Network Anomaly Detection. Par exemple, si vous créez une règle de seuil indiquant que pas plus de 220 clients peuvent se connecter au serveur entre 08 et 17 heures, les règles génèrent une alerte lorsque le 221^{ème} client tente de se connecter. <p data-bbox="711 957 1386 1052">Lorsque vous sélectionnez l'option Add Threshold Rule, l'assistant des règles s'affiche, rempli avec les options appropriées pour la création d'une règle de seuil.</p> <ul data-bbox="678 1062 1456 1293" style="list-style-type: none"> <li data-bbox="678 1062 1456 1293">• Add Behavioral Rule - Sélectionnez cette option afin de créer une règle de seuil. Une règle de comportement teste le trafic de flux afin que le volume change dans le comportement qui se produit dans des modèles saisonniers réguliers. Par exemple, si un serveur de message communique typiquement avec 100 hôtes par seconde à minuit et qu'ensuite il commence à communiquer avec 1000 hôtes par seconde, une règle comportementale génère une alerte. <p data-bbox="711 1304 1403 1398">Lorsque vous sélectionnez l'option Add Behavioral Rule, l'assistant des règles s'affiche, rempli avec les options appropriées pour la création d'une règle comportementale.</p> <ul data-bbox="678 1409 1456 1671" style="list-style-type: none"> <li data-bbox="678 1409 1456 1671">• Add Anomaly Rule - Sélectionnez cette option afin de créer une règle d'anomalie. Une règle d'anomalie teste le trafic du flux pour une activité anormale, telle que l'existence d'un trafic nouveau ou inconnu, qui est un trafic qui subitement arrête ou change de pourcentage dans un temps donné un objet est actif <Par exemple, vous pouvez créer une règle d'anomalie pour comparer le volume moyen du trafic des cinq dernières minutes avec le volume moyen du trafic sur la dernière heure. S'il s'agit d'un changement de plus de 40%, la règle génère une réponse. <p data-bbox="711 1682 1370 1776">Lorsque vous sélectionnez l'option Add Anomaly Rule, l'assistant de règle s'affiche, rempli avec les options appropriées pour la création d'une règle d'anomalie</p> <p data-bbox="678 1787 1386 1841">Pour plus d'informations sur les règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>.</p>

Tableau 5-1 Les options de la barre d'outils de l'onglet Network Activity (suite)

Option	Description
Actions	<p>Cliquez sur Actions pour effectuez les options suivantes :</p> <ul style="list-style-type: none"> • Show All - Sélectionnez cette option afin de déplacer tous les filtres sur le critère de recherche et pour afficher tous les flux infiltrés. • Print - Sélectionnez cette option afin d'imprimer les flux affichés sur la page. • Export to XML - Sélectionnez cette option pour exporter les flux en format XML. Voir Exportation des flux. • Export to CSV - Sélectionnez cette option pour exporter les flux en format CSV. Voir Exportation des flux. • Delete - Sélectionnez cette option pour supprimer un résultat de recherche. Voir Effacer un recherche. • Notify - Sélectionnez cette option pour indiquer que vous souhaitez recevoir une notification par email à la fin des recherches sélectionnées. Cette option est uniquement activée pour les recherches en cours. <p>Remarque : Les options Print, Export to XML et Export to CSV sont activées en mode diffusion en flux et lors de l'affichage des résultats de recherche partielle.</p>
Quick Filter	<p>Entrez vos critères de recherche dans la zone Quick Filter et cliquez sur l'icône Quick Filter ou appuyez sur Enter de votre clavier. Tous les flux qui correspondent aux critères de recherche sont affichés dans la liste des flux. Une recherche de texte s'exécute sur le contenu de l'événement afin de déterminer celui qui correspond à votre critère spécifiques.</p> <p>Remarque : Lorsque vous cliquez sur la zone Quick Filter, un infobulle s'affiche, fournissant des informations sur la syntaxe appropriée à utiliser pour le critère de recherche. Pour plus d'informations sur la syntaxe, voir Utilisation de Quick Filter Syntax.</p>

Utilisation de Quick Filter Syntax

Le filtre rapide vous permet de rechercher les contenus des flux à l'aide de la ligne recherche de texte. La fonctionnalité Quick Filter est disponible dans les emplacements suivants sur l'interface utilisateur :

- **Network Activity toolbar** - Sur la barre d'outils, une zone **Quick Filter** vous permet d'entrer une ligne de recherche de texte et de cliquer sur l'icône **Quick Filter** afin d'appliquer votre filtre rapide pour la liste des flux en cours.
- **Add Filter dialog box** - A partir de la boîte de dialogue **Add Filter**, accédez en cliquant sur l'icône **Add Filter** sur l'onglet **Network Activity**, vous pouvez sélectionner **Quick Filter** en tant que paramètre de filtre et entrer une ligne de recherche de texte. Ceci vous permet d'appliquer votre filtre rapide à la liste de flux actuellement affichée. Pour plus d'informations sur la boîte de dialogue Add Filter, voir [Etude de sous-recherche](#).

- **Flow search pages** - A partir des pages, vous pouvez ajouter un filtre rapide à votre liste de filtre à inclure dans vos critères de recherche. Pour plus d'informations sur la configuration du critère de recherche, voir [Recherche d'événements ou flux](#).

Lorsque vous affichez les flux en mode temps réel (streaming) ou en mode dernier intervalle, vous ne pouvez entrer que les mots et les phrases simples dans la zone **Quick Filter**. Lorsque vous affichez un flux à l'aide d'un intervalle de temps, utilisez les guides de syntaxe pour entrer votre critère de recherche :

- Les termes de recherche peuvent contenir n'importe quel texte brut que vous attendez trouver dans le contenu. Par exemple, `Firewall`
- Notamment les différents termes entre guillemets pour indiquer que vous souhaitez rechercher la phrase exacte. Par exemple, `"Firewall deny"`
- Les termes de recherche peuvent contenir un ou plusieurs caractères génériques. Un terme de recherche ne peut pas commencer par un caractère générique. Par exemple, `F?rewall` ou `F??ew*`
- Les termes de groupes utilisant des expressions logiques telles que AND, OR et NOT. La syntaxe est sensible à la casse et les opérateurs doivent être en majuscules afin qu'ils soient reconnus en tant qu'expressions logiques et non pas en tant que termes de recherche. Par exemple : `(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`

Lorsque vous créez un critère de recherche qui comprend l'expression logique NOT, vous devez inclure au moins un autre type d'expression logique, si non, votre filtre ne trouvera aucun résultat. Par exemple : `(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`

- Les caractères suivants doivent être précédés par une barre oblique inversée afin d'indiquer que le caractère fait partie du terme de recherche : + - && || ! () {} [] ^ " ~ * ? : \. Par exemple : `"%PIX\ -5\ -304001"`

Utilisation des options du menu contextuel

Sur l'onglet **Network Activity**, vous pouvez effectuer un clic droit sur un flux afin d'accéder à un critère de filtre supplémentaire.

Les options du menu contextuel sont :

Tableau 5-2 Options du menu contextuel

Option	Description
Filter on	Sélectionnez cette option pour filtrer les flux sélectionnés, en fonction du paramètre sélectionné dans le flux.
False Positive	Sélectionnez cette option afin d'ouvrir la fenêtre False Positive Tuning, qui vous permet d'ajuster les flux connus pour être des faux positifs à partir de la création des violations. En mode de transmission en continu, cette option est désactivée. Voir Exportation des flux .
More options:	Sélectionnez cette option pour étudier une adresse IP. Voir Etude des adresses IP .

Remarque : Cette option s'affiche en mode de diffusion en flux

Utilisation de la barre d'état

Lors de la diffusion des flux, la barre d'état affiche la moyenne des résultats reçus par seconde. Ceci est le nombre de résultats que la console a reçus avec succès du processeur d'événement. Si ce nombre est supérieur à 40 résultats par seconde, uniquement 40 résultats s'affichent. Le reste est mémorisé dans la mémoire tampon. Pour afficher les informations sur l'état, placez le pointeur de votre souris sur la barre d'état.

Lorsque QRadar Network Anomaly Detection ne diffuse pas les flux, la barre d'état affiche le nombre de résultats de recherche actuellement affichés ainsi que le temps nécessaire pour le traitement des résultats de recherche.

Affichage des flux

Par défaut, l'onglet **Network Activity** affiche les flux en mode diffusion en flux, vous permettant d'afficher les flux en temps réel. Pour plus d'informations sur le mode de diffusion, voir [Affichage des flux de diffusion en flux](#). Vous pouvez spécifier un intervalle pour filtrer les flux utilisant la zone de liste **View**.

REMARQUE

Si vous possédez des droits d'administration, vous pouvez indiquer le nombre maximal de flux que vous souhaitez envoyer à partir de QRadar QFlow Collector vers les processeurs d'événement. Toutes les données collectées après l'atteinte de la limite de flux configuré sont regroupées dans un enregistrement de flux unique. Cet enregistrement de flux s'affiche ensuite sur l'onglet **Network Activity** avec l'adresse IP source de 127.0.0.4 et l'adresse IP de destination de 127.0.0.5. Cet enregistrement de flux indique le dépassement sur l'onglet **Network Activity**.

Vous pouvez afficher les flux en utilisant l'une des options suivantes :

- [Affichage des flux de diffusion en flux](#)
- [Affichage des flux normalisés](#)
- [Affichage des flux groupés](#)

Affichage des flux de diffusion en flux

Le mode de diffusion en flux vous permet d'afficher les données entrantes à votre système. Ce mode vous fournit avec un affichage en mode temps réel de votre activité de flux en cours en affichant les derniers 50 flux.

Si vous appliquez n'importe quel filtre dans l'onglet **Network Activity** ou dans votre critère de recherche avant d'activer le mode de diffusion en flux, les filtres sont maintenus en mode de diffusion en flux. Cependant, le mode de diffusion en flux ne prend pas en charge les recherches qui comprennent les flux groupés. Si vous activez le mode de diffusion en flux sur des flux groupés ou, sur des critères de recherche, l'onglet **Network Activity** affiche les flux normalisés. Voir [Affichage des flux normalisés](#).

Pour afficher les flux de diffusion :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez déjà sauvegardé un critère de recherche pour qu'il soit un critère par défaut, les résultats de ce critère de recherche s'affichent.

Etape 2 A partir de zone de liste **View**, sélectionnez **Real Time (diffusion en flux)**.

Les flux de diffusion s'affichent. Pour obtenir des informations sur les options de la barre d'outils, voir [Tableau 5-1](#). Pour plus d'informations sur les paramètres affichés en mode continu, voir [Tableau 5-3](#).

- Pour sélectionner un enregistrement de flux, cliquez sur l'icône **Pause** pour mettre la diffusion de flux en pause.

Lorsque la diffusion en flux est mise en pause, les derniers 1000 flux s'affichent.

► Pour redémarrer le mode de diffusion en flux, cliquez sur l'icône **Play**.

Affichage des flux normalisés Pour afficher les flux normalisés :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez déjà sauvegardé une recherche en tant que recherche par défaut, les résultats de cette recherche s'affichent.

Etape 2 A partir de la zone de liste **Display**, sélectionnez **Default (Normalisé)**.

Etape 3 A partir de la zone de liste **View**, sélectionnez le cadre de l'heure que vous souhaitez afficher.

REMARQUE

Si vous avez sélectionné un cadre de temps à afficher, un graphique de séries temporelles s'affiche. Pour plus d'informations sur l'utilisation des graphiques de séries temporelles, voir [Affichage des violations associées](#).

L'onglet **Network Activity** affiche les paramètres suivants :

Tableau 5-3 Paramètres de l'onglet Network Activity

Paramètre	Description
Current Filters	En haut du tableau s'affichent les détails des filtres appliqués aux résultats de la recherche. Pour supprimer ces valeurs de filtres, cliquez sur Clear Filter . <i>Remarque : Ce paramètre n'est affiché après avoir appliqué un filtre.</i>
Affichage	A partir de la zone de liste, vous pouvez sélectionner l'intervalle à partir duquel vous souhaitez filtrer.

Tableau 5-3 Paramètres de l'onglet Network Activity (suite)

Paramètre	Description
Current Statistics	<p>Lorsque vous n'êtes pas définis sur le mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours sont affichées, notamment :</p> <p>Remarque : Cliquez sur la flèche suivante de Statistiques en cours pour afficher ou masquer les statistiques.</p> <ul style="list-style-type: none"> • Total Results - Indique le nombre total des résultats correspondant à votre critère de recherche. • Data Files Searched - Indique le nombre total des fichiers de données recherchés pendant l'intervalle de temps. • Compressed Data Files Searched - Indique le nombre total des fichiers de données compressés dans l'intervalle de temps. • Index File Count - Indique le nombre total de fichiers d'indexation recherchés dans l'intervalle de temps. • Duration - Indique la durée de la recherche. <p>Remarque : Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les flux, vous pouvez être invités à fournir les informations de statistiques en cours.</p>
Charts	<p>Affiche les graphiques configurables représentant les enregistrements correspondants par intervalle de temps et option de groupement. Cliquez sur Hide Charts si vous souhaitez supprimer les graphiques de votre affichage.</p> <p>Les graphiques ne sont affichés qu'après avoir sélectionné le cadre de l'heure du dernier intervalle (actualisation automatique) ou au-dessus, et une option de groupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir Affichage des violations associées.</p> <p>Remarque : Si vous utilisez Mozilla Firefox comme navigateur et qu'un bloqueur de publicités est installé, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer le bloqueur de publicités. Pour plus d'informations, voir la documentation du navigateur.</p>
Offense icon	<p>Cliquez sur l'icône Offenses pour voir les détails des actifs associés au flux. Pour plus d'informations, voir Affichage des violations associées.</p>

Tableau 5-3 Paramètres de l'onglet Network Activity (suite)

Paramètre	Description
Flow Type	Indique le type de flux. Les types de flux sont mesurés par le ratio de l'activité entrante vers l'activité sortante. Les types de flux incluent : <ul style="list-style-type: none"> • Standard Flow- Trafic Bidirectionnel • Type A - un-vers-plusieurs (unidirectional), par exemple, un hôte unique effectuant une analyse de réseau. • Type B - plusieurs-vers-un (unidirectional), par exemple, une attaque DoS (DDoS) distribuée. • Type C - un-vers-un (unidirectional), par exemple, un hôte vers une analyse de port d'hôte.
First Packet Time	Indique la date et l'heure où QRadar Network Anomaly Detection reçoit le flux.
Storage time	Indique le temps où le flux a été enregistré sur la base de données de QRadar Network Anomaly Detection.
Source IP	Indique l'adresse IP de la source du flux.
Source port	Indique le port de la source du flux.
Destination IP	Indique l'adresse IP de destination du flux.
Destination port	Indique le port de destination du flux.
Source Bytes	Indique le nombre d'octets envoyés à partir de l'hôte source.
Destination Bytes	Indique le nombre d'octets envoyés à partir de l'hôte de destination.
Total Bytes	Indique le nombre total d'octets associés au flux.
Source Packets	Indique le nombre total de paquets envoyés à partir de l'hôte de la source.
Destination Packets	Indique le nombre total de paquets envoyés à partir de l'hôte de destination.
Total Packets	Indique le nombre total de paquets associés au flux.
Protocol	Indique le protocole associé au flux.
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'application, voir le <i>IBM Security QRadar Guide de configuration d'application</i> .
ICMP Type/Code	Indique le type et le code de Internet Control Message Protocol (ICMP), si applicable. Si le flux est du type ICMP et que les informations du code sont en un format connu, la zone s'affiche en tant que Type <A>, Code où <A> et sont les valeurs numériques du type et du code.
Source Flags	Indique les balises de Transmission Control Protocol(TCP) détectées dans le paquet source, si applicable.
Destination Flags	Indique les balises du TCP détectées dans le paquet de destination, si applicable.

Tableau 5-3 Paramètres de l'onglet Network Activity (suite)

Paramètre	Description
Source QoS	Indique le niveau de service de Quality of service (QoS) du flux. QoS permet au serveur de fournir les différents niveaux de service pour les flux. QoS fournit les différents niveaux des services de base : <ul style="list-style-type: none"> • Best Effort - Ce niveau de service ne garantit pas la livraison. La livraison du flux est considérée comme étant un meilleur effort. • Differenciated Service - Certains flux ont la priorité sur d'autres flux. Cette priorité est accordée en fonction de classification de trafic. • Guaranteed Service - Ce niveau de service garantit la réservation des ressources du réseau pour certains flux.
Destination QoS	Indique le niveau QoS du service pour le flux de destination.
Flow Source	Indique le système qui a détecté le flux. Pour plus d'informations sur les sources de flux, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Flow Interface	Indique l'interface qui reçoit le flux.
Source If Index	Indique le nombre d'index interface (IFIndex) source.
Destination If Index	Indique le nombre de destination d'IFIndex.
Source ASN	Indique les valeurs Autonomous System Number (ASN) source.
Destination ASN	Indique les valeurs ASN de destination.

Etape 4 Faites un double clic sur les flux que vous souhaitez afficher avec plus de détails.

REMARQUE

Si vous affichez les flux en mode de diffusion, vous devez mettre en pause la diffusion en flux avant de double cliquer sur un flux.

La page Flow details fournit les informations suivantes :

Tableau 5-4 Détails de flux

Paramètre	Description
Information sur les flux	
Protocol	Indique le protocole associé à ce flux. Pour plus d'informations sur les protocoles, voir le <i>IBM Security QRadar Guide de configuration d'application</i> .
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'application, voir <i>IBM Security QRadar Guide de configuration d'application</i> .
Magnitude	Indique l'ampleur de ce flux. Pour plus d'informations sur l'ampleur, voir le Glossaire .

Tableau 5-4 Détails de flux (suite)

Paramètre	Description
Relevance	Indique la pertinence de ce flux. Pour plus d'informations sur la pertinence, voir le Glossaire .
Severity	Indique la gravité de ce flux. Pour plus d'informations sur la gravité, voir le Glossaire .
Credibility	Indique la crédibilité de ce flux. Pour plus d'informations sur la crédibilité, voir le Glossaire .
First Packet Time	Indique l'heure de début du flux, telle que reportée à QRadar Network Anomaly Detection par la source du flux. Pour plus d'informations sur les sources de flux, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Last Packet Time	Indique l'heure de fin du flux, telle que reportée à QRadar Network Anomaly Detection par la source du flux. Pour plus d'informations sur les sources de flux, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Storage Time	Indique le temps où le flux a été enregistré sur la base de données de QRadar Network Anomaly Detection.
Event Name	Indique le nom normalisé du flux.
Low Level Category	Indique la catégorie de bas niveau de ce flux. Pour plus d'informations sur les catégories, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Event Description	Indique une description du flux, si disponible.
Informations sur la source et la destination	
Source IP	Indique l'adresse IP de la source du flux.
Destination IP	Indique l'adresse IP de destination du flux.
Source Asset Name	Indique l'actif de la source du flux. Pour plus d'informations sur les actifs, voir Gestion des actifs .
Destination Asset Name	Indique le nom d'actif de destination du flux. Pour plus d'informations sur les actifs, voir Gestion des actifs .
IPv6 Source	Indique l'adresse IPv6 de la source du flux.
IPv6 Destination	Indique l'adresse IPv6 de la destination du flux.
Source port	Indique le port de la source du flux.
Destination port	Indique le port de destination du flux.
Source QoS	Indique le niveau de service flux source.
Destination QoS	Indique le niveau QoS du service pour le flux de destination.
Source ASN	Indique le nombre des valeurs ASN de la source.

Remarque : Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres des valeurs ASN source correspondant sont répertoriés.

Tableau 5-4 Détails de flux (suite)

Paramètre	Description
Destination ASN	Indique le nombre des valeurs ASN de destination. <i>Remarque</i> : Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres des valeurs ASN de destination correspondant sont répertoriés.
Source If Index	Indique le nombre d'IFIndex source. <i>Remarque</i> : Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres d'IFIndex source correspondant sont répertoriés.
Destination If Index	Indique le nombre de destination d'IFIndex. <i>Remarque</i> : Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres d'IFIndex source correspondant sont répertoriés.
Source Payload	Indique le nombre de paquet et d'octets pour le contenu de la source.
Destination Payload	Indique le nombre de paquet et d'octets pour le contenu de destination.
Informations sur le contenu	
Source Payload	Indique le contenu de la source du flux. La zone offre trois formats pour afficher le contenu : <ul style="list-style-type: none"> • Universal Transformation Format (UTF) - Cliquez sur UTF. • Hexidecimal - Cliquez sur HEX. • Base64 - Cliquez Base64. <i>Remarque</i> : Si votre source de flux est Netflow v9 ou IPFIX, des zones non interprétées de ces sources peuvent être affichées dans la zone Source Payload . Le format de cette zone non interprétée est <name>=<value>. Par exemple, MIN_TTL=x .
Destination Payload	Indique le contenu de la destination du flux. La zone offre trois formats pour afficher le contenu : <ul style="list-style-type: none"> • Universal Transformation Format (UTF) - Cliquez sur UTF. • Hexidecimal - Cliquez sur HEX. • Base64 - Cliquez Base64.
Informations supplémentaires	
Flow Type	Indique le type de flux. Les types de flux sont mesurés par le ratio de l'activité entrante vers l'activité sortante. Les types de flux incluent : <ul style="list-style-type: none"> • Standard - trafic bidirectionnel • Type A - Un -vers-plusieurs (unidirectional) • Type B - Plusieurs-vers-un (unidirectional) • Type C - un-vers-un (unidirectional)

Tableau 5-4 Détails de flux (suite)

Paramètre	Description
Flow Direction	Indique la direction du flux. Les directions du flux comprennent : <ul style="list-style-type: none"> • L2L - trafic interne du réseau local vers un autre réseau local. • L2R - Trafic interne d'un réseau local vers un réseau distant. • R2L - Trafic interne d'un réseau distant vers un réseau local. • R2R - Trafic interne d'un réseau distant vers un réseau distant.
Custom Rules	Indique les règles personnalisées qui correspondent à ce flux. Pour plus d'informations sur les règles voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Les règles personnalisées partiellement correspondantes	Indique les règles personnalisées qui correspondent partiellement à ce flux. Pour plus d'informations sur règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .
Source du flux/Interface	Indique le nom de la source du flux du système qui a détecté le flux. Remarque : Si ce flux possède plusieurs enregistrements de diverses sources de flux, les sources de flux correspondantes sont répertoriées.
Annotations	Indique l'annotation ou les notes pour ces flux. Les annotations sont des descriptions de texte que les règles peuvent automatiquement ajouter aux flux dans le cadre de la réponse au flux. Pour plus d'informations sur règles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i> .

La barre d'outils des détails de flux fournit les fonctions suivantes :

Tableau 5-5 Barre d'outils des détails de flux

Fonction	Description
Return to Results	Cliquez sur Return to Results pour retourner à la liste des flux.
Offense	Cliquez sur Offense pour afficher les violations auxquelles le flux est corrélé.
Extract Property	Cliquez sur Extract Property pour créer une propriété de flux personnalisé à partir du flux sélectionné. Pour plus d'informations, voir Utilisation des propriétés de flux personnalisé .
False Positive	Cliquez sur False Positive afin d'ouvrir la fenêtre d'optimisation des faux positifs, qui vous permet d'ajuster les flux connus en tant que faux positifs à partir de la création des violations. Cette option est désactivée en mode de diffusion en flux. Voir Exportation des flux .
Previous	Cliquez sur Previous pour afficher le flux précédent dans la liste d'événements.

Tableau 5-5 Barre d'outils des détails de flux (suite)

Fonction	Description
Next	Cliquez sur Next pour afficher le flux suivant dans la liste d'événements.
Print	Cliquez sur Print pour imprimer les détails d'un flux.

Affichage des flux groupés L'onglet **Network Activity**, vous permet d'afficher les flux groupés par divers options. A partir de la zone de liste **Display**, vous pouvez sélectionner le paramètre par lequel vous souhaitez grouper les flux.

REMARQUE

La zone de liste **Display** ne s'affiche pas en mode diffusion en flux parce que ce mode ne prend pas en charge les flux groupés. Si vous entrez le mode de diffusion en flux à l'aide d'un critère de recherche non groupé, cette option s'affiche.

Pour afficher les flux groupés :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 A partir de la zone de liste **View**, sélectionnez le cadre de temps que vous souhaitez afficher.

REMARQUE

L'affichage des flux groupés n'est pas une option en mode de diffusion en flux.

Etape 3 A partir de la zone de liste **Display**, choisissez l'une des options suivantes :

Tableau 5-6 flux groupés

Option du groupe	Description
Flux unis	Affiche les divers flux dans un seul modèle ininterrompu via des différents intervalles, dans un enregistrement unique. Par exemple, si un flux est de cinq minutes de longueur, le flux uni s'affiche en tant qu'un seul flux de cinq minutes de longueur. Sans le flux uni, le flux s'affiche en tant que cinq flux : un flux pour chaque minute. Les flux unis affichent une liste résumée de flux groupés par informations du flux uni.
Source or Destination IP	Affiche une liste résumée des flux groupés par une adresse IP associée avec le flux.
Source IP	Affiche une liste résumée des flux groupés par une adresse IP source du flux.
Destination IP	Affiche une liste résumée de la liste des flux groupés par adresse IP de destination du flux.

Tableau 5-6 flux groupés (suite)

Option du groupe	Description
Source port	Affiche une liste résumée des flux groupés par le port source du flux.
Destination port	Affiche une liste résumée des flux groupés par port de destination du flux.
Source IP	Affiche une liste résumée des flux groupés par le réseau source du flux.
Destination Network	Affiche une liste résumée des flux groupés par le réseau de destination du flux.
Application	Affiche une liste résumée des flux groupés par l'application d'origine du flux.
Geographic	Affiche une liste résumée des flux groupés par emplacement géographique.
Protocol	Affiche une liste résumée des flux groupés par le protocole associé avec le flux.
Flow Bias	Affiche une liste résumée des flux groupés par la direction du flux.
ICMP Type	Affiche une liste résumée des flux groupés par le type d'ICMP du flux.

L'agencement de colonne des données dépend de l'option de groupe choisie. Chaque ligne dans le tableau de flux représente un groupe de flux. L'onglet **Network Activity** fournit les informations suivantes lors de l'affichage des flux suivantes :

Tableau 5-7 Paramètres de flux groupés

Paramètre	Description
Grouping By	Indique le paramètre sur lequel le paramètre est groupé.
Current Filters	En haut du tableau s'affichent les détails du filtre appliqué aux résultats de la recherche. Pour supprimer ces valeurs de filtres, cliquez sur Clear Filter .
Affichage	A partir de la zone de liste, vous pouvez sélectionner l'intervalle à partir duquel vous souhaitez filtrer.

Tableau 5-7 Paramètres de flux groupés (suite)

Paramètre	Description
Current Statistics	<p>Lorsque vous n'êtes pas définis sur le mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours sont affichées, notamment :</p> <p>Remarque : Cliquez sur la flèche suivante de Statistiques en cours pour afficher ou masquer les statistiques.</p> <ul style="list-style-type: none"> • Total Results - Indique le nombre total des résultats correspondant à votre critère de recherche. • Data Files Searched - Indique le nombre total des fichiers de données recherchés pendant l'intervalle de temps. • Compressed Data Files Searched - Indique le nombre total des fichiers de données compressés dans l'intervalle de temps. • Index File Count - Indique le nombre total de fichiers d'indexation recherchés dans l'intervalle de temps. • Duration - Indique la durée de la recherche. <p>Remarque : Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les flux, vous pouvez être invités à fournir les informations de statistiques en cours.</p>
Charts	<p>Affiche les graphiques configurables représentant les enregistrements correspondants par intervalle de temps et option de groupement. Cliquez sur Hide Charts si vous souhaitez supprimer les graphiques de votre affichage.</p> <p>Les graphiques ne sont affichés qu'après avoir sélectionné le cadre de l'heure du dernier intervalle (actualisation automatique) ou au-dessus, et une option de groupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir Affichage des violations associées.</p> <p>Remarque : Si vous utilisez Mozilla Firefox comme navigateur et qu'un bloqueur de publicités est installé, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer le bloqueur de publicités. Pour plus d'informations, voir la documentation du navigateur.</p>
Source IP (Unique Count)	Indique l'adresse IP de la source du flux.
Destination IP (Unique Count)	Indique l'adresse IP de destination du flux. S'il existe plusieurs adresses IP de destination associées à ce flux, cette zone indique les divers termes et leur nombre d'adresses IP.
Source Port (Unique Count)	Indique le port de source du flux.

Tableau 5-7 Paramètres de flux groupés (suite)

Paramètre	Description
Destination Port (Unique Count)	Indique le port de destination du flux. S'il existe plusieurs ports de destination associés à ce flux, cette zone indique les divers termes et le nombre des ports.
Source Network (Unique Count)	Indique le réseau de la source du flux. S'il existe plusieurs réseaux source associés au flux, cette zone indique le terme et le nombre de réseaux.
Destination Network (Unique Count)	Indique le port de destination du flux. S'il existe plusieurs réseaux de destination associés au flux, cette zone indique le terme et le nombre de réseaux.
Application (Unique Count)	Indique l'application détectée des flux. S'il existe multiple applications associées à ce flux, cette zone indique le terme et le nombre d'applications.
Total Bytes (Sum)	Indique le nombre total d'octets associés au flux.
Source Bytes (Sum)	Indique le nombre d'octets de la source.
Destination Bytes (Sum)	Indique le nombre d'octets de la destination.
Source Packets (Sum)	Indique le nombre de paquets de la source.
Destination Packets (Sum)	Indique le nombre de paquets de la destination.
Total Packets	Indique le nombre total de paquets associés au flux.
Count	Indique le nombre de flux envoyés ou reçus.

Etape 4 Faites un double-clic sur le groupe de flux que vous souhaitez étudier.

La page Flows List affiche les flux appartenant au groupe sélectionné.

Pour plus d'informations sur les paramètres Flows List, voir [Tableau 5-3](#).

Etape 5 Faites un double-clic sur le flux que vous souhaitez étudier.

Pour plus d'informations sur la page Flow details, voir [Tableau 5-4](#). Pour plus d'informations sur la barre d'outils Flow details, voir [Tableau 5-5](#).

Affichage des violations associées

si un flux correspond à un rôle, une violation peut être générée dans l'onglet **Offenses**. Dans l'onglet **Network Activity**, vous pouvez afficher les violations associées au flux en cliquant sur l'icône **Offense** du flux correspondant. Pour plus d'informations sur les règles, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*. Pour plus d'informations sur la gestion des infractions, voir [Etudes des offenses](#).

Pour afficher une violation associée :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

REMARQUE

Si vous affichez les flux en mode de diffusion, vous devez mettre en pause la diffusion en flux avant d'étudier un flux.

Etape 2 Cliquez sur l'icône **Offense** en regard du flux que vous souhaitez étudier.

Si le Magistrat n'a pas encore enregistré la violation associée au flux sélectionné sur le disque ou si la violation a été purgée de la base de données, un message d'information s'affiche.

Pour plus d'informations sur la gestion des infractions [Etudes des offenses](#)

Utilisation des propriétés de flux personnalisé

La fonctionnalité Custom Flow Properties vous permet de rechercher, afficher et rapporter les informations au sein des flux que QRadar Network Anomaly Detection ne normalise et n'affiche pas typiquement.

REMARQUE

Pour créer des fonctionnalités de flux personnalisé, vous devez avoir des droits de propriété de flux personnalisé. Vérifiez avec votre administrateur pour assurer que vous possédez les droits requis. Pour plus d'informations sur les droites, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Vous pouvez créer des propriétés de flux personnalisé à partir de deux emplacements dans l'onglet **Network Activity** :

- **Flow details** - Sélectionnez un flux à partir de l'onglet **Network Activity** pour créer une propriété de flux dérivée du contenu.
- **Search page** - Vous pouvez créer et éditer une propriété de flux personnalisé de la page de recherche. Lorsque vous créez une nouvelle propriété de flux personnalisé à partir de la page de recherche, la propriété de flux n'est pas dérivée d'un flux particulier ; par conséquent la fenêtre Flow Properties Definition n'est pas préremplie. Vous pouvez copier et coller le contenu des informations à partir d'une autre source.

REMARQUE

Si vous possédez des droits d'administration, vous pouvez également créer et modifier les propriétés de flux personnalisé à partir de l'onglet **Admin**.

Cette section comprend les rubriques suivantes :

- [Création d'une propriété de flux personnalisé](#)
- [Modifier une propriété de flux personnalisé](#)
- [Copier une propriété de flux personnalisé](#)

- **Supprimer une propriété de flux personnalisé**

Création d'une propriété de flux personnalisé

A l'aide de la fonctionnalité propriété de flux personnalisé, vous pouvez créer deux types de propriétés de flux personnalisé :

- **Regex** - Instruction sur l'utilisation des expressions régulières (Regex), vous pouvez extraire des données non normalisées du contenu du flux.

L'utilisation de ce flux nécessite une connaissance avancée des instructions regex. Regex définit la zone que vous souhaitez définir en tant que propriété de flux personnalisé. Après avoir entré une instruction regex, vous pouvez la valider contre le contenu. Lorsque vous définissez des modèles regex, adhérez à des règles regex telles que définies par la programmation Java™ language. Pour plus d'informations, vous pouvez vous référer aux didacticiels regex disponible sur le Web.

Une propriété de flux personnalisé peut être associée aux différentes expressions régulières. Lorsqu'un flux est tracé, chaque modèle de regex est testé sur le flux jusqu'à ce que les modèles correspondent au contenu. Le premier modèle de regex à correspondre au contenu du flux détermine les données à extraire.

- **Calculated** - l'utilisation des propriétés de flux personnalisé en fonction du calcul, vous pouvez effectuer un calcul sur les propriétés de flux numérique existantes pour procédez au calcul de la propriété. Par exemple, vous pouvez créer une propriété qui affiche un pourcentage en divisant une propriété numérique par une autre propriété numérique.

Cette section comprend les rubriques suivantes :

- **Création d'une propriété de flux personnalisé en fonction de Regex.**
- **Création d'une propriété de flux personnalisé basée sur le calcul**

Création d'une propriété de flux personnalisé en fonction de Regex.

Une propriété de flux personnalisé basée sur regex correspond aux contenus du flux pour une expression régulière.

Pour créer une propriété de flux personnalisé en fonction d'une expression régulière :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Faites un double-clic sur le flux sur lequel vous souhaitez baser la propriété de flux personnalisé.**REMARQUE**

Si vous affichez les flux en mode de diffusion, vous devez mettre en pause la diffusion en flux avant de double cliquer sur un flux.

Etape 3 Cliquez sur **Extract Property**.**REMARQUE**

Si vous possédez des droits d'administration, vous pouvez accéder à la fenêtre des propriétés de flux personnalisé sur l'onglet **Admin**. Cliquez sur **Admin > Data Sources > Custom Flow Properties**. Pour plus d'informations, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Etape 4 Dans le panneau Property Type, sélectionnez l'option **Regex Based**.**Etape 5** Configurez les paramètres de propriété de flux personnalisé :**Tableau 5-8** Paramètres de la fenêtre Custom Flow Properties

Paramètre	Description
Test Field	Indique le contenu extrait du flux non normalisé.
Définition de la propriété	
Définition de la propriété	Pour sélectionner une propriété existante, sélectionnez cette option, ensuite sélectionnez un nom de propriété déjà sauvegardé de la zone de liste.
New Property	Pour créer une nouvelle propriété, sélectionnez cette option, ensuite entrez un nom unique pour cette propriété de flux personnalisé. La nouvelle propriété ne peut pas être le nom de la propriété du flux normalisé

Tableau 5-8 Paramètres de la fenêtre Custom Flow Properties (suite)

Paramètre	Description
Optimisez l'analyse syntaxique pour les règles, les rapports et les recherches	<p>Pour analyser et stocker la propriété la première fois que QRadar Network Anomaly Detection reçoit le flux, sélectionnez la case à cocher. Lorsque vous sélectionnez la case à cocher, la propriété ne nécessite pas une analyse supplémentaire pour le test de rapport, de recherche et de règle.</p> <p>Si vous désélectionnez cette case à cocher, la propriété est analysée à chaque fois le teste de rapport de recherche ou de règle est effectué.</p> <p>Cette option est désactivée par défaut.</p>
Field Type	<p>A partir de cette zone de liste, sélectionnez le type de la zone. Le type de zone détermine comment une propriété de flux personnalisé est affichée dans QRadar Network Anomaly Detection and et les options disponibles pour agrégation. Les options du type de zone sont :</p> <ul style="list-style-type: none"> • Alpha-Numeric • Numeric • IP • Port <p>L'option par défaut est Alpha-Numeric.</p>
Description	Entrez une description de cette propriété de flux personnalisé.
Définition de l'expression propriété	
Event Name	<p>Pour indiquer un nom d'événement pour lequel vous souhaitez appliquer une propriété de flux, sélectionnez cette option.</p> <p>Cliquez sur Browse pour accéder au navigateur d'événement et sélectionnez l'identificateur de QRadar (QID) pour le nom d'événement que vous souhaitez appliquer à cette propriété de flux personnalisé</p> <p>Cette option est activée par défaut</p>
Category	<p>Pour spécifier une catégorie de bas niveau pour laquelle s'applique cette propriété de flux personnalisé, sélectionnez cette option.</p> <p>Pour sélectionner une catégorie de bas niveau :</p> <ol style="list-style-type: none"> 1 A partir de la zone de liste High Level Category sélectionnez la catégorie bas niveau. La liste Low Level Category se met à jour pour inclure uniquement les catégories associées avec la catégorie haut niveau sélectionnée. 2 A partir de la zone de liste Low Level Category sélectionnez la catégorie bas niveau pour laquelle cette propriété de flux personnalisé s'applique.

Tableau 5-8 Paramètres de la fenêtre Custom Flow Properties (suite)

Paramètre	Description
RegEx	<p>Entrez l'expression régulière que vous souhaitez utiliser pour extraire les données du contenu. Les expressions régulières sont sensibles à la casse.</p> <p>Echantillon d'expressions régulières :</p> <ul style="list-style-type: none"> • email : <code>(.+@[^\.]*\.[a-z]{2,})\$</code> • URL : <code>(http\:\/\/[a-zA-Z0-9\-\.\.]+\.[a-zA-Z]{2,3}(\/*s*)?\$)</code> • Domain Name : <code>(http[s]?:\/\/(.*?)["/?:])</code> • Floating Point Number : <code>([-+]?\d*\.\d*\$)</code> • Integer : <code>([-+]?\d*\$)</code> • IP Address : <code>(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)</code> <p>Par exemple : pour correspondre un flux qui ressemble aux suivantes :</p> <p><code>SEVERITY=43</code> Rédigez les expressions régulières comme suit : <code>SEVERITY=([-+]?\d*\$)</code></p> <p>Remarque : Les groupes de capture doivent être mis entre parenthèses.</p>
Capture Group	<p>Entrez les groupes de capture que vous souhaitez utiliser si regex contient plus d'un seul groupe de capture.</p> <p>Les groupes de capture traitent les divers caractères comme étant une seule unité. Dans un groupe de capture, les caractères sont regroupés entre parenthèses.</p>
Test	<p>Cliquez sur Test pour tester l'expression régulière contre le contenu.</p>
Enabled	<p>Sélectionnez cette case à cocher pour activer cette propriété de flux personnalisé. Si vous supprimez cette case à cocher, cette propriété de flux personnalisé ne s'affiche pas dans les filtres de recherche de flux ou la propriété du flux n'est pas analysée à partir des contenus.</p> <p>Ce paramètre est activé par défaut.</p>

Etape 6 Cliquez sur **Test** pour tester les expressions régulières à l'encontre du contenu.

Etape 7 Cliquez sur **Save**.

La propriété du flux personnalisée s'affiche en tant qu'option dans la liste des colonnes sur la page de recherche.

REMARQUE

Les propriétés de flux personnalisé ne sont automatiquement incluses dans les énumérations de flux. Afin d'inclure une propriété de flux personnalisé dans la

liste des flux, vous devez sélectionner la propriété de flux personnalisé à partir de la liste des colonnes disponibles lors de la création d'une recherche.

Création d'une propriété de flux personnalisé basée sur le calcul

Pour créer une propriété de flux personnalisé basé sur le calcul :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Faites un double-clic sur le flux sur lequel vous souhaitez baser la propriété de flux personnalisé.

REMARQUE

Si vous affichez les flux en mode de diffusion, vous devez mettre en pause la diffusion en flux avant de double cliquer sur un flux.

Etape 3 Cliquez sur **Extract Property**.

REMARQUE

Si vous possédez des droits d'administration, vous pouvez accéder à la fenêtre des propriétés de flux personnalisé sur l'onglet **Admin**. Cliquez sur **Admin > Data Sources > Custom Flow Properties**. Pour plus d'informations, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Etape 4 Dans le panneau Property Type, sélectionnez l'option **Calculation Based**.

Etape 5 Configurez les paramètres de propriété de flux personnalisé :

Tableau 5-9 Paramètres de la fenêtre Custom Flow Properties

Paramètre	Description
Définition de la propriété	
Property Name	Entrez un nom unique pour cette propriété de flux personnalisé. Le nouveau nom de la propriété ne peut pas être le nom d'une propriété de flux normalisé.
Description	Entrez une description de cette propriété de flux personnalisé.
Définition de Property Calculation	
Property 1	A partir de la zone de liste, sélectionnez la première propriété que vous souhaitez utiliser lors de votre calcul. Les options incluent toutes les propriétés de flux personnalisés et normalisés numériques. Vous pouvez également indiquer les valeurs numériques spécifiques. A partir de la zone de liste de Property 1 , sélectionnez l'option User Defined . Le paramètre Numeric Property s'affiche. Entrez une valeur numérique spécifique.

Tableau 5-9 Paramètres de la fenêtre Custom Flow Properties (suite)

Paramètre	Description
Operator	A partir de la zone de liste, sélectionnez l'opérateur que vous souhaitez appliquer à la propriété sélectionnée dans le calcul. Les options comprennent : <ul style="list-style-type: none"> • Add • Subtract • Multiply • Divide
Property 2	A partir de la zone de liste, sélectionnez la seconde propriété que vous souhaitez utiliser lors de votre calcul. Les options incluent toutes les propriétés de flux personnalisés et normalisés numériques. Vous pouvez également indiquer les valeurs numériques spécifiques. A partir de la zone de liste de Property 1 , sélectionnez l'option User Defined . Le paramètre Numeric Property s'affiche. Entrez une valeur numérique spécifique.
Enabled	Sélectionnez cette case à cocher pour activer cette propriété de flux personnalisé. Si vous supprimez cette case à cocher, cette propriété de flux personnalisé ne s'affiche pas dans les filtres de recherche de flux ou la propriété du flux n'est pas analysée à partir des contenus. Ce paramètre est activé par défaut.

Etape 6 Cliquez sur **Save**.

La propriété du flux personnalisé s'affiche en tant qu'option dans la liste des colonnes sur la page de recherche.

REMARQUE

Les propriétés de flux personnalisé ne sont automatiquement incluses dans les énumérations de flux. Afin d'inclure une propriété de flux personnalisé dans une liste des flux, vous devez sélectionner la propriété de flux personnalisé à partir de la liste des colonnes disponibles lors de la création d'une recherche.

Modifier une propriété de flux personnalisé

Pour modifier une propriété de flux personnalisé :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Dans la zone de liste **Search**, sélectionnez **Edit Search**.

Etape 3 Cliquez sur **Manage Custom Properties**.

La fenêtre Custom Flow Properties fournit les informations suivantes :

Tableau 5-10 Colonnes de Custom Flow Property

Column	Description
Property Name	Indique un seul nom pour cette propriété de flux personnalisé
Property Description	Indique une description pour cette propriété de flux personnalisé.
Test Field	Indique si la zone de teste est un contenu de source ou de destination.
Regular Expression	Indique l'expression régulière que vous souhaitez utiliser pour l'extraction des données à partir du contenu.
Username	Indique le nom de l'utilisateur qui a créé cette propriété de flux personnalisé.
Enabled	Indique si cette propriété de flux est activée. Cette zone indique vrai ou faux
Creation Date	Indique la date de création de la propriété de flux personnalisé.
Modification Date	Indique la date de la dernière modification de la propriété de flux personnalisé

La barre d'outils Custom Flow Property fournit les fonctions suivantes :

Tableau 5-11 Options de barre d'outils de Custom Flow Property

Option	Description
Add	Cliquez sur Add pour ajouter une nouvelle propriété de flux personnalisé. Voir Création d'une propriété de flux personnalisé .
Edit	Cliquez sur Edit pour éditer la propriété de flux personnalisé sélectionnée. Voir Etape 4 .
Copy	Cliquez sur Copy pour copier les propriétés de flux personnalisé
Delete	Cliquez sur Delete pour supprimer les propriétés de flux personnalisés.
Activer/Désactiver	Cliquez sur Enable/Disable pour activer ou désactiver les propriétés de flux personnalisé pour l'analyse et l'affichage dans des listes de colonne ou des filtres de recherche.

Etape 4 Sélectionnez la propriété de flux personnalisé que vous souhaitez éditer et cliquez sur **Edit**.

REMARQUE

Vous pouvez également cliquer sur la propriété de flux personnalisé que vous souhaitez éditer.

Etape 5 Editez les paramètres nécessaires. Voir [Tableau 5-8](#).

Etape 6 Si vous avez édité l'expression régulière, cliquez sur **Test** pour tester l'expression régulière à l'encontre du contenu.

Etape 7 Cliquez sur **Save**.

La propriété du flux personnalisé est maintenant mise à jour dans la liste des colonnes disponibles sur la page de recherche.

REMARQUE

Les propriétés de flux personnalisé ne sont automatiquement incluses dans les énumérations de flux. Afin d'inclure une propriété de flux personnalisé dans une liste des flux, vous devez sélectionner la propriété de flux personnalisé à partir de la liste des colonnes disponibles lors de la création d'une recherche.

Copier une propriété de flux personnalisé

Pour copier une propriété de flux :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Dans la zone de liste **Search**, sélectionnez **Edit Search**.

Etape 3 Cliquez sur **Manage Custom Properties**.

Etape 4 Sélectionnez la propriété de flux que vous souhaitez copier et cliquez sur **Copy**.

Etape 5 Sélectionnez l'option **New Property** et entrez le nom d'une nouvelle propriété.

Etape 6 Editez les paramètres nécessaires. Voir [Tableau 5-8](#).

Etape 7 Si vous avez édité l'expression régulière, cliquez sur **Test** pour tester l'expression régulière à l'encontre du contenu.

Etape 8 Cliquez sur **Save**.

La propriété de flux personnalisé est maintenant disponible dans la liste des colonnes disponibles sur la page de recherche.

REMARQUE

Les propriétés de flux personnalisé ne sont automatiquement incluses dans les énumérations de flux. Afin d'inclure une propriété de flux personnalisé dans une liste des flux, vous devez sélectionner la propriété de flux personnalisé à partir de la liste des colonnes disponibles lors de la création d'une recherche.

Supprimer une propriété de flux personnalisé

Vous pouvez supprimer n'importe quelle propriété personnalisée, une propriété personnalisée n'est pas associée avec une autre propriété personnalisée. Si vous tentez de supprimer une propriété personnalisée associée avec une autre propriété personnalisée, un message d'erreur s'affiche, fournissant le nom de la propriété personnalisée associée.

Pour supprimer une propriété de flux personnalisée :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Dans la zone de liste **Search**, sélectionnez **Edit Search**.

Etape 3 Cliquez sur **Manage Custom Properties**.

Etape 4 Sélectionnez la propriété de flux personnalisé que vous souhaitez supprimer et cliquez sur **Delete**.

Etape 5 Cliquez sur **Oui**.

La propriété de flux personnalisé supprimée n'affiche plus les détails du flux.

Réglage des faux Positifs

Vous ne pouvez pas utiliser la fonction False Positive Tuning pour régler les flux des faux positifs à partir des violations créées. Vous devez avoir des droits appropriés pour la création des règles personnalisées afin de régler les faux positifs. Pour plus d'informations sur les rôles, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*. Pour plus d'informations sur les faux positifs, voir le [Glossaire](#).

Pour régler un flux des faux positifs :

Etape 1 Cliquez sur l'onglet **Network Activity**.

Etape 2 Sélectionnez le flux que vous souhaitez régler.

Etape 3 Cliquez sur **False Positive**.

REMARQUE

Si vous affichez les flux en mode de diffusion, vous devez mettre le mode de diffusion en pause avant de cliquer sur **False Positive**.

La fenêtre False Positive s'affiche fournissant les informations dérivées du flux sélectionné.

Etape 4 Sélectionnez les options suivantes :

- Event/Flow(s) with a specific QID of <Event>
- Any Event/Flow(s) with a low-level category of <Event>
- Any Event/Flow(s) with a high-level category of <Event>

Etape 5 Sélectionnez l'une ses options de direction de trafic suivantes :

- <Source IP Address> to <Destination IP Address>
- <Source IP Address> to Any Destination
- Any Source to <Destination IP Address>
- Any Source to any Destination

Etape 6 Cliquez sur **Tune**.

REMARQUE

Vous pouvez régler les flux des faux positifs à partir de la page des détails.

Exportation des flux

Vous pouvez exporter les flux en format XML ou en format CSV. Le fichier résultant XML ou CSV contient les paramètres spécifiés dans le panneau Column Definition de vos paramètres de recherche. La durée nécessaire pour exporter vos données dépend du nombre de paramètres spécifiés.

Pour exporter les flux :

Etape 1 Cliquez sur l'onglet **Network Activity**.

REMARQUE

Si vous affichez les flux en mode de diffusion, vous devez mettre en pause la diffusion avant d'exporter les informations du flux.

Etape 2 Sélectionnez l'une des options suivantes :

- Si vous souhaitez exporter les flux au format XML, sélectionnez **Export to XML** dans la zone de liste **Actions**.
- Si vous souhaitez exporter les flux au format CSV, sélectionnez **Export to CSV** dans la zone de liste **Actions**.

Lorsque l'exportation est terminée, vous recevez une notification vous informant que l'exportation est terminée. Si vous n'avez pas sélectionné l'icône **Notify When Done**, la fenêtre d'état s'affiche.

6

UTILISATION DE LA FONCTION GRAPHIQUE

A l'aide de la fonction Chart sur les onglets **Log Activity** et **Network Activity**, vous pouvez afficher vos données à l'aide des options de configuration de graphique.

Cette section comprend les rubriques suivantes :

- [Présentation de la fonction Graphique](#)
- [Légendes de graphiques](#)
- [Configuration des graphiques](#)
- [Gestion des graphiques de séries temporelles](#)

Présentation de la fonction Graphique

Si vous sélectionnez un cadre de temps ou une option de groupement pour afficher vos données, les graphiques s'affichent sur les onglets **Log Activity** et **Network Activity**. Les types de graphiques sont : barre, graphique circulaire, table et séries temporelles. Les graphiques sont configurables, ce qui vous permet de sélectionner les données que vous voulez tracer dans le graphique. Vous pouvez configurer des graphiques indépendamment les uns des autres pour afficher vos résultats de recherche à partir de différentes perspectives.

REMARQUE

Vous devez disposer des autorisations appropriées pour gérer et afficher des graphiques de séries temporelles. Pour plus d'informations sur les autorisations des rôles, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration IBM Security*.

Après avoir configuré un graphique, vos configurations de graphique sont conservées lorsque vous :

- Changez votre affichage d'événement à l'aide de la zone de liste **Display**.
- Appliquez un filtre.
- Enregistrez votre critère de recherche.

Vos configurations de graphique ne seront pas conservées lorsque vous :

- Démarrez une nouvelle recherche.
- Accédez à une recherche rapide.

- Affichez les résultats groupés dans une fenêtre de branche.
- Sauvegardez vos résultats de recherche.

REMARQUE

Si vous utilisez Mozilla Firefox comme navigateur et qu'un bloqueur de publicités est installé, les graphiques ne s'affichent pas. Pour afficher des graphiques, vous devez supprimer le bloqueur de publicités. Pour plus d'informations, voir la documentation de votre navigateur.

Légendes de graphiques

Chaque graphique fournit une légende, qui correspond à une référence visuelle pour vous aider à associer les objets des graphiques aux paramètres qu'ils représentent. En utilisant la fonctionnalité de légende, vous pouvez effectuer les actions suivantes :

- Déplacez le pointeur de votre souris sur un élément de la légende ou le bloc de couleur de la légende pour afficher plus d'informations sur les paramètres qu'il représente.
- Cliquez avec le bouton droit de la souris sur l'élément de légende afin d'étudier davantage ce dernier. Pour plus d'informations sur les options du menu contextuel, voir [A propos de la détection des anomalies du réseau IBM Sécurité Qradar](#).
- Cliquez sur un élément de graphique circulaire, à barre ou tableau pour masquer l'élément dans le graphique. Cliquez sur l'élément de légende de nouveau pour masquer l'élément masqué. Vous pouvez également cliquer sur l'élément de graphique correspondant pour masquer et afficher l'élément.
- Cliquez sur **Legend**, ou sur la flèche d'à côté, si vous souhaitez supprimer la légende de votre affichage de graphique.

Configuration des graphiques

Pour configurer un graphique :

Etape 1 Cliquez l'onglet **Log Activity** ou **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

Etape 2 Effectuez une recherche groupée. Voir [Recherche d'événements ou flux](#).

Les graphiques et la liste des événements sont affichés.

Etape 3 Cliquez sur **Save Criteria** sur la barre d'outils.

Etape 4 Dans le panneau Charts, cliquez sur l'icône **Configure**.

Les options de configuration s'affichent.

Etape 5 Configurez les paramètres suivants :

Tableau 6-1 Paramètres du Menu Graphique

Paramètres	Description
Value to Graph	<p>Dans la zone de liste, sélectionnez le type d'objet que vous souhaitez tracer sur l'axe Y du graphique. Les options comprennent tous les paramètres d'événements normalisés et personnalisés ou de flux inclus dans vos paramètres de recherche.</p> <p>Remarque : QRadar Network Anomaly Detection peut accumuler des données de sorte que lorsque vous effectuez une recherche de séries temporelles, un cache de données d'événement soit disponible à l'affichage des données pour la période précédente. Après avoir activé le temps de capture de données de séries temporelles pour un paramètre sélectionné, un astérisque (*) est affiché en regard du paramètre dans la zone de liste Value to Graph.</p>
Display Top	<p>A partir de la zone de liste, sélectionnez le nombre d'objectifs que vous souhaitez afficher dans le graphique. Les options comprennent les valeurs 5, 10 et 20. La valeur par défaut est 10.</p> <p>Remarque : Si plus de 10 éléments sont tracés, vos données risquent d'être illisibles.</p>
Chart Type	<p>Dans la zone de liste, sélectionnez le type de graphique que vous souhaitez afficher. Ces options incluent :</p> <ul style="list-style-type: none"> • Bar Chart - Affiche les données dans un graphique à barres. Cette option est uniquement disponible pour les événements groupés. • Pie Chart - Affiche les données dans un graphique circulaire. Cette option est uniquement disponible pour les événements groupés. • Table - Affiche les données dans un tableau. Cette option est uniquement disponible pour les événements groupés. <p>Remarque : Si votre graphique à barres, circulaire ou tableau repose sur des critères de recherche enregistrés avec un intervalle de plus d'une heure, vous devez cliquer sur Update Details pour mettre à jour le graphique et remplir les détails d'événement.</p> <ul style="list-style-type: none"> • Time Series - Affiche un graphique en ligne interactif représentant les enregistrements correspondant par intervalle de temps spécifique. Pour plus d'informations sur la configuration des critères de recherche de séries temporelles, voir Gestion des graphiques de séries temporelles. <p>Remarque : Vous devez posséder les permissions de rôle appropriés pour gérer et afficher les graphiques de séries temporelles. Pour plus d'informations sur les autorisations des rôles, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>.</p>

Tableau 6-1 Paramètres du Menu Graphique (suite)

Paramètres	Description
Capture Time Series Data	Sélectionnez cette case à cocher si vous souhaitez activer la capture des données de séries temporelles. Lorsque vous activez cette case à cocher, la fonction de graphique commence à accumuler des données pour les graphiques de séries temporelles. Cette option est désactivée par défaut. <i>Remarque : Cette option est uniquement disponible sur les graphiques de séries temporelles.</i>
Time Range	Dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez afficher. <i>Remarque : Cette option est uniquement disponible sur les graphiques de séries temporelles.</i>

REMARQUE

Pour démarrer une accumulation des données pour votre graphique de séries temporelles, vous devez sauvegarder votre critère de recherche. Cette action démarre l'accumulation de données et votre graphique de séries temporelles est affiché. Configuration d'un graphique à barres, graphique circulaire ou tableau qui ne vous oblige pas à enregistrer vos options de configuration. Le graphique s'actualise automatiquement.

Etape 6 Pour afficher la liste des événements, si votre plage horaire est supérieure à 1 heure, cliquez sur **Update Details**.

Les graphiques de séries temporelles ont des options supplémentaires de configuration et de navigation. Pour plus d'informations sur l'utilisation des graphiques de séries temporelles, voir [Gestion des graphiques de séries temporelles](#).

Gestion des graphiques de séries temporelles

Les graphiques de séries temporelles sont des représentations graphiques de votre journal ou activité de réseau au fil du temps. Les sommets et les creux affichés dans les graphiques indiquent l'activité de volume élevé et bas. Les graphiques de séries temporelles sont utiles pour les tendances de données de court et long terme. A l'aide des graphiques de séries temporelles, vous pouvez accéder, naviguer et enquêter sur le journal ou l'activité de réseau à partir des divers affichages et perspectives.

REMARQUE

Vous devez disposer des autorisations appropriées pour gérer et afficher des graphiques de séries temporelles. Pour plus d'informations sur les autorisations de rôle, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Pour afficher les graphiques de séries temporelles, vous devez créer et enregistrer une recherche qui inclut des séries temporelles et les options de regroupement. QRadar Network Anomaly Detection comprend, par défaut, les recherches

sauvegardées des séries temporelles, auxquelles vous pouvez accéder à partir des recherches sauvegardées disponibles sur la page de recherche de flux. Vous pouvez facilement identifier les recherches des séries temporelles enregistrées sur le menu **Quick Searches**, parce que le nom de la recherche est ajouté à la plage de temps spécifiée dans les critères de recherche.

Si vos paramètres de recherche correspondent à une recherche déjà sauvegardée pour les options de groupement et de définition, un graphique de séries temporelles peut s'afficher automatiquement pour vos résultats de recherche. Si un graphique de séries temporelles ne s'affiche pas automatiquement pour votre critère de recherche non sauvegardée, aucune recherche sauvegardée n'existe pour correspondre à vos paramètres de recherche. Si cela se produit, vous devez activer la capture des données de séries temporelles et sauvegarder votre critère de recherche.

Cette section comprend les rubriques suivantes :

- [Création des recherches de séries temporelles](#)
- [Gestion des graphiques de séries temporelles](#)
- [Navigation des graphiques de séries temporelles](#)

Création des recherches de séries temporelles

Nous recommandons de planifier votre recherche de séries temporelles selon les données que vous souhaitez étudier et comment voulez vous afficher les données dans votre graphique de séries temporelles. Par exemple, envisagez comment vous souhaitez grouper la recherche, les colonnes que vous souhaitez afficher et les filtres que vous souhaitez appliquer.

REMARQUE

QRadar Network Anomaly Detection prend en charge jusqu'à 100 recherches de séries temporelles.

Pour créer une recherche de séries temporelles :

Etape 1 Cliquez sur l'onglet **Log Activity** ou **Network Activity**.

Si vous avez enregistré précédemment une recherche par défaut, les résultats pour cette recherche enregistrée s'affichent.

REMARQUE

Les graphiques ne s'affichent en mode de diffusion.

Etape 2 Configurez vos paramètres de recherche de séries temporelles. Choisissez l'une des opérations suivantes :

- Cliquez sur **Search > New Search** pour créer une recherche, en vous assurant que la recherche est groupée et qu'elle spécifie un intervalle de temps. Voir [Recherche d'événements ou flux](#).
- A partir des zones de listes **Display** et **View**, sélectionnez un cadre de temps et un paramètre sur lequel vous souhaitez grouper vos résultats.

Les résultats de votre recherche sont affichés, offrant deux graphiques : un graphique à barres et un graphique circulaire.

Etape 3 Sauvegardez votre critère de recherche. Choisissez l'une des opérations suivantes :

- Sur la barre d'outils Log Activity ou Network Activity, cliquez sur **Save Criteria**. Voir [Sauvegarde des critères de recherche](#).
- Dans le volet Chart Configuration, cliquez sur l'icône **Save**.

REMARQUE

La sauvegarde de votre critère de recherche active QRadar Network Anomaly Detection pour démarrer l'accumulation de vos données nécessaires pour votre graphique de séries temporelles.

Etape 4 Configurez un ou deux graphiques en sorte qu'il soit des graphiques de séries temporelles :

- a Cliquez sur l'icône **Configure**.
- b Dans la zone de liste **Chart Type**, sélectionnez **Time Series**.
- c Dans la zone de liste **Value to Graph**, sélectionnez le paramètre que vous souhaitez tracer.
- d Cochez la case **Capture Time Series Data**.
- e Cliquez sur **Save**.

Etape 5 Pour afficher la liste des événements ou flux si votre plage horaire est supérieure à 1 heure, cliquez sur **Update Details**.

La liste d'événements ou flux se met à jour pour afficher le journal ou l'activité de réseau en fonction de de la configuration du graphique de séries temporelles.

Navigation des graphiques de séries temporelles

A l'aide des graphiques de séries temporelles, vous pouvez agrandir et balayer une ligne de temps pour étudier l'activité du journal ou du réseau. Le tableau

suisant fournit des fonctions vous permettant d'afficher des graphiques de séries temporelles, notamment :

Tableau 6-2 Fonctions de graphiques de séries temporelles

Si vous souhaitez...	Alors...
Afficher les données avec plus de détails	<p>À l'aide de la fonction zoom, vous pouvez étudier les plus petites tranches horaires du trafic de l'événement.</p> <ul style="list-style-type: none"> Placez le pointeur de votre souris sur le graphique, ensuite, utilisez la roulette de votre souris pour agrandir le graphique (roulez la roulette de la souris vers le haut). Surlignez la zone de votre graphique que vous souhaitez agrandir. Lorsque vous relâchez le bouton de votre souris, le graphique affiche un segment de temps plus petit. Maintenant, cliquez et glissez le graphique pour l'analyser. <p>Lorsque vous agrandissez un graphique de séries temporelles, le graphique s'actualise pour afficher un segment de temps plus petit.</p>
Afficher un intervalle de temps de données plus large	<p>La fonctionnalité zoom vous permet d'étudier les segments de temps les plus grands ou retourner à l'intervalle maximal. Vous pouvez étendre un intervalle de temps en utilisant l'une des options suivantes :</p> <ul style="list-style-type: none"> Cliquez sur Zoom Reset au coin supérieur gauche du graphique. Déplacez le pointeur de votre souris sur le graphique, ensuite utilisez la roulette de la souris pour agrandir l'affichage (roulez la roulette de la souris vers le bas).
Analyser le graphique	<p>Lorsque vous avez amplifié un graphique de séries temporelles, vous pouvez :</p> <ul style="list-style-type: none"> ► Cliquez et faites glisser le graphique à gauche ou à droite pour analyser la ligne de temps.

7

RECHERCHE DE DONNÉES

La fonction de recherche vous permet de rechercher des données en utilisant des critères spécifiques et d'afficher des données qui correspondent aux critères de recherche dans une liste de résultats. Vous pouvez créer une nouvelle recherche ou charger un ensemble de critères de recherche précédemment enregistré. Vous pouvez sélectionner, organiser et regrouper les colonnes de données à afficher dans les résultats de recherche.

Cette section comprend les rubriques suivantes :

- [Recherche d'événements ou de flux](#)
- [Recherche des violations](#)
- [Enregistrement des critères de recherche](#)
- [Suppression des critères de recherche](#)
- [Effectuer une sous-recherche](#)
- [Gérer les résultats de recherche](#)
- [Gestion de Search Groups](#)

REMARQUE

Lorsque vous créez ou personnalisez un modèle de rapport qui contient un graphique des événements, vous pouvez baser les données de graphique sur des critères de recherche enregistrée. Cela vous permet de personnaliser facilement le graphique. Pour plus d'informations, voir [Gestion des rapports](#).

Recherche d'événements ou de flux

Pour rechercher les événements :

Etape 1 Sélectionnez l'une des options suivantes :

- Pour rechercher des événements, cliquez sur l'onglet **Log Activity**.
- Pour rechercher des flux, cliquez sur l'onglet **Network Activity**.

Etape 2 Dans la zone de liste **Search**, sélectionnez **New Search**.

Etape 3 Sélectionnez l'une des options suivantes :

- Pour charger une recherche précédemment sauvegardé, allez à [Etape 4](#).

- Pour créer une nouvelle recherche, allez à [Etape 5](#).

Etape 4 Sélectionnez une recherche précédemment sauvegardé :

- Sélectionnez l'une des options suivantes :
 - A partir de la liste **Available Saved Searches**, sélectionner la recherche enregistrée que vous voulez charger.
 - Dans le champs **Type Saved Search or Select from List**, saisissez le nom de la recherche que vous voulez charger.

b Cliquez sur **Load**.

Après avoir chargé la recherche sauvegardée, le panneau Edit Search s'affiche.

c Dans le panneau Edit Search, sélectionnez les options souhaitées pour cette recherche :

Tableau 7-1 Modifier les options de recherche

Paramètre	Description
Inclure dans mes recherches rapides	Cochez cette case si vous souhaitez inclure cette recherche dans votre menu Quick Search , qui se trouve sur les barres d'outils Log Activity et Network Activity . Pour plus d'informations sur le menu Quick Search , voir Tableau 7-2 .
Include in my Dashboard	Cochez cette case si vous voulez inclure les données de votre recherche enregistrée dans votre tableau de bord. Pour plus d'informations sur tableau de bord, voir Utilisation de l'onglet Dashboard . <i>Remarque : Ce paramètre ne s'affiche que si la recherche est regroupée.</i>
Définir par défaut	Cochez cette case si vous souhaitez définir cette recherche comme votre recherche par défaut lorsque vous accédez à l'onglet Log Activity ou Network Activity .
Partager avec tout le monde	Cochez cette case si vous souhaitez partager ces critères de recherche avec tous les autres utilisateurs.

Etape 5 Dans le panneau Time Range, sélectionnez une option pour l'intervalle que vous voulez capturer pour cette recherche.

a Saisissez les valeurs pour les paramètres suivants :

Tableau 7-2 Intervalle

Paramètre	Description
Diffusion temps réel (diffusion)	Sélectionnez cette option si vous souhaitez filtrer des événements ou des flux tout en mode streaming. La diffusion en temps réel (diffusion) est activée par défaut. Pour plus d'informations sur le mode de diffusion, voir Affichage d'événements en continu ou affichage des flux en continu <i>Remarque : Quand une diffusion en temps réel (diffusion) est activée, vous ne parvenez pas à grouper vos résultats de recherche. Si vous sélectionnez n'importe quelle option de regroupement dans le panneau Column Definition, un message d'erreur est affiché.</i>
Dernier intervalle (actualisation automatique)	Sélectionnez cette option si vous souhaitez filtrer des événements tout en mode actualisation automatique. Les onglets Log Activity and Network Activity s'actualisent par intervalles d'une minute pour afficher l'information la plus récente.
Récent	Sélectionnez l'option et, dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez filtrer.
Intervalle caractéristique	Sélectionnez cette option et, à l'aide de l'agenda, sélectionnez la date et la plage de temps que vous souhaitez filtrer.

- b Facultatif. Cliquez sur **Filter** si vous avez terminé la configuration de la recherche et que vous voulez afficher les résultats.

Etape 6 Dans la sous-fenêtre Search Parameters, définissez vos critères de recherche :

- a A partir de la première zone de liste, sélectionnez le paramètre que vous souhaitez rechercher. Par exemple, Device, Source Port, ou Event Name.

REMARQUE

Le paramètre **Quick Filter** vous permet de rechercher des événements ou des flux qui correspondent à la chaîne de texte dans le contenu d'événement ou de flux. Pour plus d'informations sur la façon d'utiliser le paramètre **Quick Filter**, voir [Utilisation de la syntaxe de filtre rapide](#).

- b Dans la deuxième zone de liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. Les modificateurs qui sont disponibles dépendent du paramètre sélectionné dans la première liste.
- c Dans la zone de saisie, entrez des informations spécifiques liées à votre paramètre de recherche.
- d Cliquez sur **Add Filter**.
- e Répétez les étapes de a à d pour chaque filtre que vous souhaitez ajouter aux critères de recherche.

Le filtre s'affiche dans la zone de texte **Current Filters**.

Etape 7 Si vous souhaitez enregistrer automatiquement les résultats de recherche lorsque la recherche est terminée, sélectionnez la case **Save results when search is complete**, et puis saisissez un nom pour la recherche enregistrée.

Etape 8 A l'aide du panneau Column Definition, définissez les colonnes et l'âgeement de colonne que vous souhaitez utiliser pour afficher les résultats :

- a A partir de la liste **Display**, sélectionnez l'affichage préconfiguré que vous souhaitez associer à cette recherche
- b Cliquez sur la flèche à côté de **Advanced View Definition** afin d'afficher les paramètres de recherche avancée.
- c Personnaliser les colonnes à afficher dans les résultats de recherche :

Tableau 7-3 Options de définition d'affichage avancées

Paramètre	Description
Saisissez Column ou Sélectionner dans la liste	<p>Filter les colonnes dans la liste Available Columns.</p> <p>Vous pouvez saisir le nom de la colonne que vous souhaitez localiser ou saisir un mot-clé pour afficher une liste de noms de colonnes qui incluent ce mot-clé. Par exemple, saisissez Device pour afficher la liste des colonnes qui comprend Device dans le nom de la colonne.</p>
Colonnes disponibles	Listes de colonnes disponibles. Les colonnes qui sont actuellement en usage pour cette recherche enregistrée sont soulignées et affichées dans la liste Columns .
Ajouter et supprimer des icônes de colonne (premier ensemble)	<p>Les premiers ensembles d'icônes vous permettent de personnaliser la liste Group By.</p> <ul style="list-style-type: none"> • Ajouter colonne - Sélectionnez une ou plusieurs colonnes dans la liste Available Columns et cliquez sur l'icône Add Column. • Suppression de colonne - Sélectionnez une ou plusieurs colonnes dans la liste Group By et cliquez sur l'icône Remove Column.
Ajouter et supprimer des icônes de colonne (dernier ensemble)	<p>Les derniers ensembles d'icône vous permettent de personnaliser la liste Columns.</p> <ul style="list-style-type: none"> • Ajouter colonne - Sélectionnez une ou plusieurs colonnes dans la liste Available Columns et cliquez sur l'icône Add Column. • Suppression de colonne - Sélectionnez une ou plusieurs colonnes dans la liste Columns et cliquez sur l'icône Remove Column.
Group By	<p>Indique les colonnes dans lesquelles la recherche enregistrée regroupe les résultats. Vous pouvez personnaliser davantage la liste Group By en utilisant les options suivantes :</p> <ul style="list-style-type: none"> • Move Up - Sélectionnez une colonne et déplacez-le vers la liste prioritaire en utilisant l'icône Move Up. • Move Down - Sélectionnez une colonne et déplacez-le vers le bas liste prioritaire en utilisant l'icône Move Down. <p>La liste de priorité indique l'ordre dans lequel les résultats sont regroupés. Les résultats de la recherche sont regroupés dans la première colonne de la liste Group By puis dans le groupe de la colonne suivante sur la liste.</p>

Tableau 7-3 Options de définition d'affichage avancées (suite)

Paramètre	Description
Columns	<p>Indique les colonnes choisies pour la recherche. Les colonnes sont chargées depuis une recherche enregistrée. Vous pouvez personnaliser la liste Columns en sélectionnant des colonnes à partir de la liste Available Columns. Vous pouvez personnaliser d'avantage la liste Columns en utilisant les options suivantes :</p> <ul style="list-style-type: none"> • Move Up - Sélectionnez une colonne et déplacez-le vers la liste prioritaire en utilisant l'icône Move Up. • Move Down - Sélectionnez une colonne et déplacez-le vers le bas liste prioritaire en utilisant l'icône Move Down. <p>Si le type de colonne est numérique ou à base de temps et qu'il existe une entrée dans la liste Group By, la colonne contient une zone de liste qui vous permet de choisir la façon dont vous souhaitez regrouper la colonne.</p> <p>Si le type de colonne est un groupe, la colonne contient une zone de liste qui vous permet de choisir combien de niveau vous souhaitez inclure dans le groupe.</p>
Order By	<p>A partir de la première zone de liste, sélectionnez la colonne dans laquelle vous voulez trier les résultats de la recherche. Puis, à partir de la deuxième zone de liste, sélectionnez la commande que vous souhaitez afficher pour les résultats de la recherche : Descending ou Ascending.</p>

Etape 9 Cliquer **Filter**.

Les résultats de la recherche sont affichés.

Lorsque vous générez une recherche qui s'affiche sur l'onglet **Log Activity** ou **Network Activity** tab avant que la recherche ne collecte tous les résultats, la page de résultats partielle est affichée. Si la recherche n'est pas terminée, l'état **In Progress (<percent>% Complete)** est affiché dans le coin supérieur droit.

Lors de l'affichage des résultats de recherche partiels, le moteur de recherche fonctionne en arrière-plan pour effectuer la recherche et actualise les résultats partiels afin de mettre à jour l'affichage.

Lorsque la recherche est terminée, l'état **Completed** est affiché dans le coin supérieur droit. Pour plus d'informations sur l'affichage des résultats de votre recherche, voir [Utilisation de l'onglet Log Activity](#) ou [Affichage des flux](#).

Recherche des violations

Grâce à la fonction Search, vous pouvez rechercher des violations en utilisant des critères spécifiques et afficher des violations qui correspondent aux critères de recherche dans une liste de résultats. Vous pouvez créer une nouvelle recherche ou charger un ensemble de critères de recherche précédemment enregistré.

Cette section comprend les rubriques suivantes :

- [Recherche de My Offenses et de All Offenses](#)
- [Recherche d'IP sources](#)

- [Recherche d'IP de destination](#)
- [Recherche de réseaux](#)
- [Enregistrement des critères de recherche](#)

Recherche de My Offenses et de All Offenses

Pour chercher les violations :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Dans la zone de liste **Search**, sélectionnez **New Search**.
- Etape 3** Sélectionnez l'une des options suivantes :
- Pour charger une recherche précédemment sauvegardé, allez à [Etape 4](#).
 - Pour créer une nouvelle recherche, allez à [Etape 7](#).
- Etape 4** Sélectionner une recherche préalablement enregistrée à l'aide de l'une des options suivantes :
- A partir de la liste **Available Saved Searches**, sélectionner la recherche enregistrée que vous voulez charger.
 - Dans le champs **Type Saved Search or Select from List**, saisissez le nom de la recherche que vous voulez charger.
- Etape 5** Cliquez sur **Load**.
Après avoir chargé la recherche sauvegardée, le panneau Edit Search s'affiche.
- Etape 6** Sélectionner la case **Set as Default** si vous souhaitez définir cette recherche comme votre recherche par défaut.
Si vous définissez cette recherche comme votre recherche par défaut, la recherche s'effectue automatiquement et affiche les résultats à chaque fois que vous accédez à l'onglet **Offenses**.
- Etape 7** Dans le panneau Time Range, sélectionnez une option pour l'intervalle que vous voulez capturer pour cette recherche.

Tableau 7-4 Intervalle

Paramètre	Description
All Offenses	Sélectionnez cette option si vous souhaitez rechercher toutes les violations quelle que soit l'intervalle de temps.
Récent	Sélectionnez l'option et, dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez rechercher.

Tableau 7-4 Intervalle (suite)

Paramètre	Description
Intervalle caractéristique	<p>Si vous voulez indiquer un intervalle spécifique de recherche, sélectionnez l'option Intervalle caractéristique, puis sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> • Démarrer la date entre - Cochez cette case si vous souhaitez rechercher les violations qui ont commencé au cours d'une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. • Dernier événement / flux entre - Cochez cette case si vous souhaitez rechercher les violations que le dernier événement détecté est survenu //dans une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Recherche	Cliquer Search si vous avez terminé la configuration de la recherche et que vous voulez afficher les résultats.

Etape 8 Dans le panneau Search Parameters, définissez les critères de recherche caractéristique :

Tableau 7-5 Paramètres de recherches

Élément	Description
ID de violation	Entrez l'ID de la violation que vous souhaitez rechercher.
Description	Entrez la description que vous souhaitez rechercher.
Affecté à un utilisateur	Dans la zone de liste, sélectionnez le nom d'utilisateur que vous souhaitez rechercher.
Direction	<p>Dans la zone de liste, sélectionnez la direction de la violation que vous souhaitez rechercher. Les options incluent :</p> <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote • Local to Remote ou Local • Remote to Remote ou Local
IP source	Entrez l'adresse IP ou l'intervalle CIDR que vous souhaitez rechercher.
Destination IP	Entrez l'adresse IP de destination ou l'intervalle CIDR que vous souhaitez rechercher.
Amplitude	Dans la zone de liste, sélectionnez si vous souhaitez rechercher une amplitude égale, inférieure ou supérieure à la valeur configurée. L'intervalle est entre 0 et 10.
Gravité	Dans la zone de liste, sélectionnez si vous souhaitez rechercher une gravité égale, inférieure ou supérieure à la valeur configurée. L'intervalle est entre 0 et 10.

Tableau 7-5 Paramètres de recherches (suite)

Élément	Description
Crédibilité	Dans la zone de liste, sélectionnez si vous souhaitez rechercher une crédibilité égale, inférieure ou supérieure à la valeur configurée. L'intervalle est entre 0 et 10.
Pertinence	Dans la zone de liste, sélectionnez si vous souhaitez rechercher une pertinence égale, inférieure ou supérieure à la valeur configurée. L'intervalle est entre 0 et 10.
Contient des nom d'utilisateurs	Entrez une déclaration d'expression régulière pour rechercher les violations contenant le nom d'utilisateur spécifié. Lorsque vous définissez des modèles des expressions régulières, optez pour des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.
Réseau de la source	Dans la zone de liste, sélectionnez le réseau de source que vous souhaitez rechercher.
Réseau de destination	Dans la zone de liste, sélectionnez le réseau de destination que vous souhaitez rechercher.
High Level Category	Dans la zone de liste, sélectionnez la catégorie de niveau supérieur que vous souhaitez rechercher. Pour plus d'informations sur les catégories, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i> .
Low Level Category	Dans la zone de liste, sélectionnez la catégorie de niveau inférieur que vous souhaitez rechercher. Pour plus d'informations sur les catégories, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i> .
Exclure	Sélectionnez les cases à cocher pour les violations que vous souhaitez exclure des résultats de recherche. Les options incluent : <ul style="list-style-type: none"> • Active Offenses • Hidden Offenses (sélectionné par défaut) • Closed Offenses (sélectionné par défaut) • Inactive offenses • Protected Offense
Fermer par Utilisateur	Ce paramètre ne s'affiche que lorsque la case Closed Offenses n'est pas cochée dans le panneau Exclure. Le défaut c'est Any . Dans la zone de liste, sélectionnez le nom d'utilisateur pour lequel vous souhaitez rechercher des violations fermées ou sélectionner Any pour afficher toutes les violations fermées. Le nom d'utilisateur est le nom de l'utilisateur qui a fermé la violation. Le défaut c'est Any .
Cause de fermeture	Ce paramètre ne s'affiche que lorsque la case Closed Offenses n'est pas cochée dans le panneau Exclure. Dans la zone de liste, sélectionnez la cause pour laquelle vous souhaitez rechercher des violations fermées ou sélectionner Any pour afficher toutes les violations fermées. Cette cause est celle que l'utilisateur a spécifiée lors de la fermeture de la violation.

Tableau 7-5 Paramètres de recherches (suite)

Élément	Description
Événements	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un comptage d'événement égal, inférieur ou supérieur à la valeur configurée.
Flux	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un comptage de flux égal, inférieur ou supérieur à la valeur configurée.
Événements/Flux total	Dans la zone de liste, sélectionnez si vous souhaitez rechercher le comptage total d'événements et de flux égal, inférieur ou supérieur à la valeur configurée.
Destinations	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un comptage de l'adresse IP de destination égal, inférieur ou supérieur à la valeur configurée.
Contient Source de journal	
Groupe de source de journal	Dans la zone de liste, sélectionnez un groupe de sources journal qui contient la source du journal que vous souhaitez rechercher. La zone de liste Log Source affiche toutes les sources de journaux affectées au groupe source du journal sélectionné.
Source de journal	Dans la zone de liste, sélectionnez la source de journal que vous souhaitez rechercher.
Règle de contribution	
Groupe de règle	Dans la zone de liste, sélectionnez un groupe de règles qui contient la règle que vous voulez rechercher. La zone de liste Rule affiche toutes les règles affectées au groupe de règle sélectionné.
Règle	Dans la zone de liste, sélectionnez la règle de contribution que vous souhaitez rechercher.

Étape 9 Dans le panneau **Offense Source**, indiquez la source et le type de violation que vous souhaitez rechercher :

- a Dans la zone de liste, sélectionnez le type de violation que vous souhaitez rechercher.

Lorsque vous sélectionnez un type de violation, les paramètres de recherche correspondants sont affichés.

- b Entrez les critères de recherche :

Tableau 7-6 Paramètres de source de type de violation

Types de violation	Description
Any	Sélectionnez cette option pour chercher toutes les sources de violations. C'est configuré par défaut.
IP source	Sélectionnez cette option et saisissez l'adresse IP source que vous souhaitez rechercher.
Destination IP	Sélectionnez cette option et saisissez l'adresse IP destination que vous souhaitez rechercher.

Tableau 7-6 Paramètres de source de type de violation (suite)

Types de violation	Description
Nom de l'événement	<p>Cliquez sur l'icône Browse pour ouvrir le navigateur d'événements et trouvez l'emplacement du nom de l'événement (QID) que vous souhaitez rechercher.</p> <p>Rechercher un QID particulier en utilisant l'une des options suivantes :</p> <ul style="list-style-type: none"> • Pour rechercher un QID par catégorie, sélectionnez la case Browse by Category et sélectionnez la catégorie à haut ou à bas niveau dans les zones liste. • Pour rechercher un QID par type de source de journal, sélectionnez la zone de liste Browse by Log Source Type et sélectionnez un type de source de journal à partir de la zone de liste Log Source Type. • Pour rechercher un QID par nom, cochez la case de recherche QID et saisissez un nom dans le champ QID/Name. <p>Une liste de QIDS est affichée.</p> <p>Saisissez le QID que vous souhaitez rechercher.</p>
Nom d'utilisateur	Sélectionnez cette option et saisissez le nom d'utilisateur que vous souhaitez rechercher.
Adresse MAC source	Sélectionnez cette option et saisissez l'adresse MAC source que vous souhaitez rechercher.
Adresse MAC source de destination	Sélectionnez cette option et saisissez l'adresse MAC destination que vous souhaitez rechercher.
Source de journal	<p>Dans la zone de liste Log Source Group sélectionnez un groupe de sources journal qui contient la source du journal que vous souhaitez rechercher. La zone de liste Log Source affiche toutes les sources de journal affectées au groupe source du journal sélectionné.</p> <p>Dans la zone de liste Log Source, sélectionnez la source de journal que vous souhaitez rechercher.</p>
Nom d'hôte	Sélectionnez cette option et saisissez le nom d'hôte que vous souhaitez rechercher.
Port de la source	Sélectionnez cette option et saisissez le port source que vous souhaitez rechercher.
Port de destination	Sélectionnez cette option et saisissez le port destination que vous souhaitez rechercher.
IPv6 Source	Sélectionnez cette option et saisissez l'adresse IPv6 source que vous souhaitez rechercher.
IPv6 Destination	Sélectionnez cette option et saisissez l'adresse IPv6 destination que vous souhaitez rechercher.
Source ASN	Dans la zone de liste Source ASN , sélectionnez la source ASN que vous souhaitez rechercher.

Tableau 7-6 Paramètres de source de type de violation (suite)

Types de violation	Description
ASN de la destination	Dans la zone de liste Destination ASN , sélectionnez la destination ASN que vous souhaitez rechercher.
Règle	Dans la zone de liste Rule Group , sélectionnez un groupe de règles qui contient la règle que vous voulez rechercher. La zone de liste Rule Group affiche toutes les règles affectées au groupe de règle sélectionné. Dans la zone de liste Rule , sélectionnez la règle que vous souhaitez rechercher.
ID application	Dans la zone de liste App ID , sélectionnez l'application ID que vous souhaitez rechercher.

- Etape 10** A l'aide du panneau Column Definition, définissez l'ordre dans lequel vous souhaitez trier les résultats :
- a A partir de la première zone de liste, sélectionnez la colonne dans laquelle vous voulez trier les résultats de la recherche.
 - b A partir de la deuxième zone de liste, sélectionnez la commande que vous souhaitez afficher pour les résultats de recherche : Décroissant ou Croissant.

- Etape 11** Cliquez sur **Search**.
Les résultats de la recherche sont affichés.

Recherche d'IP sources

Pour rechercher l'adresse IP source :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **By Source IP**.
- Etape 3** Dans la zone de liste **Search**, sélectionnez **New Search**.
- Etape 4** Dans le panneau Time Range, sélectionnez une option pour l'intervalle que vous voulez capturer pour cette recherche.

Tableau 7-7 Options d'intervalle de temps

Paramètre	Description
All Offenses	Sélectionnez cette option si vous souhaitez rechercher toutes les adresses IP source quelle que soit l'intervalle de temps.
Récent	Sélectionnez l'option et, dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez rechercher.

Tableau 7-7 Options d'intervalle de temps (suite)

Paramètre	Description
Intervalle caractéristique	<p>Si vous voulez indiquer un intervalle spécifique de recherche, sélectionnez l'option Intervalle caractéristique, puis sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> • Démarrer la date entre - Cochez cette case si vous souhaitez rechercher les adresses IP source associées aux violations qui ont commencé au cours d'une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. • Dernier événement/flux entre - Cochez cette case si vous souhaitez rechercher les adresses IP source associées aux violations que le dernier événement détecté est survenu ///dans une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Recherche	Cliquer Search si vous avez terminé la configuration de la recherche et que vous voulez afficher les résultats.

Etape 5 Dans le panneau Search Parameters, définissez les critères de recherche caractéristique :

Tableau 7-8 Paramètres de recherche d'adresse IP source

Elément	Description
IP source	Entrez l'adresse IP ou l'intervalle CIDR que vous souhaitez rechercher.
Amplitude	Dans la zone de liste, sélectionnez si vous souhaitez rechercher une amplitude égale, inférieure ou supérieure à la valeur configurée. L'intervalle est entre 0 et 10.
Risque VA	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un risque VA égal, inférieur ou supérieur à la valeur configurée. L'intervalle est entre 0 et 10.
Événement / Flux	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un comptage d'événement et de flux égal, inférieur ou supérieur à la valeur configurée.
Exclure	<p>Sélectionnez les cases à cocher pour les violations que vous souhaitez exclure des résultats de recherche. Les options incluent :</p> <ul style="list-style-type: none"> • Active Offenses • Hidden Offenses (sélectionné par défaut) • Closed Offenses (sélectionné par défaut) • Inactive offenses • Protected Offense

Etape 6 A l'aide du panneau Column Definition, définissez l'ordre dans lequel vous souhaitez trier les résultats :

- a A partir de la première zone de liste, sélectionnez la colonne dans laquelle vous voulez trier les résultats de la recherche.
- b A partir de la deuxième zone de liste, sélectionnez la commande que vous souhaitez afficher pour les résultats de recherche : Décroissant ou Croissant.

Etape 7 Cliquez sur **Search**.

Les résultats de la recherche sont affichés. Les résultats de la recherche considèrent tous les adresses IP sources associées à des violations actives.

Recherche d'IP de destination

Pour rechercher l'adresse IP destination :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Sur le menu de navigation, cliquez sur **By Destination IP**.

Etape 3 Dans la zone de liste **Search**, sélectionnez **New Search**.

Etape 4 Dans le panneau Time Range, sélectionnez une option pour l'intervalle que vous voulez capturer pour cette recherche.

Tableau 7-9 Options d'intervalle de temps

Paramètre	Description
All Offenses	Sélectionnez cette option si vous souhaitez rechercher toutes les adresses IP destination quelle que soit l'intervalle de temps.
Récent	Sélectionnez l'option et, dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez rechercher.
Intervalle caractéristique	Si vous voulez indiquer un intervalle spécifique de recherche, sélectionnez l'option Intervalle caractéristique, puis sélectionnez l'une des options suivantes : <ul style="list-style-type: none"> • Démarrer la date entre - Cochez cette case si vous souhaitez rechercher les adresses IP source associées aux violations qui ont commencé au cours d'une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. • Dernier événement/flux entre - Cochez cette case si vous souhaitez rechercher les adresses IP destination associées aux violations que le dernier événement détecté est survenu ///dans une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Recherche	Cliquer Search si vous avez terminé la configuration de la recherche et que vous voulez afficher les résultats.

Etape 5 Dans le panneau Search Parameters, définissez les critères de recherche caractéristique :

Tableau 7-10 Paramètres de recherche d'adresse IP destination

Élément	Description
Destination IP	Entrez l'adresse IP de destination ou l'intervalle CIDR que vous souhaitez rechercher.
Amplitude	Dans la zone de liste, sélectionnez si vous souhaitez rechercher une amplitude égale, inférieure ou supérieure à la valeur configurée. L'intervalle est entre 0 et 10.
Risque VA	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un risque VA égal, inférieur ou supérieur à la valeur configurée. L'intervalle est entre 0 et 10.
Événement / Flux	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un comptage d'événement et de flux égal, inférieur ou supérieur à la valeur configurée.

- Etape 6** A l'aide du panneau Column Definition, définissez l'ordre dans lequel vous souhaitez trier les résultats :
- A partir de la première zone de liste, sélectionnez la colonne dans laquelle vous voulez trier les résultats de la recherche.
 - A partir de la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de recherche : Décroissant ou Croissant.

Etape 7 Cliquez sur **Search**.

Les résultats de la recherche sont affichés. Les résultats de la recherche considèrent tous les adresses IP de destination associées à des violations actives.

Recherche de réseaux Pour rechercher des réseaux :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez sur **By Networks**.
- Etape 3** Dans la zone de liste **Search**, sélectionnez **New Search**.
- Etape 4** Dans le panneau Search Parameters, définissez les critères de recherche caractéristique :

Tableau 7-11 Paramètres de recherche de réseau

Élément	Description
Réseau	Dans la zone de liste, sélectionnez le réseau que vous souhaitez rechercher.
Amplitude	Dans la zone de liste, sélectionnez si vous souhaitez rechercher une amplitude égale, inférieure ou supérieure à la valeur configurée. L'intervalle est entre 0 et 10.
Risque VA	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un risque VA égal, inférieur ou supérieur à la valeur configurée. L'intervalle est entre 0 et 10.

Tableau 7-11 Paramètres de recherche de réseau (suite)

Élément	Description
Événement / Flux	Dans la zone de liste, sélectionnez si vous souhaitez rechercher un comptage d'événement et de flux égal, inférieur ou supérieur à la valeur configurée.

- Étape 5** A l'aide du panneau Column Definition, définissez l'ordre dans lequel vous souhaitez trier les résultats :
- a A partir de la première zone de liste, sélectionnez la colonne dans laquelle vous voulez trier les résultats de la recherche.
 - b A partir de la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de recherche : Décroissant ou Croissant.

- Étape 6** Cliquez sur **Search**.
Les résultats de la recherche sont affichés.

Enregistrement des critères de recherche Pour enregistrer les critères de recherche spécifiés pour une utilisation ultérieure :

- Étape 1** Cliquez sur l'onglet **Offenses**.
- Étape 2** Effectuez une recherche. Voir [Recherche des violations](#).
Les résultats de la recherche sont affichés.
- Étape 3** Cliquez sur **Save Criteria**.
- Étape 4** Entrez des valeurs pour les paramètres :

Tableau 7-12 Enregistrer les paramètres de recherche

Paramètre	Description
Non de recherche	Entrez un nom que vous souhaitez attribuer à ces critères de recherche.
Attribuer une recherche au Groupe (s)	Cochez la case pour les groupes auxquels vous souhaitez affecter cette recherche enregistrée. Si vous ne sélectionnez pas un groupe, cette recherche enregistrée est attribuée à l'autre groupe par défaut.
Gérer les groupes	Cliquez sur Manage Groups pour gérer des groupes de recherche. Voir Gestion de Search Groups .

Tableau 7-12 Enregistrer les paramètres de recherche (suite)

Paramètre	Description
Options Timespan :	<p>Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> • Toutes les violations - Sélectionnez cette option si vous souhaitez rechercher toutes les violations quelle que soit la plage de temps. • Récent - Sélectionnez l'option et, dans la zone de liste, sélectionnez la plage horaire que vous souhaitez rechercher. • Intervalle caractéristique - Si vous souhaitez indiquer un intervalle particulier de recherche, sélectionner l'option Specific Interval et ensuite les options suivantes : <ul style="list-style-type: none"> Démarrer la date entre - Cochez cette case si vous souhaitez rechercher les violations qui ont commencé au cours d'une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. Dernier événement / flux entre - Cochez cette case si vous souhaitez rechercher les violations que le dernier événement détecté est survenu ///dans une certaine plage de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Définir par défaut	Cochez cette case si vous souhaitez définir cette recherche en tant que votre recherche par défaut.

Etape 5 Cliquez sur **OK**.

Enregistrement des critères de recherche

Pour enregistrer les critères de recherche spécifiés pour une utilisation ultérieure :

REMARQUE

L'enregistrement de vos critères de recherche permet aussi de sauvegarder la configuration de graphique. Pour plus d'informations sur la configuration des graphiques, voir [Configuration des graphiques](#).

Etape 1 Sélectionnez l'une des options suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Effectuez une recherche. Voir [Recherche d'événements ou de flux](#).

Les résultats de la recherche sont affichés.

Etape 3 Cliquez sur **Save Criteria**.

Etape 4 Entrez des valeurs pour les paramètres :

Tableau 7-13 Paramètres des critères de sauvegarde

Paramètre	Description
Non de recherche	<p>Saisissez un nom unique que vous souhaitez attribuer à ces critères de recherche.</p> <p>Remarque : Si vous indiquez un intervalle pour la recherche, Détection des anomalies QRadar ajoute le nom de la recherche à l'intervalle spécifié. Par exemple, une recherche enregistrée nommée <i>Exploits by Source</i> avec un intervalle de 5 dernières minutes devient un <i>Exploits by Source - 5 dernières minutes</i>.</p> <p>Remarque : Si vous modifiez un ensemble de colonnes dans une recherche précédemment sauvegardée, puis enregistrez les critères de recherche en utilisant le même nom, les accumulations antérieures des graphiques de séries temporelles sont perdues.</p>
Attribuer une recherche au Groupe (s)	<p>Cochez la case pour les groupes auxquels vous souhaitez affecter cette recherche enregistrée. Si vous ne sélectionnez pas un groupe, cette recherche enregistrée est attribuée à l'autre groupe par défaut. Pour plus d'informations, voir Gestion de Search Groups.</p>
Gérer les groupes	<p>Cliquez sur Manage Groups pour gérer des groupes de recherche. Pour plus d'informations, voir Gestion de Search Groups.</p>
Options Timespan :	<p>Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> • Diffusion en temps réel (streaming) - Sélectionnez cette option si vous souhaitez filtrer vos résultats de recherche tout en mode de diffusion. Pour plus d'informations sur le mode de diffusion, voir Affichage d'événements en continu ou affichage des flux en continu. • Dernier intervalle (actualisation intégrée) - Sélectionnez cette option si vous souhaitez filtrer vos résultats de recherche tout en mode d'actualisation intégrée. Les onglets Log Activity et Network Activity s'actualisent par intervalles d'une minute pour afficher les informations les plus récentes. • Récent - Sélectionnez l'option et, dans la zone de liste, sélectionnez l'intervalle que vous souhaitez filtrer. • Intervalle caractéristique - Sélectionnez cette option et, à partir de l'agenda, sélectionnez la date et l'intervalle que vous souhaitez filtrer.
Inclure dans mes recherches rapides	<p>Cochez cette case si vous souhaitez inclure cette recherche dans votre zone de liste Quick Search, qui se trouve sur les barres d'outils Log Activity et Network Activity. Pour plus d'informations sur l'option de la barre d'outils Quick Search, voir Tableau 4-1 ou Tableau 5-1.</p>
Include in my Dashboard	<p>Cochez cette case si vous voulez inclure les données de votre recherche enregistrée dans votre tableau de bord. Pour plus d'informations sur l'onglet Dashboard, voir Utilisation de l'onglet Dashboard.</p> <p>Remarque : Ce paramètre ne s'affiche que si la recherche est regroupée.</p>

Tableau 7-13 Paramètres des critères de sauvegarde (suite)

Paramètre	Description
Définir par défaut	Cochez cette case si vous souhaitez définir cette recherche comme votre recherche par défaut lorsque vous accédez à l'onglet Log Activity ou Network Activity .
Partager avec tout le monde	Cochez cette case si vous souhaitez partager ces critères de recherche avec tous les autres utilisateurs Détection des anomalies QRadar.

Etape 5 Cliquez sur **OK**.

Suppression des critères de recherche

Vous pouvez supprimer des critères de recherche. Lorsque vous supprimez une recherche enregistrée, les objets Détection des anomalies QRadar qui sont associés à la recherche enregistrée peuvent ne plus fonctionner. Les rapports et les règles de détection d'anomalies sont des objets Détection des anomalies QRadar qui utilisent des critères de recherche sauvegardés. Après avoir supprimé une recherche enregistrée, nous vous recommandons de modifier les objets associés afin de s'assurer qu'ils continuent de fonctionner.

Pour supprimer des critères de recherche sauvegardée:

Etape 1 Sélectionnez l'une des options suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Dans la zone de liste **Search**, sélectionnez **New Search** ou **Edit Search**.

Etape 3 Dans le panneau Saved Searches, sélectionnez une recherche sauvegardée à partir de la zone de liste **Available Saved Searches**.

Etape 4 Cliquez sur **Delete**.

Si les critères de recherche enregistrée ne sont pas associés à d'autres objets Détection des anomalies QRadar, une fenêtre de confirmation s'affiche. Voir [Etape 5](#).

Si les critères de recherche enregistrée sont associés à d'autres objets Détection des anomalies QRadar, la fenêtre Delete Saved Search est affichée. La fenêtre liste tous les objets Détection des anomalies QRadar qui sont associés à la recherche enregistrée que vous souhaitez supprimer. Nous vous recommandons de noter les objets associés. Voir [Etape 6](#).

Etape 5 Cliquez sur **OK**.

La recherche enregistrée est maintenant supprimée de votre système.

Etape 6 Sélectionnez l'une des options suivantes :

- Cliquez sur **OK** afin de poursuivre. La recherche enregistrée est maintenant supprimée.
- Cliquez sur **Cancel** pour fermer la fenêtre Delete Saved Search.

Si vous avez choisi de supprimer la recherche enregistrée, elle sera maintenant supprimée de votre système. Nous vous recommandons d'accéder aux objets associés que vous avez notés et de les modifier afin de supprimer leur association avec la recherche sauvegardée supprimée.

Effectuer une sous-recherche

Chaque fois que vous effectuez une recherche, Détection des anomalies QRadar recherche dans la base de données entière des événements ou des flux qui correspondent à vos critères. Ce processus peut prendre une longue période de temps selon la taille de la base de données.

La fonction de sous-recherche vous permet d'effectuer des recherches dans un ensemble de résultats de recherche déjà réalisée. La fonction de sous-recherche vous permet d'affiner vos résultats de recherche sans avoir besoin de rechercher à nouveau dans la base de données.

Cette fonction n'est pas disponible pour les recherches regroupées, les recherches en cours, ou en mode de diffusion. Lors de la définition d'une recherche que vous souhaitez utiliser comme une base de la sous-recherche, assurez-vous que l'option Real Time (streaming) est désactivée et que la recherche n'est pas regroupée.

Pour effectuer une sous-recherche :

Etape 1 Sélectionnez l'une des options suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Effectuez une recherche. Voir [Recherche d'événements ou de flux](#).

Les résultats de la recherche sont affichés.

Cette recherche devient la recherche de base à partir de laquelle toute sous-recherche peut être effectuée. Avant de continuer, assurez-vous que la recherche est terminée.

Le panneau Current Filter indique les filtres sur lesquels se fonde cette recherche.

Etape 3 Pour ajouter un filtre :

- a Cliquez sur **Add Filter**.
- b Dans la zone de liste, sélectionnez un paramètre que vous souhaitez rechercher.

REMARQUE

Le paramètre **Quick Filter** parameter vous permet de rechercher des événements ou des flux qui correspondent à la chaîne de texte dans le contenu d'événement. Pour plus d'informations sur la façon d'utiliser le paramètre **Quick Filter**, voir [Utilisation de la syntaxe de filtre rapide](#) (événements) ou [utilisation de la syntaxe de filtre rapide](#) (flux).

- c A partir de la deuxième zone de liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. La liste des modificateurs qui sont disponibles dépend de l'attribut sélectionné dans la première liste.
- d Dans la zone de saisie, entrez des informations spécifiques liées à votre recherche.
- e Cliquez sur **Add Filter**.

REMARQUE

Vous pouvez cliquer avec le bouton droit de la souris sur un événement et sélectionner l'option **Filter on**.

Les résultats de la sous-recherche s'affichent. Si la recherche est toujours en cours, les résultats partiels sont affichés.

Le panneau Original Filter indique les filtres appliqués à la recherche de base. Le panneau Current Filter indique les filtres appliqués à la sous-recherche.

REMARQUE

Vous pouvez effacer les sous- recherche de filtres sans avoir à redémarrer la recherche de base. Cliquez sur le lien Clear Filter à côté du filtre que vous souhaitez effacer. Si vous désactivez un filtre dans le panneau Original Filter, la recherche de base est relancée.

Etape 4 Cliquez sur **Save Criteria** pour enregistrer les critères de sous-recherche. Voir [Enregistrement des critères de recherche](#).

REMARQUE

Si vous supprimez les critères de recherche de base, vous avez toujours accès aux critères de sous-recherche sauvegardée. Si vous ajoutez un filtre, la sous-recherche recherche dans la base de données entière puisque la fonction de recherche ne fonde plus sa recherche sur un ensemble de données précédemment recherchées.

Gérer les résultats de recherche

Vous pouvez effectuer des plusieurs recherches, tout en naviguant sur d'autres onglets. Vous pouvez configurer la fonction de recherche pour vous envoyer une notification par courrier électronique lorsqu'une recherche est terminée. A tout moment pendant qu'une recherche est en cours, vous pouvez consulter les résultats partiels.

REMARQUE

La fonction Manage Search Results conserve les configurations graphiques à partir des critères de recherche enregistrée associés, cependant, si le résultat de la recherche sauvegardée est basé sur des critères de recherche enregistrée qui ont été supprimés, les graphiques par défaut (barre et graphique circulaire) s'affichent.

Cette section comprend les rubriques suivantes :

- [Affichage de Managed Search Results](#)
- [Sauvegarde de Search Results](#)
- [Annulation d'une recherche](#)
- [Suppression d'une recherche](#)

Affichage de Managed Search Results

Pour chercher les résultats de recherche :

Etape 1 Sélectionnez l'une des options suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 A partir du menu Search, sélectionnez **Manage Search Results**.

La page de gestion des résultats de la recherche fournit les paramètres suivantes :

Tableau 7-14 Gérer les pages des résultats de recherche

Paramètre	Description
Indicateurs	Indique qu'une notification par courrier électronique est en attente pour la fin de la recherche.
Utilisateur	Indique le nom de l'utilisateur ayant lancé la recherche.

Tableau 7-14 Gérer les pages des résultats de recherche (suite)

Paramètre	Description
Nom	Spécifie le nom de la recherche, si la recherche a été enregistrée. Pour plus d'informations sur la sauvegarde d'une recherche, voir Sauvegarde de Search Results .
Started On	Indique la date et l'heure de lancement de la recherche.
Ended On	Indique la date et l'heure de la fin de la recherche.
Duration	Indique la durée d'exécution qu'il a fallu pour la recherche. Si la recherche est actuellement en cours, le paramètre Duration indique la durée du traitement de la recherche à ce jour. Si la recherche a été annulée, le paramètre Duration indique la durée du traitement de la recherche avant l'annulation.
Expires On	Indique la date et l'heure d'expiration d'un résultat de recherche non enregistré. Le chiffre de conservation de recherche enregistrée est configuré dans les paramètres du système. Pour plus d'informations sur la configuration des paramètres du système, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i> . Les critères de recherche enregistrée n'expirent pas.
Status	Indique le statut de la recherche. Les options incluent : <ul style="list-style-type: none"> • Queued - Indique que la recherche est en attente pour démarrer. • <percent>% Complete - Indique l'état d'avancement de la recherche en termes de pourcentage intégrale. Vous pouvez cliquer sur le lien pour afficher des résultats partiels. • Sorting - Indique que la recherche a fini de collecter des résultats et les prépare actuellement pour l'affichage. • Canceled - Indiquer que la recherche a été annulée. Vous pouvez cliquer sur le lien pour voir les résultats. • Completed - Indique que la recherche est terminée. Vous pouvez cliquer sur le lien pour afficher les résultats. Voir Affichage d'événements ou Affichage des flux.
Taille	Indique la taille du fichier de l'ensemble des résultats de recherche.

La barre d'outils des résultats de la recherche fournit les options suivantes :

Tableau 7-15 Gérer les barres d'outils des résultats de recherche

Paramètre	Description
New Search	Cliquez sur New Search afin créer une recherche. Lorsque vous cliquez sur cette icône, la page de recherche s'affiche. Voir Recherche d'événements ou de flux .
Save Results	Click Save Results afin de sauvegarder les résultats de recherche. Voir Sauvegarde de Search Results . <i>Remarque : Cette option est activée uniquement lorsque vous avez sélectionné une ligne dans la liste Manage Search Results.</i>

Tableau 7-15 Gérer les barres d'outils des résultats de recherche (suite)

Paramètre	Description
Cancel	Cliquez sur Cancel afin d'annuler les recherches qui sont en cours ou qui sont en attente pour démarrer. Voir Annulation d'une recherche .
Delete	Cliquez sur Delete afin de supprimer un résultat de recherche. Voir Suppression d'une recherche .
Notify	Sélectionnez les recherches pour lesquelles vous souhaitez recevoir de notification, puis cliquez sur Notify pour activer la notification par courrier lorsque la recherche est terminée.
Affichage	Dans la zone de liste, sélectionnez les résultats de la recherche que vous voulez lister sur la page Search Results. Les options incluent : <ul style="list-style-type: none"> • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

Sauvegarde de Search Results

Pour sauvegarder les résultats de recherche :

Etape 1 Sélectionnez l'une des options suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Effectuez une recherche ou une sous-recherche. Pour plus d'informations sur la façon d'effectuer une recherche, voir [Recherche d'événements ou de flux](#). Pour plus d'informations sur la façon d'effectuer une sous-recherche, voir [Effectuer une sous-recherche](#).

Etape 3 Cliquez sur **Save Results**.

REMARQUE

L'icône **Save Results** est activée uniquement lorsque la recherche est terminée ou si la recherche a été annulé en cours d'exécution.

REMARQUE

Vous pouvez également enregistrer les résultats de la page Search Results. Cliquez sur **Search > Manage Search Results** et sélectionnez résultats de recherche. Cliquez sur **Save Results**.

Etape 4 Saisissez un nom unique pour les résultats de la recherche.

Etape 5 Cliquez sur **OK**.

Les résultats de recherche enregistrés affichent le nom de la colonne **Name** de la page Manage Search Results.

Annulation d'une recherche

Pour annuler une recherche :

- Etape 1** A partir de la page Manage Search Results, sélectionnez les résultats de recherche en attente ou en cours que vous souhaitez annuler.
- Etape 2** Cliquez sur **Cancel**.

REMARQUE

Vous pouvez sélectionner plusieurs recherches pour annuler.

- Etape 3** Cliquez sur **Oui**.
- Si la recherche était en cours lors de l'annulation, les résultats qui ont été accumulés jusqu'à l'annulation sont maintenus.

Suppression d'une recherche

Pour supprimer d'une recherche :

- Etape 1** A partir de la page Manage Search Results page, sélectionnez les résultats de recherche que vous souhaitez supprimer.
- Etape 2** Cliquez sur **Delete**.
- Etape 3** Cliquez sur **Oui**.

La recherche est supprimée de page Manage Search Results.

Gestion de Search Groups

A l'aide de la fenêtre Search Groups, vous pouvez créer et gérer des groupes de recherche. Ces groupes vous permettent de localiser facilement les critères de recherche enregistrée (voir [Recherche d'événements ou de flux](#) or [Recherche des violations](#)) ou baser un rapport sur une recherche enregistrée (voir [Managing Reports](#)).

Cette section comprend les rubriques suivantes :

- [Affichage de Search Groups](#)
- [Création d'un nouveau groupe](#)
- [Modification d'un groupe](#)
- [Copie d'une recherche sauvegardée vers un autre groupe](#)
- [Suppression d'une recherche enregistrée d'un groupe](#)
- [Suppression d'un groupe](#)

Affichage de Search Groups

Détection des anomalies QRadar fournit un ensemble par défaut des groupes et sous-groupes. Pour afficher les groupes de recherche :

- Etape 1** Sélectionnez l'une des options suivantes :
- Cliquez sur l'onglet **Log Activity**.
 - Cliquez sur l'onglet **Network Activity**.

- Cliquez sur l'onglet **Offenses**.

Etape 2 Sélectionnez **Search > Edit Search**.

Etape 3 Cliquez sur **Manage Groups**.

Vous pouvez ajouter de nouveaux groupes ou de modifier des groupes existants. Toutes les recherches enregistrées qui ne sont pas affectés à un groupe se trouvent dans le groupe **Other**.

Création d'un nouveau groupe Pour créer un nouveau groupe :

Etape 1 Sélectionnez le groupe dans lequel vous voulez créer le nouveau groupe.

Etape 2 Cliquez sur **New Group**.

Etape 3 Dans la zone **Name**, saisissez un nom unique du nouveau groupe.

Etape 4 Facultatif. Dans la zone **Description**, saisissez une description.

Etape 5 Cliquez **OK**.

Modification d'un groupe Pour modifier un groupe :

Etape 1 Sélectionnez le groupe que vous souhaitez modifier.

Etape 2 Cliquez sur **Edit**.

Etape 3 Pour modifier le nom, saisissez un nouveau nom dans la zone **Name**.

Etape 4 Pour modifier la description, saisissez une nouvelle description dans la zone **Description**.

Etape 5 Cliquez sur **OK**.

Copie d'une recherche sauvegardée vers un autre groupe Pour copier une recherche enregistrée vers un autre groupe :

Etape 1 Localisez et sélectionnez la recherche enregistrée que vous souhaitez copier vers un autre groupe.

Etape 2 Cliquez sur **Copy**.

Etape 3 Cochez la case pour le groupe sur lequel vous souhaitez copier la recherche enregistrée.

Etape 4 Cliquez sur **Assign Groups**.

Suppression d'une recherche enregistrée d'un groupe Pour supprimer une recherche enregistrée d'un groupe :

Etape 1 Sélectionnez la recherche sauvegardée que vous voulez supprimer du groupe.

REMARQUE

Lorsque vous supprimez une recherche enregistrée d'un groupe, la recherche enregistrée n'est pas supprimée de votre système. La recherche enregistrée est supprimée du groupe et déplacée automatiquement vers le groupe **Other**.

Etape 2 Cliquez sur **Remove**.

Etape 3 Cliquez sur **OK**.

Suppression d'un groupe Pour supprimer un groupe :

Etape 1 Sélectionnez le groupe que vous souhaitez supprimer.

REMARQUE

Vous ne pouvez pas supprimer les groupes **Event Search Groups**, **Flow Search Groups**, **Offense Search Groups**, et **Other**.

Etape 2 Cliquez sur **Remove**.

Etape 3 Cliquez sur **OK**.

8

CONFIGURING RULES

Les onglets **Log Activity**, **Network Activity** et **Offenses** vous permettent de configurer les règles ou les éléments structurants.

Cette section comprend les rubriques suivantes :

- [Présentation des règles](#)
- [Types de règles](#)
- [Rule Conditions](#)
- [Rule Responses](#)
- [Affichage des règles](#)
- [Création d'une règle personnalisée](#)
- [Création d'une règle de détection des anomalies](#)
- [Copie d'un règle](#)
- [Managing Rules](#)
- [Grouping Rules](#)
- [Modification d'un bloc de construction](#)

Présentation des règles

Les règles effectuent des tests sur les événements, les flux ou les violations et si les toutes les conditions sont réunies pour réaliser un test, la règle génère une réponse. Pour obtenir une liste exhaustive des règles par défaut, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Les deux catégories de règles sont les suivantes :

- **Custom Rules** - les règles personnalisées effectuent des tests sur les événements, les flux ou les violations pour détecter une activité inhabituelle sur votre réseau.
- **Anomaly Detection Rules** - Les Règles de détection des anomalies effectuent des tests sur les résultats de flux enregistrés ou les événements recherchés comme un moyen de détecter les modèles de trafic inhabituels sur votre réseau.

Un utilisateur sans droits d'accès administrateur peut créer des règles pour les zones de réseau auxquelles il peut accéder. Vous devez disposer des autorisations de rôles appropriées pour gérer des règles. Pour plus d'informations sur les autorisations de rôle d'utilisateur, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Types de règles

Les règles personnalisées comprennent les types de règles suivants :

- **Event Rule** - Une règle d'événement effectue des tests sur les événements au fur et à mesure qu'ils sont traités en temps réel par le processeur d'événements. Vous pouvez créer une règle d'événement pour détecter un événement unique (au sein de certaines propriétés) ou des séquences d'événements. Par exemple, pour éviter les problèmes de connexion votre réseau, l'accès à plusieurs hôtes ou la reconnaissance d'événement suivie par un exploit, vous pouvez créer une règle d'événement. Il est fréquent de voir des règles d'événement créer des violations comme une réponse.
- **Flow Rule** - Une règle de flux effectue des tests au fur et à mesure qu'ils sont traités en temps réel par QRadar QFlow Collector. Vous pouvez créer une règle de flux pour détecter un événement unique (au sein de certaines propriétés) ou des séquences de flux. Il est fréquent de voir des règles de flux créer des violations comme une réponse.
- **Common Rule** - Une règle commune effectue des tests sur les zones communes aux enregistrements de flux et d'événements. Par exemple vous pouvez créer une règle commune qui détecte les événements et les flux ayant une adresse IP source spécifique. Il est fréquent de voir des règles communes créer des violations comme une réponse.
- **Offense Rule** - Une règle de violation traite les violations uniquement si des modifications sont apportées à la violation, comme lorsque de nouveaux événements sont ajoutés ou si le système a planifié la violation pour une réévaluation. Il est fréquent de voir des règles de violation envoyer une notification comme une réponse.

Anomaly Detection Rules - Les Règles de détection des anomalies effectuent des tests sur les résultats de flux enregistrés ou les événements recherchés comme un moyen de détecter les modèles de trafic inhabituels sur votre réseau. Cette catégorie de règles comprend les types de règles suivants :

- **Anomaly** - Une règle d'anomalie teste le trafic des événements et des flux d'une activité anormale, telle qu'un trafic existant ou inconnu, qui cesse brusquement ou une variation en pourcentage dans le temps ou un objet actif. Par exemple, vous pouvez créer une règle d'anomalie pour comparer le volume moyen du trafic des cinq dernières minutes à celui de la dernière heure. S'il s'agit d'un changement de plus de 40%, la règle génère une réponse.
- **Threshold** - Une règle de seuil teste les événements et le flux de l'activité qui est inférieure, égale ou supérieure à un seuil défini ou à l'intérieur d'une plage spécifiée. Un seuil peut être basé sur n'importe quelles données collectées par QRadar Network Anomaly Detection. Par exemple, si vous créez une règle de seuil indiquant que le nombre de clients qui peuvent se connecter au serveur ne doit pas dépasser 220 clients entre 08h00 et 17h00, les règles génèrent une alerte lorsque 221 clients tentent de se connecter. La règle de seuil génère une alerte lorsque le 221^{ème} client tente de se connecter.
- Une règle de comportement teste le trafic de flux pour un changement de volume dans le comportement qui se produit régulièrement dans les modèles

saisonniers. Par exemple, si un serveur de messagerie communique généralement avec 100 hôtes par seconde au milieu de la nuit et puis recommence à communiquer avec 1000 hôtes par seconde, une règle de comportement génère une alerte.

Conditions de règle Les tests de chaque règle peuvent également faire des références aux autres blocs de construction et règles. Vous n'êtes pas obligé de créer des règles dans n'importe quel ordre particulier parce que le système vérifie les dépendances chaque fois qu'une nouvelle règle est ajoutée, modifiée ou supprimée. Si une règle qui est référencée par une autre règle est supprimée ou désactivée, un message d'avertissement est affiché et aucune mesure n'est prise.

Chaque règle peut contenir les éléments suivants :

- **Functions** - Grâce à ce composant, vous pouvez utiliser des blocs de construction et d'autres règles pour créer les fonctions suivantes : multi-événement, multi-flux ou multi-violation. Vous pouvez relier les règles à l'aide des fonctions qui prennent en charge les opérateurs booléens, comme OR et AND. Par exemple, si vous souhaitez connecter les règles d'événements, vous pouvez utiliser **lorsqu'un événement correspond à l'une des règles suivantes** : fonction. Pour une liste complète des fonctions, consultez [Tests de règle](#).
- **Building blocks** - Un bloc de construction est une règle sans réponse et utilisée en tant qu'une variable commune à plusieurs règles ou pour construire un complexe des règles ou des logiques que vous souhaitez utiliser dans d'autres règles. Vous pouvez enregistrer un groupe de tests comme blocs de construction pour une utilisation avec d'autres fonctions. Un bloc de construction vous permet de réutiliser des tests de règles spécifiques dans d'autres règles. Par exemple, vous pouvez enregistrer un bloc de construction qui comprend les adresses IP de tous les serveurs de messagerie de votre réseau, puis utiliser ce bloc de construction pour exclure les hôtes d'une autre règle. Les blocs de construction par défaut sont fournis à titre indicatif, qui devraient être revus et modifiés en fonction des besoins de votre réseau. Pour une liste exhaustive des blocs de construction, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
- **Tests** - Vous pouvez exécuter des tests sur la propriété d'un événement, d'un flux, ou d'une violation, tels que l'adresse IP source, la gravité de l'événement, ou l'analyse des taux. Pour une liste complète des tests, consultez [Tests de règle](#).

Réponses de règle QRadar Network Anomaly Detection Lorsque les conditions de règle sont respectées, les réponses peuvent inclure une ou plusieurs des réponses suivantes :

- Création d'une violation.
- Envoi d'un courrier électronique.
- Générer des notifications du système en utilisant la fonction Dashboard.
- Création ou ajout de données à des ensembles de références.

L'onglet **Rules** vous permet de créer une règle pour importer des événements et des flux de données dans un ensemble de références. Un ensemble de

références est un ensemble de données, comme une liste d'adresses IP ou des noms d'utilisateurs. Après avoir créé un ensemble de références, vous pouvez créer des règles pour détecter l'activité du journal ou du réseau associée à l'ensemble de références qui se produit sur votre réseau.

Vous pouvez créer un ensemble de références contenant des données dérivées d'un fichier externe. Par exemple, vous pouvez créer un ensemble de références pour conserver les données des employés licenciés. Tout d'abord, ajoutez une source de journal pour importer un fichier texte contenant les données des employés licenciés, telles que les adresses IP et les noms d'utilisateurs. Puis, à l'aide de l'assistant de règles personnalisées, créez un ensemble de référence en précisant les données que doit retenir du fichier externe. Pour plus d'informations sur la configuration des sources de journaux, voir le guide d'utilisation *IBM Security QRadar Log Sources*.

Lorsqu'un ensemble de références est créé, vous pouvez créer une règle qui génère une réponse si un élément de l'ensemble de références, comme l'adresse IP d'un employé licencié, est détecté sur votre réseau.

- Générer une réponse à un système externe, comprenant les types de serveurs suivants :
 - **Local Syslog** - Syslog est un standard qui vous permet de stocker des informations sur l'événement, le flux et la violation dans un fichier journal du logiciel indépendant. L'assistant Rules vous permet de configurer des règles pour générer un fichier syslog.
 - **Forwarding Destinations** - QRadar Network Anomaly Detection permet de transférer des données de journal brutes provenant de sources de journaux et de données d'événements QRadar Network Anomaly Detection normalisées vers un ou plusieurs systèmes de fournisseur (billetterie ou systèmes d'alerte, par exemple). Sur l'interface d'utilisateur QRadar Network Anomaly Detection, ces systèmes des fournisseurs sont appelés Destinations de transfert.
 - **Simple Network Management Protocol (SNMP)** - Le protocole SNMP permet à QRadar Network Anomaly Detection d'envoyer des notifications d'événements, de flux et de violation à un autre hôte pour être stockés. L'assistant Rules vous permet de configurer des règles pour générer des réponses qui incluent l'envoi d'interruptions SNMP à l'hôte configuré.
 - **Interface For Metadata Access Points (IF-MAP)** - La réponse de règle Interface For Metadata Access Points (IF-MAP) permet à QRadar Network Anomaly Detection de publier des données d'alerte et de violation à partir d'événements, de flux et de données de violation sur un serveur IF-MAP.

Affichage des règles

Pour afficher les règles déployées :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Dans le menu de la navigation, cliquez sur **Rules**.

Etape 3 Dans la zone de liste **Display**, Sélectionnez **Rules**.

La liste des règles déployées fournit les informations suivantes pour chaque règle :

Tableau 8-1 Paramètres de page Rules

Paramètre	Description
Rule Name	Indique le nom de la règle.
Group	Indique le groupe auquel cette règle est affectée. Pour plus d'informations à propos des groupes, voir Groupement de règles .
Rule Category	Indique les catégories de la règle. Options include: <ul style="list-style-type: none"> • Custom Rule • Anomaly Detection Rule
Rule Type	Indique le type de la règle. Les types des règles incluent : <ul style="list-style-type: none"> • Event • Flow • Common • Offense • Anomaly • Threshold • Behavioral Pour plus d'informations sur les types de règles, voir Types de règles .
Enabled	Indique si cette règle est activée ou désactivée. Pour plus d'informations sur l'activation ou la désactivation des règles, voir Activation/désactivation de règles .
Response	Indique la réponse de la règle, le cas échéant. Les réponses à la règle incluent : <ul style="list-style-type: none"> • Dispatch New Event • Email • Log • Notification • SNMP • Reference Set • IF-MAP Response Pour plus d'informations sur les réponses de règles, voir Activation/désactivation de règles .
Event/Flow Count	Indique le nombre d'événements ou de flux associés à cette règle lorsque celle-ci contribue à une violation.
Offense Count	Indique le nombre des violations générées par cette règle.
Origin	Indique s'il s'agit d'une règle par défaut (Système) ou d'une règle personnalisée (Utilisateur).

Tableau 8-1 Paramètres de page Rules (suite)

Paramètre	Description
Creation Date	Indique la date et l'heure de la création de cette règle.
Modification Date	Indique la date et l'heure de la modification de cette règle.

La barre d'outils de l'onglet Rules assure les fonctions suivantes :

Tableau 8-2 Barre d'outils de l'onglet Rules

Fonction	Description
Display	Dans la zone de liste, sélectionnez si vous voulez afficher les règles ou les blocs de construction dans la liste des règles.
Group	Dans la zone de liste, sélectionnez le groupe de règles que vous souhaitez afficher dans la liste des règles.
Groups	Cliquez sur Groups pour gérer les groupes de règles. Pour plus d'informations sur le groupement de règles, voir Groupement de règles .
Actions	<p>Cliquez sur Actions et sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> • New Event Rule - Sélectionnez cette option pour créer une nouvelle règle d'événement. Voir Création d'une règle personnalisée. • New Flow Rule - Sélectionnez cette option pour créer une nouvelle règle de flux. Voir Création d'une règle personnalisée. • New Common Rule - Sélectionnez cette option pour créer une nouvelle règle commune. Voir Création d'une règle personnalisée. • New Offense Rule - Sélectionnez cette option pour créer une nouvelle règle de violation. Voir Création d'une règle personnalisée. • Enable/Disable - Sélectionnez cette option pour activer ou désactiver les règles sélectionnées. Voir Activation/désactivation de règles. • Duplicate - Sélectionnez cette option pour copier une règle sélectionnée. Voir Copie d'un règle. • Edit - Sélectionnez cette option pour éditer une règle sélectionnée. Voir Modification d'une règle. • Delete - Sélectionnez cette option pour supprimer une règle sélectionnée. Voir Suppression d'une règle. • Assign Groups - Sélectionnez cette option pour affecter les règles sélectionnées aux groupes de règles. Voir Affectation d'un élément à un groupe.

Tableau 8-2 Barre d'outils de l'onglet Rules (suite)

Fonction	Description
Revert Rule	<p>Cliquez sur Revert Rule pour rétablir une règle de système modifiée sur sa valeur par défaut. Lorsque vous cliquez sur Revert Rule, une fenêtre de confirmation s'affiche. Lorsque vous rétablissez une règle, toutes les modifications précédentes sont définitivement supprimées.</p> <p>Remarque : Pour rétablir la règle et tout de même conserver une version modifiée, dupliquez la règle et utilisez l'option Revert Rule sur la règle modifiée.</p>
Search Rules	<p>Entrez vos critères de recherche dans la zone Search Rules et cliquez sur l'icône Search Rules ou appuyez sur la touche Entrée. Toutes les règles qui correspondent à vos critères de recherche s'affichent dans la liste des règles.</p> <p>Les paramètres suivants sont recherchés pour une correspondance avec votre critère de recherche :</p> <ul style="list-style-type: none"> • Rule Name • Rule (description) • Notes • Response <p>La fonction Search Rule tente de localiser une correspondance directe avec une chaîne de texte. Si aucune correspondance n'est trouvée, la fonction Search Rule tente alors une correspondance par une expression régulière (regex).</p>

Etape 4 Sélectionnez la règle que vous souhaitez afficher.

Si vous avez sélectionné une règle qui indique une règle personnalisée comme une catégorie de règle, l'assistant Custom Rules est affiché. Dans les zones **Rule** et **Notes**, des informations descriptives sont affichées.

Création d' une règle personnalisée

Les règles personnalisées comprennent les types de règles suivants :

- **Event Rule** - Une règle d'événement effectue des tests sur les événements au fur et à mesure qu'ils sont traités en temps réel par le processeur d'événements. Vous pouvez créer une règle d'événement pour détecter un événement unique (au sein de certaines propriétés) ou des séquences d'événements. Par exemple, pour éviter les problèmes de connexion votre réseau, l'accès à plusieurs hôtes ou la reconnaissance d'événement suivie par un exploit, vous pouvez créer une règle d'événement. Il est fréquent de voir des règles d'événement créer des violations comme une réponse.
- **Flow Rule** - Une règle de flux effectue des tests sur les flux au fur et à mesure qu'ils sont traités en temps réel par QRadar QFlow Collector. Vous pouvez créer une règle de flux pour détecter un événement unique (au sein de certaines propriétés) ou des séquences de flux. Il est fréquent de voir des règles de flux créer des violations comme une réponse.

- **Common Rule**- Une règle commune effectue des tests sur les zones qui sont communes aux enregistrements des événements et des flux. Par exemple, vous pouvez créer une règle commune pour détecter les événements et les flux ayant une adresse IP source spécifique. Il est fréquent de voir des règles communes créer les violations comme une réponse.
- **Offense Rule** - Une règle de violation traite les violations uniquement lorsque des modifications sont apportées à la violation, comme, lorsque les nouveaux événements sont ajoutés ou si le système a planifié la violation pour une réévaluation. Il est fréquent que les règles de la violation envoient une notification comme une réponse.

Pour créer une nouvelle règle:

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de la navigation, cliquez sur **Rules**.

Etape 3 Dans la zone de liste **Actions**, sélectionnez l'une des options suivantes :

- New Event Rule** - Sélectionnez cette option pour configurer une règle pour les événements.
- New Flow Rule** - Sélectionnez cette option pour configurer une règle pour les flux.
- New Common Rule** - Sélectionnez cette option pour configurer une règle pour les événements et les flux.
- New Offense Rule** - Sélectionnez cette option pour configurer une règle pour les violations.

REMARQUE

Si vous ne souhaitez pas afficher le message de bienvenue sur la page Rules Wizard, cochez la case **Skip this page when running the rules wizard**.

Etape 4 Lisez le texte d'introduction. Cliquez sur **Next**.

Vous êtes invité à choisir la source à partir de laquelle vous voulez que cette règle s'applique. La valeur par défaut est le type de règle que vous avez sélectionné sur l'onglet **Offenses**

Etape 5 Si nécessaire, sélectionnez le type de règle que vous souhaitez appliquer à la règle. Cliquez sur **Next**.

Etape 6 Pour ajouter un test à une règle :

- Dans la zone de liste **Test Group**, sélectionnez le type de test que vous voulez appliquer à cette règle.

REMARQUE

Pour filtrer les options dans la zone de liste **Test Group**, entrez un texte que vous voulez filtrer dans la zone **Type to filter**.

Pour plus d'informations sur les tests, voir [Tests de règle](#).

- Pour chaque test que vous voulez ajouter à la règle, sélectionnez le signe **+** à côté du test.

Les tests sélectionnés sont affichés dans la zone **Rule**.

- c Pour chaque test ajouté à la zone **Rule** que vous voulez identifier comme un test exclu, cliquez sur **and** au début du test.

and s'affiche comme **and not**.

- d Pour chaque test ajouté à la zone **Rule**, vous devez personnaliser la variable du test. Cliquez sur le paramètre configurable souligné. Voir [Tests de règle](#).

Etape 7 Dans la zone **enter rule name here**, entrez un nom unique que vous voulez affecter à cette règle.

Etape 8 Dans la zone de liste, sélectionnez si vous voulez tester la règle localement ou globalement :

- **Local** - Cette règle est testé sur le processeur d'événement local et non partagé avec le système. Local est choisi par défaut.
- **Global** - La règle est partagée et testée par n'importe quel processeur d'événement sur le système. Les règles globales envoient des événements et des flux au processeur central de l'événement, ce qui peut réduire les performances sur le processeur de l'événement central.

Etape 9 Pour exporter la règle configurée comme un bloc de construction à utiliser avec d'autres règles :

- a Cliquez sur **Export as Building Block**.
- b Entrez un nom unique pour ce bloc de construction.
- c Cliquez sur **Save**.

Etape 10 Dans le panneau Groups, sélectionnez les cases à cocher des groupes auxquels vous souhaitez attribuer à cette règle. Pour plus d'informations sur le groupement de règles, voir [Groupement de règles](#).

Etape 11 Dans la zone **Notes**, entrez les notes que vous voulez inclure à cette règle. Cliquez sur **Next**.

Dans l'assistant Rules, la page Rule Responses s'affiche, ce qui vous permet de configurer l'action que QRadar Network Anomaly Detection doit réaliser lorsque la séquence d'événements ou de flux est détectée.

Etape 12 Sélectionnez l'une des options suivantes :

- a Si vous configurez une règle d'événement, une règle de flux ou une règle commune :

Tableau 8-3 Paramètres de page de réponse de règles communes/de flux/d'événement

Paramètre	Description
Severity	Cochez cette case si vous souhaitez que cette règle définisse ou ajuste la gravité. Lorsqu'elle est sélectionnée, vous pouvez utiliser les zones de listes pour configurer le niveau de gravité approprié. Pour plus d'informations sur la gravité, voir Glossaire .

Tableau 8-3 Paramètres de page de réponse de règles communes/de flux/d'événement

Paramètre	Description
Credibility	Cochez cette case si vous souhaitez que cette règle définisse ou ajuste la crédibilité. Lorsqu'elle est sélectionnée, vous pouvez utiliser les zones de listes pour configurer le niveau de crédibilité approprié. Pour plus d'informations sur la crédibilité, voir Glossaire .
Relevance	Cochez cette case si vous souhaitez définir ou ajuster la pertinence. Lorsqu'elle est sélectionnée, vous pouvez utiliser les zones de listes pour configurer le niveau de pertinence approprié. Pour plus d'informations sur la pertinence, voir Glossaire .
Ensure the detected event is part of an offense	<p>Cochez cette case si vous souhaitez que l'événement soit transmis au composant Magistrate. Si aucune violation n'existe sur l'onglet Offenses, une nouvelle violation est créée. Si une violation existe, cet événement est ajouté à la violation.</p> <p>Lorsque vous cochez cette case, les options suivantes s'affichent :</p> <ul style="list-style-type: none"> • Index offense based on - Dans la zone de liste, sélectionnez le paramètre sur lequel vous voulez indexer la violation. La valeur par défaut est Source IPv6. <p>Pour les règles d'événements, les options incluent : destination IP, destination IPv6, destination MAC address, destination port, event name, host name, log source, rule, source IP, source IPv6, source MAC address, source port ou user name.</p> <p>Pour les règles de flux, les options incluent App ID, destination ASN, destination IP, destination IP Identity, destination port, event name, rule, source ASN, source IP, source IP identity ou source Port.</p> <p>Pour les règles communes, les options incluent destination IP, destination IP identity, destination port, rule, source IP, source IP identity et source port.</p> <ul style="list-style-type: none"> • Annotate this offense - Cochez cette case pour ajouter une annotation à cette violation et entrer l'annotation. • Include detected events by <index> from this point forward, for second(s), in the offense< - Cochez cette case et entrez le nombre de secondes pendant lesquelles vous souhaitez inclure les événements détectés <index> sur l'onglet Offenses. Cette zone indique le paramètre sur lequel la violation est indexée. La valeur par défaut est source IP.
Annotate event	Cochez cette case si vous souhaitez ajouter une annotation à cet événement et entrer l'annotation à ajouter à l'événement.
Drop the detected event	Cochez cette case pour forcer l'envoi d'un événement, qui est normalement envoyé au composant Magistrate, à la base de données Ariel pour une recherche. Cet événement ne s'affiche pas sur l'onglet offenses .
Rule Response	

Tableau 8-3 Paramètres de page de réponse de règles communes/de flux/d'événement

Paramètre	Description
Dispatch New Event	<p>Cochez cette case pour envoyer un nouvel événement en plus de l'événement ou du flux d'origine, qui sera traité comme tous les autres événements dans le système.</p> <p>Les paramètres Dispatch New Event s'affichent lorsque vous cochez cette case. Par défaut, la case est vide.</p>
Event Name	Entrez un nom unique pour l'événement que vous souhaitez afficher sur l'onglet Offenses .
Event Description	Entrez une description de l'événement. La description s'affiche sur le panneau Annotations des détails de l'événement.
Severity	Dans la zone de liste, sélectionnez la gravité de l'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est 0. La gravité s'affiche dans le panneau Annotation des détails de l'événement. Pour plus d'informations sur la gravité, voir Glossaire .
Credibility	Dans la zone de liste, sélectionnez la crédibilité de l'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est 10. La crédibilité s'affiche dans le panneau Annotations des détails de l'événement. Pour plus d'informations sur la crédibilité, voir Glossaire .
Relevance	Dans la zone de liste, sélectionnez la pertinence de l'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est 10. La pertinence s'affiche dans le panneau Annotations des détails de l'événement. Pour plus d'informations sur la pertinence, voir Glossaire .
High-Level Category	<p>Dans la zone de liste, sélectionnez les catégories d'événements supérieures dont vous avez besoin lors du traitement des événements.</p> <p>Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>
Low-Level Category	<p>Dans la zone de liste, sélectionnez les catégories d'événements supérieures dont vous avez besoin lors du traitement des événements.</p> <p>Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>
Annotate this offense	Cochez cette case pour ajouter une annotation à cette violation et entrer l'annotation.

Tableau 8-3 Paramètres de page de réponse de règles communes/de flux/d'événement

Paramètre	Description
Assurer-vous que l'événement envoyé fait partie d'une violation.	<p>Cochez cette case si vous voulez, qu'à la suite de cette règle, l'événement soit transmis au composant Magistrate. Si aucune violation n'est créée sur l'onglet Offenses, une nouvelle violation est créée. Si une violation existe, cet événement est ajouté.</p> <p>Lorsque vous cochez cette case, les options suivantes s'affichent :</p> <ul style="list-style-type: none"> Index offense based on - Dans la zone de liste, sélectionnez le paramètre sur lequel vous voulez indexer la violation. La valeur par défaut est source IP. <p>Pour les règles d'événements, les options incluent : destination IP, destination IPv6, destination MAC address, destination port, event name, host name, log source, rule, source IP, source IPv6, source MAC address, source port ou user name.</p> <p>Pour les règles de flux, les options incluent App ID, destination ASN, destination IP, destination IP Identity, destination port, event name, rule, source ASN, source IP, source IP identity ou source Port.</p> <p>Pour les règles communes, les options incluent destination IP, destination IP identity, destination port, rule, source IP, source IP identity et source port.</p> Include detected events by <index> A partir de ce point, pour les secondes, in the offense - Cochez cette case et entrez le nombre de secondes pendant lesquelles vous voulez inclure les événements détectés par <index> sur l'onglet Offenses. Cette zone indique le paramètre sur lequel la violation est indexée. La valeur par défaut est source IP. Offense Naming - Sélectionnez une des options suivantes : <p>This information should contribute to the name of the associated offense(s) - Sélectionnez cette option si vous souhaitez que les informations du nom de l'événement contribuent au nom de la violation.</p> <p>This information should set or replace the name of the associated offense(s) - Sélectionnez cette option si vous voulez que le nom de l'événement configuré soit le nom de la violation.</p> <p>This information should not contribute to the naming of the associated offense(s) - Sélectionnez cette option si vous voulez que les informations du nom de l'événement ne contribuent pas au nom de la violation. < Il s'agit de la valeur par défaut.</p>
Email	Cochez cette case pour afficher les options de courrier électronique. Par défaut, la case est vide.

Tableau 8-3 Paramètres de page de réponse de règles communes/de flux/d'événement

Paramètre	Description
Enter email addresses to notify	Entrez l'adresse de courrier électronique pour envoyer une notification si cette règle est générée. S'il y a plusieurs adresses de courrier électronique, séparez-les par une virgule.
Alerte SNMP	<p>Ce paramètre ne s'affiche que lorsque les paramètres SNMP sont configurés dans les paramètres du système. Pour plus d'informations sur la configuration des paramètres du système, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p> <p>► Activez cette règle en cochant cette case pour envoyer une notification SNMP (interruption).</p> <p>La sortie d'alerte SNMP comprend l'heure du système, l'ID objet de l'interruption et les données de notification, tels que définis par Q1 Labs MIB.</p> <p>Par exemple, la notification SNMP peut ressembler à :</p> <pre>"Wed Sep 28 12:20:57 GMT 2005, QRADAR Custom Rule Engine Notification - Rule 'SNMPTRAPTest' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name: ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes: Offense description"</pre>
Send to Local SysLog	<p>Cochez cette case si vous voulez consigner l'événement ou le transporter localement. Par défaut, la case est vide.</p> <p>Par exemple, la sortie syslog peut ressembler à :</p> <pre>Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description</pre>
Send to Forwarding Destinations	<p>Cette case ne s'affiche que pour les Règles d'événements.</p> <p>Cochez cette case si vous voulez consigner un événement ou le transférer à une destination de transfert. Une destination de transfert est un système de fournisseur, tel que SIEM, la billetterie ou les systèmes d'alerte. Lorsque vous cochez cette case, une liste des destinations de renvoi est affichée. Cochez la case de destination que vous souhaitez envoyer ou fluxer à l'événement.</p> <p>Pour ajouter, éditer, ou supprimer une destination de transfert, cliquez sur le lien Manage Destination. Pour plus d'informations sur la configuration des destinations de transfert, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>

Tableau 8-3 Paramètres de page de réponse de règles communes/de flux/d'événement

Paramètre	Description
Notify	<p>Cochez cette case si vous voulez que les événements qui se génèrent à la suite de cette règle s'affichent dans l'élément des notifications du système sur l'onglet Dashboard.</p> <p>Pour plus d'informations sur l'onglet Dashboard, voir Utilisation de l'onglet Dashboard.</p> <p>Remarque : Si vous activez les notifications, nous vous recommandons de configurer le paramètre Response Limiter</p>
Add to Reference Set	<p>Cochez cette option si vous voulez que les événements qui se génèrent à la suite de cette règle ajoutent des données à l'ensemble de référence.</p> <p>Pour ajouter des données à l'ensemble de références :</p> <ol style="list-style-type: none"> 1 A partir de la zone de liste, sélectionnez les données que vous voulez ajouter. Les options incluent toutes les données normalisées ou personnalisées. 2 A partir de la zone de liste, sélectionnez l'ensemble de références que vous voulez ajouter aux données spécifiées. <p>La réponse à la règle Add to Reference Set offre les fonctions suivantes :</p> <ul style="list-style-type: none"> • New - Cliquez sur NEW pour ajouter un nouvel ensemble de références et configurer les paramètres suivants : <ul style="list-style-type: none"> Nom - Entrez un nom unique pour l'ensemble de références. Type - Dans la zone de liste, sélectionnez le type de données. Les options incluent String, Numeric, IP et Port. Maximum number of elements - Entrez le nombre maximum des éléments de données que vous voulez stocker dans l'ensemble de référence. La valeur par défaut est 10.000 et le maximum est 100.000. • Edit - Cliquez sur Edit pour modifier le nom de l'ensemble de références et le nombre maximum des éléments de données pour l'ensemble de références sélectionné. • Delete - Cliquez sur Delete pour supprimer l'ensemble de références. • Purge - Cliquez sur Purge pour supprimer le contenu de l'ensemble de références tout en maintenant l'ensemble de références.
Publish on the IF-MAP Server	<p>Si les paramètres IF-MAP sont configurés et déployés dans les paramètres du système, sélectionnez cette option pour publier les informations de l'événement sur le serveur IF-MAP. Pour plus d'informations sur la configuration des paramètres IF-MAP, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>

Tableau 8-3 Paramètres de page de réponse de règles communes/de flux/d'événement

Paramètre	Description
Response Limiter	Cochez la case et utilisez la zone de liste pour configurer la fréquence à laquelle cette règle doit répondre.
Enable Rule	Cochez cette case pour activer cette règle. Par défaut, la case est cochée.

b Si vous configurez une règle de violation :

Tableau 8-4 Paramètres de page Offense Rule Response

Paramètre	Description
Rule Action	
Name/Annotate the detected offense	Cochez cette case pour afficher les noms des options.
New Offense Name	Entrez le nom que vous voulez affecter à la violation.
Offense Annotation	Entrez l'annotation de la violation que vous souhaitez afficher sur l'onglet Offenses
Offense Name	Sélectionnez une des options suivantes : <ul style="list-style-type: none"> • This information should contribute to the name of the associated offense(s) - Sélectionnez cette option si vous souhaitez que les informations du nom de l'événement contribuent au nom de la violation. • This information should set or the name of the associated offense(s) - Sélectionnez cette option si vous souhaitez que le nom de l'événement soit le nom de la violation.
Rule Response	
Email	Cochez cette case pour afficher les options de courrier électronique. Par défaut, la case est vide.
Enter email address to notify	Entrez l'adresse électronique pour envoyer une notification si cet événement est généré. S'il y a plusieurs adresses de courrier électronique, séparez-les par une virgule.

Tableau 8-4 Paramètres de page Offense Rule Response (suite)

Paramètre	Description
Alerte SNMP	<p>Ce paramètre ne s'affiche que lorsque les paramètres SNMP sont configurés dans les paramètres du système. Pour plus d'informations sur la configuration des paramètres du système, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p> <p>► Activez cette règle en cochant cette case pour envoyer une notification SNMP (interruption).</p> <p>La sortie d'alerte SNMP inclut l'heure du système, l'ID objet de l'interruption et la notification des données, tels que définis par Q1 Labs MIB.</p> <p>Par exemple, la notification SNMP peut ressembler à :</p> <pre>"Wed Sep 28 12:20:57 GMT 2005, QRADAR Custom Rule Engine Notification - Rule 'SNMPTRAPTest' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name: ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes: Offense description"</pre>
Send to Local SysLog	<p>Cochez cette case si vous voulez consigner l'événement ou le transporter localement. Par défaut, la case est vide.</p> <p>Par exemple, la sortie syslog peut ressembler à :</p> <pre>Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description</pre>
Send to Forwarding Destinations	<p>Cochez cette case si vous voulez consigner un événement ou le transférer à une destination de transfert. Une destination de transfert est un système de fournisseur, tel que SIEM, ticketing, ou les systèmes d'alerte. Lorsque vous cochez cette case, une liste des destinations de renvoi est affichée. Cochez la case de destination que vous souhaitez envoyer ou fluxer à l'événement.</p> <p>Pour ajouter, éditer, ou supprimer une destination de transfert, cliquez sur le lien Manage Destination. Pour plus d'informations sur la configuration des destinations de transfert, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>
Publish on the IF-MAP Server	<p>Si les paramètres IF-MAP sont configurés et déployés dans les paramètres du système, sélectionnez cette option pour publier les informations de l'événement sur le serveur IF-MAP. Pour plus d'informations sur la configuration des paramètres IF-MAP, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>
Response Limiter	<p>Sélectionnez cette case et utilisez les zones de liste pour configurer la fréquence à laquelle cette règle doit répondre.</p>

Tableau 8-4 Paramètres de page Offense Rule Response (suite)

Paramètre	Description
Enable Rule	Cochez cette case pour activer cette règle. Par défaut, la case est cochée.

Etape 13 Cliquez sur **Next**.

Etape 14 Vérifiez la règle configurée pour s'assurer que les paramètres sont corrects. Marquez les changements si nécessaire, puis cliquez sur **Finish**.

Création d'une règle de détection des anomalies

Anomaly Detection Rules - Les Règles de détection des anomalies effectuent des tests sur les résultats de flux enregistrés ou les événements recherchés comme un moyen de détecter les modèles de trafic inhabituels sur votre réseau. Cette catégorie de règles comprend les types de règles suivants :

- Une règle d'anomalie teste le trafic des flux pour une activité anormale, telle qu'un trafic existant ou inconnu, qui cesse brusquement ou une variation en pourcentage dans le temps ou un objet actif. Par exemple, vous pouvez créer une règle d'anomalie pour comparer le volume moyen du trafic des cinq dernières minutes à celui de la dernière heure. S'il s'agit d'un changement de plus de 40%, la règle génère une réponse.
- **Threshold** - Une règle du seuil teste les événements et le flux de l'activité qui est inférieure, égale ou supérieure à un seuil défini, à l'intérieur ou une plage spécifiée. Un seuil peut être basé sur n'importe quelles données collectées par QRadar Network Anomaly Detection. Par exemple, si vous créez une règle de seuil indiquant que le nombre de clients qui peuvent se connecter au serveur ne doit pas dépasser 220 clients entre 08h00 et 17h00, les règles génèrent une alerte lorsque 221 clients tentent de se connecter. La règle de seuil génère une alerte lorsque le 221^{ème} client tente de se connecter.

- Une règle de comportement teste le trafic de flux pour un changement de volume dans le comportement qui se produit régulièrement dans les modèles saisonniers. Par exemple, si un serveur de messagerie communique généralement avec 100 hôtes par seconde au milieu de la nuit et puis recommence à communiquer avec 1000 hôtes par seconde, une règle de comportement génère une alerte.

Pour créer une nouvelle règle de détection d'anomalie :

Etape 1 Cliquez sur **Log Activity** ou sur **Network Activity**.

Etape 2 Effectuez une recherche.

Vos critères de recherche doivent être agrégés. La règle de détection des anomalies utilise tous les critères de filtrage et de regroupement des critères de recherche qui sont sauvegardés, mais n'utilise pas n'importe quelle plage horaire des critères de recherche. L'assistant Anomaly Detection Rule permet d'appliquer des critères d'intervalles en utilisant des tests de données et de temps.

Les résultats de la recherche s'affichent.

Etape 3 Dans le menu **Rules**, sélectionnez le type de règle que vous souhaitez créer. Ces options incluent :

- Add Anomaly Rule
- Add Threshold Rule
- Add Behavioral Rule

REMARQUE

Si vous ne souhaitez pas afficher à nouveau le message de bienvenue sur la page Rules Wizard, cochez la case **Skip this page when running the rules wizard**.

Etape 4 Lisez le texte d'introduction. Cliquez sur **Next**.

Vous êtes invité à choisir la source à partir de laquelle vous voulez que cette règle s'applique. **La valeur par défaut est le type de règle que vous avez sélectionné sur l'onglet Activity**

Etape 5 Si nécessaire, sélectionnez le type de règle que vous souhaitez appliquer à la règle. Cliquez sur **Next**.

La règle est remplie avec des tests par défaut. Vous pouvez modifier les tests par défaut ou ajouter des tests à la pile des tests. Au moins un test Accumulated Property doit être inclus dans la pile de tests.

Etape 6 Pour ajouter un test à une règle :

- a Dans la zone de liste **Test Group**, sélectionnez le type de test que vous voulez appliquer à cette règle.

REMARQUE

Pour filtrer les options dans la zone de liste **Test Group**, entrez un texte que vous voulez filtrer dans la zone **Entrez un message**.

La liste des tests s'affiche. Pour plus d'informations sur les tests, voir [Tests de règle](#).

- b Pour chaque test que vous voulez ajouter à la règle, sélectionnez le signe **+** à côté du test.

Les tests sélectionnés sont affichés dans la zone **Rule**.

- c Pour chaque test ajouté à la zone **Rule** que vous voulez identifier comme un test exclu, cliquez sur **and** au début du test.

and s'affiche comme **and not**.

- d Pour chaque test ajouté à la zone **Rule**, vous devez personnaliser la variable du test. Cliquez sur le paramètre configurable souligné pour configurer la variable. Voir [Tests de règle](#).

Par défaut, la règle teste la propriété accumulée et sélectionnée pour chaque groupe d'événements ou de flux séparément. Par exemple, si la valeur accumulée sélectionnée est UniqueCount(sourcelP), la règle teste chaque adresse IP source unique de chaque groupe d'événements/de flux

- Etape 7** Pour tester toutes les propriétés accumulées sélectionnées de chaque groupe d'événement/de flux, décochez la case **Test the [Selected Accumulated Property] value of each [group] separately**.

Il s'agit d'une zone dynamique. La valeur **[Selected Accumulated Property]** dépend de l'option que vous avez sélectionnée pour la zone de test **this accumulated property**. Pour plus d'informations sur les tests, voir [Tests de règle](#). La valeur **[group]** dépend des options de regroupement spécifiées dans les critères de recherche enregistrés. Si plusieurs options de regroupement sont incluses, le texte peut être tronqué. Déplacez le pointeur de la souris sur le texte pour afficher tous les groupes.

- Etape 8** Dans la zone **enter rule name here**, entrez un nom unique que vous voulez affecter à cette règle.

- Etape 9** Dans le panneau Groups, sélectionnez les cases à cocher des groupes auxquels vous souhaitez affecter cette règle. Pour plus d'informations sur le groupement de règles, voir [Groupement de règles](#).

- Etape 10** Dans la zone **Notes**, entrez les notes que vous voulez inclure à cette règle. Cliquez sur **Next**.

La page Rule Responses vous permet de configurer l'action que QRadar Network Anomaly Detection doit effectuer lorsque la séquence d'événements ou du flux est détectée.

- Etape 11** Configurez les paramètres :

Tableau 8-5 Paramètres de page de réponse des règles de détection des anomalies

Paramètre	Description
Rule Response	

Tableau 8-5 Paramètres de page de réponse des règles de détection des anomalies

Paramètre	Description
Dispatch New Event	Indique que cette règle envoie un nouvel événement en plus de l'événement ou du flux d'origine, qui est traité comme tous les autres événements dans le système. Par défaut cette case est sélectionnée et ne peut pas être effacée.
Event Name	Entrez un nom unique pour l'événement que vous souhaitez afficher sur l'onglet Offenses .
Event Description	Entrez une description de l'événement. La description est affichée dans le panneau Annotations des détails de l'événement.
Offense Naming	Sélectionnez une des options suivantes : <ul style="list-style-type: none"> • This information should contribute to the name of the associated offense(s) - Sélectionnez cette option si vous souhaitez que les informations du nom de l'événement contribuent au nom de la violation. • This information should set or replace the name of the associated offense(s) - Sélectionnez cette option si vous voulez que le nom de l'événement configuré soit le nom de la violation. • This information should not contribute to the naming of the associated offense(s) - Sélectionnez cette option si vous voulez que les informations du nom de l'événement ne contribuent pas au nom de la violation. < Il s'agit de la valeur par défaut.
Severity	Dans la zone de liste, sélectionnez la gravité de l'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est 5. La gravité est affichée sur le panneau Annotations des détails d'événement. Pour plus d'informations sur la gravité, voir Glossaire .
Credibility	Dans la zone de liste, sélectionnez la crédibilité de l'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est 5. La crédibilité s'affiche sur le panneau Annotations des détails d'événements. Pour plus d'informations sur la crédibilité, voir Glossaire .
Relevance	Dans la zone de liste, sélectionnez la pertinence de l'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est 5. La pertinence s'affiche sur le panneau d'annotations des détails d'événements. For more information on relevance, voir Glossaire .
High Level Category	Dans la zone de liste, sélectionnez les catégories d'événements supérieures dont vous avez besoin lors du traitement des événements. Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i> .

Tableau 8-5 Paramètres de page de réponse des règles de détection des anomalies

Paramètre	Description
Low Level Category	Dans la zone de liste, sélectionnez les catégories d'événements supérieures dont vous avez besoin lors du traitement des événements. Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i> .
Annotate this offense	Cochez cette case pour ajouter une annotation à cette violation et entrer l'annotation.
Assurer-vous que l'événement envoyé fait partie d'une violation.	En raison de cette règle, l'événement est transmis au composant Magistrate. Si une violation existe, cet événement est ajouté. Si aucune violation n'est créée sur l'onglet Offenses , une nouvelle violation est créée. Il s'agit de la valeur par défaut. Les options suivantes s'affichent : <ul style="list-style-type: none"> • Index offense based on - Indique que la nouvelle violation est basée sur le nom de l'événement. Ce paramètre est activé par défaut. • Include detected events by Event Name from this point forward, for second(s), in the offense - Cochez la case et entrez le nombre de secondes à inclure aux événements ou aux flux détectés à partir de la source sur l'onglet Offenses
Email	Cochez cette case pour afficher les options de courrier électronique. Par défaut, la case est vide.
Enter email address to notify	Entrez l'adresse de courrier électronique pour envoyer une notification si cette règle est générée. S'il y a plusieurs adresses de courrier électronique, séparez-les par une virgule.
Alerte SNMP	Ce paramètre ne s'affiche que lorsque les paramètres SNMP sont configurés dans les paramètres du système. Pour plus d'informations sur la configuration des paramètres du système, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i> . ▶ Activez cette règle en cochant cette case pour envoyer une notification SNMP (interruption). La sortie d'alerte SNMP inclut l'heure du système, l'ID objet de l'interruption et la notification des données, tels que définis par Q1 Labs MIB. Par exemple, la notification SNMP peut ressembler à : <code>"Wed Sep 28 12:20:57 GMT 2005, QRADAR Custom Rule Engine Notification - Rule 'SNMPTRAPTest' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name: ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes: Offense description"</code>

Tableau 8-5 Paramètres de page de réponse des règles de détection des anomalies

Paramètre	Description
Notify	<p>Cochez cette case si vous voulez que les événements qui se génèrent à la suite de cette règle s'affichent dans l'élément du système de notifications sur l'onglet Dashboard.</p> <p>Pour plus d'informations sur l'onglet Dashboard, voir Utilisation de l'onglet Dashboard.</p> <p>Remarque : Si vous activez les notifications, nous vous recommandons de configurer le paramètre Response Limiter</p>
Send to Local SysLog	<p>Cochez cette case si vous voulez consigner l'événement ou le transporter localement. Par défaut, la case est vide.</p> <p>Par exemple, la sortie syslog peut ressembler à :</p> <pre>Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description</pre>

Tableau 8-5 Paramètres de page de réponse des règles de détection des anomalies

Paramètre	Description
Add to Reference Set	<p>Cochez cette option si vous voulez que les événements qui se génèrent à la suite de cette règle ajoutent des données à l'ensemble de référence.</p> <p>Pour ajouter des données à l'ensemble de références :</p> <ol style="list-style-type: none"> 1 Dans la zone de liste, sélectionnez les données que vous voulez ajouter. Les options incluent toutes les données normalisées ou personnalisées. 2 Dans la zone de liste, sélectionnez l'ensemble de références que vous voulez ajouter aux données spécifiées. <p>La réponse à la règle Add to Reference Set offre les fonctions suivantes :</p> <ul style="list-style-type: none"> • New - Cliquez sur cette icône pour ajouter un nouvel ensemble de références et configurer les paramètres suivants : Après avoir cliqué sur New, vous devez configurer les éléments suivants : <ul style="list-style-type: none"> Nom - Entrez un nom unique pour l'ensemble de référence. Type - Dans la zone de liste, sélectionnez le type de données. Les options incluent String, Numeric, IP et Port. Maximum number of elements - Entrez le nombre maximum d'éléments de données à stocker dans l'ensemble de références. La valeur par défaut est 10.000 et le maximum est 100.000. • Edit - Cliquez sur Edit pour modifier le nom de l'ensemble de références et le nombre maximum des éléments de données de l'ensemble de références sélectionné. • Delete - Cliquez sur Delete pour supprimer l'ensemble de références. • Purge - Cliquez sur Purge pour supprimer le contenu de l'ensemble de références tout en maintenant l'ensemble de références.
Publish on the IF-MAP Server	<p>Si les paramètres IF-MAP sont configurés et déployés dans les paramètres du système, sélectionnez cette option pour publier les informations de l'événement sur le serveur IF-MAP. Pour plus d'informations sur la configuration des paramètres IF-MAP, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>
Response Limiter	<p>Cochez la case et utilisez la zone de liste pour configurer la fréquence à laquelle cette règle doit répondre.</p>
Enable Rule	<p>Cochez cette case pour activer cette règle. Par défaut, la case est cochée.</p>

Etape 12 Cliquez sur **Next**.

Etape 13 Vérifiez la règle configurée. Cliquez sur **Finish**.

Gestion règles

En utilisant la fonction des règles sur l'onglet **Offenses**, vous pouvez gérer les règles personnalisées et l'anomalie. Vous pouvez activer ou désactiver les règles, si nécessaire. En plus, vous pouvez modifier, copier ou supprimer la règle.

Cette section comprend les rubriques suivantes :

- [Activation / désactivation de règle](#)
- [Modification d'une règle](#)
- [Copie d'une règle](#)
- [Suppression d'une règle](#)

REMARQUE

La fonctionnalité anomaly detection figurant dans les onglets **Log Activity** et **Network Activity** permet uniquement de créer des règles de détection d'anomalies. Pour gérer les règles de détection d'anomalies par défaut ou précédemment créées, vous devez utiliser l'onglet **Offenses**

Activation / désactivation de règle

Lors du réglage de votre système, vous pouvez activer ou désactiver les règles appropriées pour s'assurer que votre système génère des violations importantes pour votre environnement.

Pour activer ou désactiver une règle :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Dans le menu de la navigation, cliquez sur **Rules**.
- Etape 3** Dans la zone de liste **Display**, sélectionnez **Rules**.
- Etape 4** =Sélectionner la règle que vous souhaitez activer ou désactiver.
- Etape 5** Dans la zone de liste **Actions**, sélectionnez **Enable/Disable**.

La colonne **Enabled** indique le statut.

Modification d'une règle

Vous pouvez modifier une règle pour changer le nom de la règle, le type de la règle, les tests ou les réponses.

Pour modifier une règle :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Dans le menu de navigation, cliquez sur **Rules**.
- Etape 3** Dans la zone de liste **Display**, sélectionnez **Rules**.
- Etape 4** Sélectionnez la règle que vous souhaitez modifier.
- Etape 5** Dans la zone de liste **Actions**, sélectionnez **Edit**.
- Etape 6** Modifiez les paramètres. Voir [Tableau 8-1](#).
- Etape 7** Facultatif. Si vous voulez changer le type de règle, cliquez sur **Back** et sélectionnez un nouveau type de règle.

Etape 8 Cliquez sur **Next**.

Etape 9 Modifiez les paramètres :

- Consultez [Tableau 8-3](#) pour le flux d'événement, ou les paramètres de règles communes.
- Voir [Tableau 8-4](#) pour les paramètres de règles d'anomalies.
- Consultez [Tableau 8-5](#) pour les paramètres de règles de détection d'anomalies.

Etape 10 Cliquez sur **Next**.

Etape 11 Vérifiez la règle configurée. Cliquez sur **Finish**.

Copie d'une règle Pour créer une nouvelle règle, vous pouvez copier une règle existante, entrer un nouveau nom pour la règle, puis personnaliser les paramètres de la nouvelle règle selon les besoins.

Pour copier une règle :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de navigation, cliquez sur **Rules**.

Etape 3 Dans la zone de liste **Display**, sélectionnez **Rules**.

Etape 4 Sélectionnez la règle que vous souhaitez dupliquer.

Etape 5 Dans la zone de liste **Actions**, sélectionnez **Duplicate**.

Etape 6 Dans la zone **Enter name for the copied rule**, entrez un nom pour la nouvelle règle. Cliquez sur **OK**.

Pour plus d'informations sur la modification des règles, voir [Modification d'une règle](#).

Suppression d'une règle QRadar Network Anomaly Detection vous permet de supprimer des règles. La suppression d'une règle supprime la règle complètement de votre système.

Pour supprimer une règle :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de navigation, cliquez sur **Rules**.

Etape 3 Dans la zone de liste **Display**, Sélectionnez **Rules**.

Etape 4 Sélectionnez la règle que vous souhaitez supprimer.

Etape 5 Dans la zone de liste **Actions**, sélectionnez **Delete**.

Groupement d'une règle

Si vous êtes un administrateur, vous êtes en mesure de créer, modifier et supprimer des groupes de règles. Vous pouvez regrouper et afficher vos règles et des blocs de construction en fonction de vos critères choisis. Le classement de vos règles ou de vos blocs de construction en groupes vous permettent de visualiser et suivre efficacement vos règles. Par exemple, vous pouvez afficher

toutes les règles relatives à la conformité. Par défaut, l'onglet des Rules affiche toutes les règles et le renforcement des blocs de construction.

Lorsque vous créez de nouvelles règles, vous pouvez assigner la règle à un groupe existant. Pour plus d'informations sur l'attribution d'un groupe à l'aide de l'assistant des règles, voir [Création d' une règle personnalisée](#) ou [Création d'une règle de détection des anomalies](#).

Cette section comprend les rubriques suivantes :

- [Affichage des groupes](#)
- [Creating a Group](#)
- [Modification d'un groupe](#)
- [Copie d'un élément vers un autre groupe](#)
- [Suppression d'un élément du groupe](#)
- [Affectation d'un élément à un groupe](#)

Affichage des groupes Dans l'onglet des Rules, vous pouvez filtrer les règles ou les blocs de construction pour afficher uniquement les règles ou les blocs de construction appartenant à un groupe particulier.

Pour voir les règles ou les groupes de blocs de construction :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Dans le menu de navigation, cliquez sur **Rules**.
- Etape 3** Dans la zone de liste, sélectionnez si vous voulez afficher les règles ou les blocs de construction
- Etape 4** Dans la zone de liste **Filter** sélectionnez la catégorie du groupe que vous souhaitez afficher.

La liste des éléments affectés aux groupes s'affiche.

Création d'un Groupe L'onglet Rules prévoit un groupe de règles par défaut. Cependant, vous pouvez créer un nouveau groupe.

Pour créer un groupe :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Dans le menu de navigation, cliquez sur **Rules**.
- Etape 3** Cliquez sur **Groups**.
- Etape 4** Dans l'arborescence de navigation, sélectionnez le groupe sous lequel vous souhaitez créer un nouveau groupe.

REMARQUE

Lorsque vous créez le groupe, vous pouvez faire glisser les éléments d'arborescence de navigation pour changer l'organisation des éléments de l'arborescence.

- Etape 5** Cliquez sur **New Group**.
- Etape 6** Entrez les valeurs des paramètres suivants :
 - **Name** - Entrez un nom unique à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.

- **Description** - Entrez une description à affecter au nouveau groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers un emplacement choisi dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Group.

Modification d'un groupe Vous pouvez également modifier un nom de groupe ou une description.

Pour modifier un groupe:

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de navigation, cliquez sur **Rules**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de navigation, sélectionnez le groupe que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

Etape 6 Mettez à jour les valeurs des paramètres suivants :

- **Name** - Entrez un nom unique à affecter au nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description à affecter au nouveau groupe. La description peut contenir plus de 255 caractères.

Etape 7 Cliquez sur **OK**.

Etape 8 Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers un emplacement choisi dans votre arborescence de menus.

Etape 9 Fermez la fenêtre Group.

Copie d'un élément vers un autre groupe En utilisant la fonctionnalité des groupes, vous pouvez copier une règle ou un bloc de construction vers un ou plusieurs groupes. Pour déplacer une règle ou un bloc de construction :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de navigation, cliquez sur **Rules**.

Etape 3 Cliquez sur **Groups**.

Etape 4 Dans l'arborescence de navigation, sélectionnez la règle ou le bloc de construction que vous souhaitez copier vers un autre groupe.

Etape 5 Cliquez sur **Copy**.

Etape 6 Cochez la case du groupe vers lequel que vous souhaitez copier la règle ou le bloc de construction.

Etape 7 Cliquez sur **Copier**.

Etape 8 Fermez la fenêtre Group.

Suppression d'un élément du groupe La suppression d'un élément d'un groupe ne supprime pas la règle ou le bloc de construction à partir de l'onglet Rules.

Pour supprimer une règle ou un bloc de construction d'un groupe :

Etape 1 Cliquez sur l'onglet **Offense**

Etape 2 Dans le menu de navigation, cliquez sur **Rules**.

Etape 3 Cliquez sur **Groups**.

Etape 4 En utilisant l'arborescence de navigation, recherchez et sélectionnez l'élément que vous souhaitez supprimer.

Etape 5 Cliquez sur **Remove**.

Etape 6 Cliquez sur **OK**.

Etape 7 Fermez la fenêtre Group.

Suppression d'un groupe La suppression d'un élément d'un groupe ne supprime pas la règle ou le bloc de construction à partir de l'onglet Rules.

Pour supprimer un groupe :

Etape 1 Cliquez sur l'onglet **Offense**

Etape 2 Dans le menu de navigation, cliquez sur **Rules**.

Etape 3 Cliquez sur **Groups**.

Etape 4 En utilisant l'arborescence de navigation, recherchez et sélectionnez l'élément que vous souhaitez supprimer.

Etape 5 Cliquez sur **Remove**.

Etape 6 Cliquez sur **OK**.

Etape 7 Fermez la fenêtre Group.

Affectation d'un élément à un groupe Pour affecter une règle ou un bloc de construction à un groupe :

Etape 1 Cliquez sur l'onglet **Offenses**.

Etape 2 Dans le menu de navigation, cliquez sur **Rules**.

Etape 3 Sélectionnez une règle ou un bloc de construction que vous souhaitez affecter à un groupe.

Etape 4 Dans la zone de liste **Actions**, sélectionnez **Assign Groups**.

Etape 5 Cochez la case du groupe sur lequel vous souhaitez copier la règle ou le bloc de construction.

Etape 6 Cliquez sur **Assign Groups**.

Etape 7 Fermez la fenêtre Choose Groups.

Modification d'un bloc de construction

Les blocs de construction vous permettent de réutiliser des règles spécifiques et des tests dans d'autres règles. Par exemple, vous pouvez enregistrer un bloc de construction qui exclut les adresses IP de tous les serveurs de messagerie dans le déploiement de votre règle.

Pour plus d'informations sur les blocs de construction par défaut, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Pour modifier un bloc de construction :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Dans le menu de la navigation, cliquez sur **Rules**.
- Etape 3** Dans la zone de liste **Display**, sélectionnez **Building Blocks**.
- Etape 4** Faites un double-clic sur le bloc de construction que vous souhaitez éditer.
- Etape 5** Mettez à jour le bloc de construction, au besoin. Cliquez sur **Next**.
- Etape 6** Continuez avec l'assistant. Pour plus d'informations, voir [Création d' une règle personnalisée](#).
- Etape 7** Cliquez sur **Finish**.

9

GESTION DES ACTIFS

L'onglet Assets vous permet de gérer les actifs fonctionnant sur votre réseau.

Cette section comprend les rubriques suivantes :

- [Présentation de l'onglet Asset](#)
- [Affichage des profils d'actif](#)
- [Affichage des détails de vulnérabilité](#)
- [Gestion des profils d'actif](#)
- [Utilisation de la fonction de recherche](#)

Présentation de l'onglet Asset

IBM Security QRadar Network Anomaly Detection détecte automatiquement les actifs (serveurs et hôtes) fonctionnant sur votre réseau, à partir des données de flux passifs et des données de vulnérabilité, afin de créer des profils d'actif. Les profils d'actif fournissent des informations sur chaque actif connu sur votre réseau, y compris les services qui s'exécutent sur chaque actif. Les informations de profil d'actif sont utilisées à des fins de corrélation afin de réduire les faux positifs. Par exemple, si une source tente d'exploiter un service spécifique en cours d'exécution sur un actif spécifique, QRadar Network Anomaly Detection peut déterminer si l'actif est vulnérable aux attaques en mettant en corrélation l'attaque avec le profil d'actif.

L'onglet **Assets** vous permet de :

- Rechercher des actifs spécifiques.
- Voir tous les actifs étudiés.
- Afficher les informations d'identité des actifs étudiés.
- Ajouter manuellement les profils d'actif.
- Modifier les profils d'actif pour les actifs ajoutés ou découverts manuellement.
- Ajuster les vulnérabilités de faux positifs.
- Imprimer ou exporter des profils d'actif.

REMARQUE

Les profils d'actif sont uniquement remplis si des données de flux ou des analyses d'évaluation de la vulnérabilité (VA) sont configurées. Pour que les données de flux remplissent les profils d'actif, des flux bidirectionnels sont nécessaires. Pour plus d'informations sur VA, voir le *Guide de configuration de l'évaluation de la vulnérabilité IBM Security QRadar*. Pour plus d'informations sur les sources de flux, voir le *Guide d'administration IBM Security QRadar Network Anomaly Detection*.

Affichage des profils d'actif

Pour afficher les profils d'actif :

- Etape 1** Cliquez sur l'onglet **Assets**.
- Etape 2** Effectuez une recherche. Voir [Utilisation de la fonction de recherche](#).

Les résultats de la recherche s'affichent et indiquent les informations suivantes :

Tableau 9-1 Page Asset Search Results

Paramètre	Description
IP Address	Indique l'adresse IP des actifs.
MAC	Indique la dernière adresse MAC connue de l'actif.
Name	Indique le nom, le nom d'hôte ou le nom de l'ordinateur des actifs. Si cette information n'est pas connue, cette zone est vide.
User	Indique le dernier utilisateur connu de l'actif. Si cette information n'est pas connue, cette zone est vide.
Group	Indique le dernier groupe d'utilisateurs connu de l'actif. Si cette information n'est pas connue, cette zone est vide.
Network	Indique le réseau auquel l'actif appartient.
Weight	Indique la pondération de l'actif.
Risk Level	Indique le niveau de risque des actifs.
Vulnerabilities	Indique le nombre des vulnérabilités identifiées associés à cet actif. Cette valeur inclut également le nombre de vulnérabilités actives et passives.
Last Seen	Indique la date et l'heure auxquelles l'actif a été observé pour la dernière fois. Si l'actif a été saisi manuellement, mais qu'il n'a jamais été observé de façon active ou passive, la colonne indique Never.

La barre d'outils de la page des résultats de la recherche d'actifs fournit les fonctions suivantes :

Tableau 9-2 Barre d'outils de la page des résultats de la recherche d'actifs

Fonction	Description
Modify Search	Cliquez sur Modify Search pour revenir à la page Assets Search et modifier vos critères de recherche. Voir Affichage des profils d'actif .

Tableau 9-2 Barre d'outils de la page des résultats de la recherche d'actifs (suite)

Fonction	Description
Add Asset	Cliquez sur Add Asset pour ajouter un profil d'actif. Voir Ajout d'un profil d'actif .
Edit Asset	Cliquez sur Edit Asset pour modifier un profil d'actif. Cette option est uniquement activée si vous avez sélectionné un profil d'actif dans la liste des résultats. Voir Modification d'un actif .
Actions	<p>Cliquez sur Actions pour effectuer les actions suivantes :</p> <ul style="list-style-type: none"> • Delete Asset - Sélectionnez cette option pour supprimer les profils d'actif sélectionnés. Voir Suppression d'un actif. • Delete Listed - Sélectionnez cette option pour supprimer tous les profils d'actif énumérés dans la liste des résultats. Voir Suppression de tous les actifs. • Import Assets - Sélectionnez cette option pour importer des actifs. Voir Importation de profils d'actif. • Export to XML - Sélectionnez cette option pour exporter des profils d'actif au format XML. Voir Exportation des actifs. • Export to CSV - Sélectionnez cette option pour exporter des profils d'actif au format CSV. Voir Exportation des actifs. <p><i>Remarque : Le menu Actions n'est disponible que si vous disposez des privilèges d'administration. Pour plus d'informations, voir IBM Security QRadar Network Anomaly Detection Administration Guide.</i></p>
Print	Cliquez sur Print pour imprimer les profils d'actif affichés sur la page.

REMARQUE

Pour afficher des informations supplémentaires sur cet actif, déplacez votre souris sur l'adresse IP.

Etape 3 Pour afficher les détails d'un actif, cliquez deux fois dessus.

La page Asset Profile fournit les fonctions suivantes :

Tableau 9-3 Barre d'outils de la page Asset

Fonction	Description
Return to Asset List	Cliquez sur Return to Asset List pour revenir à la page des résultats de la recherche d'actifs.
Modify Search	Cliquez sur Modify Search pour revenir à la page Assets Search et modifier vos critères de recherche. Voir Affichage des profils d'actif .
Print	Cliquez sur Print pour imprimer les profils d'actif affichés sur la page.

La page Asset Profile fournit les informations suivantes :

REMARQUE

Vous pouvez modifier certains paramètres directement sur la page Asset Profile. Pour modifier un paramètre directement à partir de la page Asset Profile, apportez les modifications nécessaires, puis cliquez sur **Save Changes**.

Tableau 9-4 Page Asset Profile

Paramètre	Description
Name	Indique le nom des actifs.
Description	Indique une description pour cet actif.
IP Address	Indique l'adresse IP des actifs.
Network	Indique le réseau auquel l'actif appartient.
Host Name (DNS Name)	Indique le nom DNS ou l'adresse IP de l'actif, si cette information est connue.
Risk Level	Indique le niveau de risque (0 à 10) pour l'actif, où 0 est le niveau le plus bas et 10 le plus élevé. Il s'agit d'une valeur pondérée par rapport à l'ensemble des autres hôtes présents dans votre déploiement.
Operating System	Indique le système d'exploitation exécuté sur l'actif. <i>Remarque : Vous pouvez directement éditer ce paramètre si le paramètre Override est défini en tant que Override Until the Next Scan ou Override Forever. A partir de la zone de liste, sélectionnez le nom du système d'exploitation.</i>
Vendor	Indique le nom du fournisseur du système d'exploitation de l'actif, tel que détecté par le scanner VA ou entré manuellement. <i>Remarque : Vous pouvez directement éditer ce paramètre si le paramètre Override est défini en tant que Override Until the Next Scan ou Override Forever. A partir de la zone de liste, sélectionnez le nom du fournisseur du système d'exploitation.</i>
Version	Indique la version du système d'exploitation. <i>Remarque : Vous pouvez éditer ce paramètre si le paramètre Override est défini en tant que Override Until the Next Scan ou Override Forever. A partir de la zone de liste, sélectionnez la version du système d'exploitation.</i>

Tableau 9-4 Page Asset Profile (suite)

Paramètre	Description
Override	<p>Le paramètre Override définit la méthode utilisée pour dériver les informations du système d'exploitation (paramètres Operating System, Vendor et Version). A partir de la zone de liste, sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> • Detected By a Scanner - Sélectionnez cette option pour indiquer que le scanner fournit des informations sur le système d'exploitation. • Override Until the Next Scan - Sélectionnez cette option pour indiquer que le scanner fournit des informations sur le système d'exploitation et que les informations peuvent être temporairement modifiées. Si vous éditez les paramètres du système d'exploitation, le scanner restaure les informations au moment de sa prochaine analyse. Il s'agit de la valeur par défaut. • Override Forever - Sélectionnez cette option pour indiquer que vous souhaitez entrer manuellement des informations sur le système d'exploitation et désactiver la mise à jour des informations par le scanner.
Asset Weight	Indique le niveau d'importance associé à cet actif. La plage est comprise entre 0 (pas important) et 10 (très important).
MAC	Indique la dernière adresse MAC connue de l'actif.
Machine Name	Indique le dernier nom connu de la machine de l'actif.
Username	Indique le dernier utilisateur connu de l'actif.
Extra Data	Indique les informations étendues basées sur un événement.
Host Name	Indique le dernier nom d'hôte connu de l'actif.
User Group	Indique le dernier groupe d'utilisateurs connu de l'actif.
Business Owner	Indique le nom du propriétaire fonctionnel de l'actif. Un directeur de service est un exemple de propriétaire technique.
Business Owner Contact Info	Indique les informations de contact du propriétaire fonctionnel.
Technical Owner	Indique le propriétaire technique de l'actif. Un responsable informatique ou un directeur est un exemple de propriétaire technique.
Technical Owner Contact Info	Indique les informations de contact du propriétaire technique.
Location	Indique l'emplacement physique de l'actif.

La barre d'outils Asset Profile fournit les options suivantes :

Tableau 9-5 Barre d'outils des profils d'actif

Options	Description
View by Network	Si cet actif est associé à une infraction, cette option vous permet d'afficher la liste des réseaux associés à cet actif. Lorsque vous cliquez sur View By Network , la fenêtre List of Networks s'affiche. Voir Affichage des violations par réseau .
View Source Summary	Si cet actif est la source d'une infraction, cette option vous permet d'afficher des informations récapitulatives sur la source. Lorsque vous cliquez sur l'option View Source Summary , la fenêtre List of Offenses s'affiche. Voir Affichage des violations par IP sources .
View Destination Summary	Si cet actif est la destination d'une infraction, cette option vous permet d'afficher les informations récapitulatives sur la destination. Lorsque vous cliquez sur l'option View Destination Summary , la fenêtre List of Destinations s'affiche. Voir Affichage des violations par IP cible .
History	<p>Cliquez sur l'option History pour afficher les informations historiques des événements de cet actif. Lorsque vous cliquez sur l'icône History, la fenêtre Event Search s'affiche. Elle est préremplie avec les critères de recherche d'événement suivants :</p> <ul style="list-style-type: none"> • Time Range - Recent (Last 24 Hours) • Search Parameters - Indique les filtres suivants à appliquer aux résultats de la recherche : <ul style="list-style-type: none"> - Identity is true - Identity IP is the IP address of the asset • Column Definition - Indique les colonnes suivantes à afficher dans les résultats de la recherche : <ul style="list-style-type: none"> - Event name - Log Source - Start Time - Identity User Name - Identity MAC - Identity Host Name - Identity Net Bios Name - Identity Group Name <p>Vous pouvez personnaliser les paramètres de recherche, si nécessaire. Cliquez sur Search pour afficher les informations historiques d'événement. Pour plus d'informations sur la recherche d'événements, voir Recherche d'événements ou flux.</p>

Tableau 9-5 Barre d'outils des profils d'actif (suite)

Options	Description
Applications	<p>Cliquez sur Applications pour afficher les informations d'application de cet actif. Lorsque vous cliquez sur l'icône Applications, la fenêtre de recherche de flux s'affiche, préremplie avec les critères de recherche d'événements suivants :</p> <ul style="list-style-type: none"> • Time Range - Recent (Last 24 Hours) • Search Parameters - Indique le filtre suivant à appliquer aux résultats de la recherche : L'adresse IP source ou cible est l'adresse IP de l'actif. • Column Definition - Indique la colonne Application Group à afficher dans les résultats de la recherche. <p>Vous pouvez personnaliser les paramètres de recherche, si nécessaire. Cliquez sur Search pour afficher les informations de l'application. Pour plus d'informations sur la recherche de flux, voir Recherche d'événements ou flux.</p>

Le panneau Ports and Vulnerabilities de la page Asset Profile affiche les informations suivantes :

Tableau 9-6 Informations sur les ports

Paramètre	Description
Port	Indique le numéro de port pour les services reconnus en cours d'exécution sur l'actif.
Service	Indique les services reconnus en cours d'exécution sur l'actif.
OSVDB ID	Spécifie l'identifiant de vulnérabilité de l'actif. Cliquez sur l'ID pour obtenir plus d'informations.
Name	Spécifie le nom de la vulnérabilité détectée. Cette valeur est uniquement disponible lors de l'intégration avec les outils VA.
Description	Indique une description de la vulnérabilité détectée. Cette valeur est uniquement disponible lors de l'intégration avec les outils VA.
Risk/Severity	Indique le niveau de risque de la vulnérabilité (de 0 à 10).
Last Seen	Indique la date et l'heure auxquelles le service a été détecté pour la dernière fois en cours d'exécution sur l'actif de façon passive ou active.
First Seen	Indique la date et l'heure auxquelles le service a été détecté pour la première fois en cours d'exécution sur l'actif de façon passive ou active.

Tableau 9-6 Informations sur les ports (suite)

Paramètre	Description
False Positive Tuning	<p>Cliquez sur False Positive Tuning pour supprimer les vulnérabilités sélectionnées de la liste.</p> <p>Remarque : Cette option est uniquement disponible si vous disposez de l'une des autorisations utilisateur suivantes : <i>Admin</i> ou <i>Remove Vulnerabilities</i>. Pour plus d'informations, voir <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>.</p>

Affichage des détails de vulnérabilité

Les scanners tiers identifient et signalent les vulnérabilités découvertes à QRadar Network Anomaly Detection à l'aide de références externes, telles que l'Open Source Vulnerability Database (OSVDB) et la National Vulnerability Database (NVD). QualysGuard et nCircle ip360 sont des exemples de scanners tiers. La base de données OSVDB assigne un identifiant de référence unique (OSVDB ID) à chaque vulnérabilité. En outre, les références de données externes peuvent identifier les vulnérabilités avec un ID. Un ID Common Vulnerability and Exposures (CVE) ou un ID Bugtraq sont des exemples d'ID de référence de données externe.

Pour plus d'informations sur les scanners et l'évaluation de la vulnérabilité, voir le *Guide de configuration de l'évaluation de la vulnérabilité IBM Security QRadar*.

Cette procédure suppose que la page Asset Profile de l'onglet **Assets** est affichée et que vous souhaitez étudier les détails d'une vulnérabilité répertoriée dans le panneau Ports and Vulnerabilities. Si aucune page Asset Profile n'est affichée, voir [Affichage des profils d'actif](#).

- ▶ Pour afficher les détails de vulnérabilité, choisissez l'une des possibilités suivantes :
 - Dans le panneau Ports and Vulnerabilities, cliquez deux fois sur la ligne de la vulnérabilité que vous souhaitez afficher.
 - Dans le panneau Ports and Vulnerabilities, cliquez sur le lien dans le paramètre **Name** de la vulnérabilité que vous souhaitez afficher.

La fenêtre Research Vulnerability Details fournit les détails suivants :

Tableau 9-7 Détails de la fenêtre Research Vulnerabilities Details

Paramètre	Description
Vuln ID	Indique l'ID de la vulnérabilité. Le paramètre Vuln ID est un identifiant unique généré par Vulnerability Information System (VIS).
Published Date	Indique la date à laquelle les détails de la vulnérabilité ont été publiés sur la base de données OSVDB.
Name	Indique le nom de la vulnérabilité.

Tableau 9-7 Détails de la fenêtre Research Vulnerabilities Details (suite)

Paramètre	Description
CVE	<p>Indique l'identifiant CVE de la vulnérabilité. Les identifiants CVE sont fournis par la base de données NVDB.</p> <p>► Cliquez sur le lien pour obtenir plus d'informations. Le site Web NVDB s'affiche dans une nouvelle fenêtre de navigateur.</p>
OSVDB	<p>Indique l'identifiant OSVDB de la vulnérabilité.</p> <p>► Cliquez sur le lien pour obtenir plus d'informations. Le site Web OSVDB s'affiche dans une nouvelle fenêtre de navigateur.</p>
CVSS Score	<p>Indique le score Common Vulnerability Scoring System (CVSS) de la vulnérabilité.</p> <p>Un score CVSS est une valeur permettant d'évaluer la gravité d'une vulnérabilité. Vous pouvez utiliser les scores CVSS pour mesurer les inquiétudes justifiées par une vulnérabilité par rapport à d'autres vulnérabilités. Pour plus d'informations sur CVSS, voir http://www.first.org/cvss/.</p>
Description	Indique une description de la vulnérabilité détectée. Cette valeur est uniquement disponible lors de l'intégration avec les outils VA.
Concern	Indique les effets que la vulnérabilité peut avoir sur votre réseau.
Solution	Suivez les instructions fournies pour résoudre la vulnérabilité.
IPS/IDS Mitigation	<p>Affiche des informations sur le périphérique Intrusion Prevention System/Intrusion Detection System (IPS/IDS) associé à cette vulnérabilité.</p> <p>Le tableau IPS/IDS Mitigation affiche les informations suivantes :</p> <ul style="list-style-type: none"> • QID - Indique le QID associé à cette vulnérabilité. Un QID assigne une catégorie de niveau supérieur et de niveau inférieur d'identifiant unique à un événement unique provenant d'un périphérique externe. • Device Type - Indique le type de périphérique associé au QID. • Signature - Indique la signature émise par le périphérique IPS/IDS.

Tableau 9-7 Détails de la fenêtre Research Vulnerabilities Details (suite)

Paramètre	Description
Reference	<p>Affiche la liste des références externes, y compris :</p> <ul style="list-style-type: none"> • Reference Type - Indique le type de référence répertoriée, tel qu'une adresse URL de recommandation ou une liste de publication des messages. • URL - Indique l'adresse URL sur laquelle vous pouvez cliquer pour afficher la référence. <p>► Cliquez sur le lien pour obtenir plus d'informations. Lorsque vous cliquez sur le lien, la ressource externe s'affiche dans une nouvelle fenêtre de navigateur.</p>
Products	<p>Affiche la liste des produits qui sont associés avec cette vulnérabilité.</p> <ul style="list-style-type: none"> • Vendor - Indique le fournisseur du produit. • Product - Indique le nom du produit. • Version - Indique le numéro de version du produit.

Gestion des profils d'actif

Cette section comprend les rubriques suivantes :

- [Ajout d'un profil d'actif](#)
- [Modification d'un actif](#)
- [Suppression des actifs](#)
- [Importation de profils d'actif](#)
- [Exportation des actifs](#)

Ajout d'un profil d'actif Pour ajouter un profil d'actif :

REMARQUE

QRadar Network Anomaly Detection détecte et ajoute automatiquement les profils d'actif ; c'est pourquoi il n'est généralement pas nécessaire d'ajouter un profil d'actif.

Etape 1 Cliquez sur l'onglet **Assets**.

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

Etape 3 Cliquez sur **Add Asset**.

Etape 4 Entrez des valeurs pour les paramètres :

Tableau 9-8 Paramètres d'ajout d'un profil d'actif

Paramètre	Description
IP	Entrez l'adresse IP ou la plage CIDR de l'actif.
Asset Name	Entrez le nom de l'actif. Ce paramètre est sensible à la casse. La longueur maximale est de 255 caractères.
Description	Entrez la description de l'actif. La longueur maximale est de 255 caractères.
Asset Weight	A partir de la zone de liste, entrez la pondération à affecter à cet actif. L'intervalle est compris entre 0 et 10. La valeur par défaut est 0.
Business Owner	Entrez le nom du propriétaire fonctionnel de l'actif. Un directeur de service est un exemple de propriétaire fonctionnel. La longueur maximale est de 255 caractères.
Business Owner Contact Info	Entrez les informations de contact du propriétaire fonctionnel. La longueur maximale est de 255 caractères.
Technical Owner	Entrez le propriétaire technique de l'actif. Un responsable informatique ou un directeur sont des exemples de propriétaire fonctionnel. La longueur maximale est de 255 caractères.
Technical Owner Contact Info	Entrez les informations de contact du propriétaire technique. La longueur maximale est de 255 caractères.
Location	Entrez l'emplacement physique de l'actif. La longueur maximale est de 255 caractères.

Etape 5 Cliquez sur **Save**.

Après avoir ajouté un profil d'actif, vous pouvez modifier le profil pour configurer des paramètres de profil d'actif supplémentaires, tels que les informations sur le propriétaire fonctionnel et sur le système d'exploitation. Voir [Modification d'un actif](#).

Modification d'un actif

Pour modifier un actif :

- Etape 1** Cliquez sur l'onglet **Assets**.
- Etape 2** Dans le menu de navigation, cliquez sur **Asset Profiles**.
- Etape 3** Recherchez des profils d'actif.
Pour plus d'informations sur les profils d'actif de recherche, voir [Affichage des profils d'actif](#)
- Etape 4** Dans la liste des actifs, sélectionnez l'actif que vous souhaitez modifier.
- Etape 5** Cliquez sur **Edit Asset**.
- Etape 6** Editez les paramètres. Pour plus d'informations sur les paramètres, voir [Tableau 9-4](#).
- Etape 7** Cliquez sur **Save Changes**.

Suppression des actifs

Vous pouvez supprimer des actifs spécifiques ou l'ensemble des actifs découverts par une recherche. Cette section comprend les rubriques suivantes :

- [Suppression d'un actif](#)
- [Suppression de tous les actifs](#)

Suppression d'un actif

Pour supprimer un actif :

- Etape 1** Cliquez sur l'onglet **Assets**.
- Etape 2** Dans le menu de navigation, cliquez sur **Asset Profiles**.
- Etape 3** Recherchez des profils d'actif.
Pour plus d'informations sur les profils d'actif de recherche, voir [Affichage des profils d'actif](#).
- Etape 4** A partir de la liste des actifs, sélectionnez l'actif que vous souhaitez supprimer.

REMARQUE

Pour supprimer plusieurs actifs, utilisez la touche de contrôle pour sélectionner plusieurs actifs.

- Etape 5** A partir de la zone de liste **Actions**, sélectionnez **Delete Asset**.
- Etape 6** Cliquez sur **OK**.

Suppression de tous les actifs

Pour supprimer tous les actifs :

- Etape 1** Cliquez sur l'onglet **Assets**.
- Etape 2** Dans le menu de navigation, cliquez sur **Asset Profiles**.
- Etape 3** Recherchez des profils d'actif.

Pour plus d'informations sur les profils d'actif de recherche, voir [Affichage des profils d'actif](#).

Etape 4 Dans la zone de liste **Actions**, sélectionnez **Delete Listed**.

Etape 5 Cliquez sur **OK**.

Importation de profils d'actif Vous pouvez importer des informations de profil d'actif dans QRadar Network Anomaly Detection. Le fichier importé doit être un fichier CSV respectant le format suivant :

```
ip,name,weight,description
```

Où :

- **IP** - Indique une adresse IP valide selon la notation décimale à points. Par exemple : 192.168.5.34.
- **Name** - Indique le nom de cet actif pouvant contenir jusqu'à 255 caractères. Les virgules ne sont pas acceptées dans cette zone et invalident le processus d'importation. Par exemple : WebServer01 est correct.
- **Weight** - Indique un nombre compris entre 0 et 10, qui correspond à l'importance de cet actif sur votre réseau. Une valeur égale à 0 représente une importance faible et une valeur égale à 10 une importance très élevée.
- **Description** - Indique une description textuelle de cet actif pouvant contenir jusqu'à 255 caractères. Cette valeur est facultative.

Par exemple, les entrées suivantes peuvent être incluses dans un fichier CSV :

```
192.168.5.34,WebServer01,5,Serveur Web de production principal
192.168.5.35,MailServ01,0,
```

Le processus d'importation fusionne les profils d'actif importés avec les informations de profil d'actif qui sont actuellement stockées dans le système.

REMARQUE

Si une erreur se produit pendant le processus d'importation, aucun actif n'est importé.

Pour importer des profils d'actif :

- Etape 1** Cliquez sur l'onglet **Assets**.
- Etape 2** Dans le menu de navigation, cliquez sur **Asset Profiles**.
- Etape 3** Cliquez sur **Browse** pour rechercher et sélectionner le fichier CSV à importer.
- Etape 4** Cliquez sur **Import Assets** pour commencer le processus d'importation.

Exportation des actifs Pour exporter des actifs au format XML ou CSV :

- Etape 1** Cliquez sur l'onglet **Assets**.
- Etape 2** Dans le menu de navigation, cliquez sur **Asset Profiles**.
- Etape 3** Recherchez des profils d'actif.

Pour plus d'informations sur les profils d'actif de recherche, voir [Affichage des profils d'actif](#).

Etape 4 A partir de la zone de liste **Actions**, sélectionnez l'une des options suivantes :

- Export to XML
- Export to CSV

REMARQUE

Si vous souhaitez poursuivre la navigation dans QRadar Network Anomaly Detection, vous pouvez cliquer sur le lien **Notify When Done**.

Etape 5 Choisissez une des options suivantes :

- **Open** - Sélectionnez cette option pour ouvrir les résultats de l'exportation dans le navigateur de votre choix.
- **Save** - Sélectionnez cette option pour enregistrer les résultats sur votre bureau.

Etape 6 Cliquez sur **OK**.

Utilisation de la fonction de recherche

La fonction de recherche vous permet de rechercher des profils d'hôte, des actifs et des informations d'identité. Les informations d'identité fournissent des détails supplémentaires sur les sources de journal de votre réseau, y compris les informations DNS, les connexions utilisateur et les adresses MAC.

Cette section comprend les rubriques suivantes :

- [Recherche de profils d'actif](#)
- [Recherche d'actifs par attribut de vulnérabilité](#)

Recherche de profils d'actif

Pour rechercher des profils d'actif :

Etape 1 Cliquez sur l'onglet **Assets**.

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

REMARQUE

Si vous souhaitez rechercher tous les profils d'actif de votre déploiement, cliquez sur **Show All**.

La barre d'outils de l'onglet **Assets** fournit les options suivantes :

Tableau 9-9 Barre d'outils de l'onglet Assets

Options	Description
Add Asset	Cliquez sur Add Asset pour ajouter un profil d'actif. Voir Ajout d'un profil d'actif .
Actions	Cliquez sur Actions pour importer des actifs. Voir Importation de profils d'actif .

Remarque : Le menu Actions est uniquement disponible si vous disposez des privilèges d'administrateur. Pour plus d'informations, voir *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Etape 3 Définissez vos critères de recherche dans le panneau Assets Properties :**Tableau 9-10** Propriétés d'actif

Paramètre	Description
IP	Entrez l'adresse IP ou la plage CIDR des actifs que vous souhaitez rechercher.
MAC	Entrez l'adresse MAC de l'actif que vous souhaitez rechercher.
Host Name	Entrez le nom d'hôte de l'actif que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Machine Name	Entrez le nom de la machine de l'actif que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Username	Entrez l'utilisateur des actifs que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
User Group	Entrez le groupe d'utilisateurs des actifs que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Extra Data	Entrez le texte que vous souhaitez rechercher. Le contenu de cette zone représente du texte défini par l'utilisateur et dépend des périphériques de votre réseau qui sont disponibles pour fournir des données d'identité. On peut citer : l'emplacement physique des périphériques, les politiques pertinentes ou les noms des ports et commutateurs réseau.
Asset Name	Entrez le nom des actifs que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Description	Entrez la description des actifs que vous souhaitez rechercher.
Port	Entrez les ports (TCP ou UDP) ou plages de ports des actifs que vous souhaitez rechercher. Vous pouvez entrer plusieurs ports, séparés par des virgules. Par exemple, 80, 8080 ou 6000 à 7000.
Risk Level	A partir de la zone de liste, sélectionnez l'opérateur inférieur, égal ou supérieur au niveau de risque défini. Entrez ensuite le niveau de risque des actifs que vous souhaitez rechercher. La plage est comprise entre 0 et 10.
Network	A partir de la zone de liste, sélectionnez le réseau des actifs que vous souhaitez rechercher.
Asset Weight	Entrez la pondération des actifs que vous souhaitez rechercher. A partir de la zone de liste, sélectionnez si vous souhaitez rechercher une pondération inférieure, égale ou supérieure à la pondération de l'actif défini. Entrez ensuite la pondération d'actifs que vous souhaitez rechercher. L'intervalle est de 0 à 10. La pondération des actifs permet à QRadar Network Anomaly Detection de définir de façon appropriée des priorités pour les infractions par rapport aux actifs de valeur élevée.

Tableau 9-10 Propriétés d'actif (suite)

Paramètre	Description
Show only hosts with vulnerabilities	Sélectionnez cette case à cocher si vous souhaitez afficher uniquement les actifs avec des vulnérabilités dans les résultats de la recherche.
Operating System	Entrez le système d'exploitation des actifs que vous souhaitez rechercher. Par exemple, Red Hat Linux®.

Tableau 9-10 Propriétés d'actif (suite)

Paramètre	Description
Service Vendor	Entrez le fournisseur de services des actifs que vous souhaitez rechercher. Par exemple, RedHat inc.
Service Version	Entrez la version de service des actifs que vous souhaitez rechercher. Par exemple, 7.1.

REMARQUE

L'icône **Search** est disponible sous chaque panneau de la page Asset Profile Search. Lorsque vous avez défini vos critères de recherche et que vous n'avez plus besoin de critères de recherche supplémentaires à partir des panneaux restants, vous pouvez cliquer sur l'icône **Search**.

Etape 4 Définissez vos critères de recherche dans le panneau Extended Assets Properties :

Tableau 9-11 Propriétés étendues des actifs

Paramètre	Description
Business Owner	Entrez le propriétaire fonctionnel des actifs que vous souhaitez rechercher. Un directeur de rayon est un exemple de propriétaire fonctionnel.
Business Owner Contact Info	Entrez les informations de contact du propriétaire fonctionnel des actifs que vous souhaitez rechercher.
Technical Owner	Entrez le propriétaire technique des actifs que vous souhaitez rechercher. Un responsable informatique ou un directeur sont des exemples de propriétaire technique.
Technical Owner Contact Info	Entrez les informations de contact du propriétaire technique des actifs que vous souhaitez rechercher.
Location	Entrez l'emplacement physique des actifs que vous souhaitez rechercher.

REMARQUE

L'icône **Search** est disponible sous chaque panneau de la page Asset Profile Search. Lorsque vous avez défini vos critères de recherche et que vous n'avez plus besoin de critères de recherche supplémentaires à partir des panneaux restants, vous pouvez cliquer sur l'icône **Search** de ce panneau.

Les résultats de la recherche sont affichés. Vous pouvez maintenant rechercher et sélectionner l'actif que vous souhaitez afficher. Voir [Affichage des profils d'actif](#).

Recherche d'actifs par attribut de vulnérabilité

Les scanners tiers (QualysGuard et nCircle ip360, par exemple) signalent les vulnérabilités à QRadar Network Anomaly Detection à l'aide de références externes provenant de OSVBD (Open Source Vulnerability Database) et de NVBD (National Vulnerability Database) afin d'identifier les vulnérabilités. Un identificateur de référence unique est attribué à chaque vulnérabilité (OSVDB ID). De plus, chaque vulnérabilité peut être identifiée par des références de données

externes, telles qu'un ID Common Vulnerability and Exposures (CVE) ou un ID Bugtraq.

À l'aide de la fonction de recherche d'actif, vous pouvez rechercher des actifs par références de données externes afin de déterminer si des vulnérabilités connues existent dans votre déploiement.

Par exemple :

Vous recevez une notification indiquant que l'ID CVE : CVE-2010-000 est exploité activement dans la zone. Pour vérifier si des hôtes de votre déploiement sont vulnérables à cette exploitation, vous pouvez entrer CVE-2010-000 dans le paramètre de recherche **CVE ID** afin d'afficher une liste de tous les hôtes qui sont vulnérables à cet ID CVE spécifique.

REMARQUE

Pour plus d'informations sur l'OSVDB, voir www.osvdb.org. Pour plus d'informations sur NVDB, voir <http://nvd.nist.gov/>.

Pour rechercher des actifs par attribut de vulnérabilité :

Etape 1 Cliquez sur l'onglet **Assets**.

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

Etape 3 Définissez vos critères de recherche dans le panneau Vulnerability Attributes :

REMARQUE

Chaque zone de paramètre de recherche respecte la casse et prend en charge les caractères spéciaux pour faciliter votre recherche. La longueur maximale de chaque chaîne de recherche est de 255 caractères.

Tableau 9-12 Attributs de vulnérabilité

Paramètre	Description
OSVDB ID	Entrez l'identifiant de vulnérabilité, tel que défini sur l'OSVDB, des actifs que vous souhaitez rechercher. Vous pouvez entrer plusieurs ID OSVDB, séparés par des virgules.
Bugtraq ID	Entrez l'ID Bugtraq que vous souhaitez rechercher. Par exemple, 1234.
CERT	Entrez le numéro de recommandation du CERT (Computer Emergency Response Team) que vous souhaitez rechercher. Par exemple, CA-2001-01.
CERT VU	Entrez le numéro de note de vulnérabilité (VU) CERT que vous souhaitez rechercher. Par exemple, 619982.
CIAC Advisory	Entrez le numéro de recommandation CIAC (Computer Incident Advisory Capability) que vous souhaitez rechercher. Par exemple, O-084.
CVE ID	Entrez l'ID CVE que vous souhaitez rechercher. Par exemple, 2004-0001.

Tableau 9-12 Attributs de vulnérabilité (suite)

Paramètre	Description
Exploit Database	Entrez l'ID de base de données d'exploitation que vous souhaitez rechercher.
FrSIRT Advisory	Entrez l'ID de la recommandation FrSIRT (French Security Incident Response Team) que vous souhaitez rechercher.
Generic Exploit URL	Entrez l'URL d'exploitation générique que vous souhaitez rechercher. Remarque : Généralement, les URL d'exploitation générique dirigent vers un script/code d'exploitation ou fichier texte détaillé expliquant comment exploiter une vulnérabilité particulière.
Generic Informational URL	Entrez l'URL d'informations génériques que vous souhaitez rechercher. Remarque : L'adresse URL d'information générique dirige vers des informations sur un type ou une classe de vulnérabilité. Par exemple, cet attribut peut contenir un lien vers un livre blanc sur les attaques DDoS.
IBM APPSCAN	Entrez l'identificateur IBM AppScan que vous souhaitez rechercher. Par exemple, security-check-applicationtestscriptdetected.
ISS X-Force ID	Entrez l'ID Internet Security System (ISS) X-Force que vous souhaitez rechercher. Par exemple, 1234.
Keyword	Entrez le mot-clé que vous souhaitez rechercher dans toutes les zones dans l'OSVDB.
Mail List Post	Entrez l'URL de l'ID de publication de la liste d'adresses que vous souhaitez rechercher.
Metasploit ID	Entrez l'ID Metasploit que vous souhaitez rechercher.
Microsoft Knowledge Base Article	Entrez l'ID de l'article de la base de données Microsoft® que vous souhaitez rechercher. Par exemple, KB958644.
Microsoft Security Bulletin	Entrez l'ID de sécurité Microsoft que vous souhaitez rechercher. Par exemple, MS04-004.
Milw0rm	Entrez l'ID Milw0rm que vous souhaitez rechercher. Par exemple, 6824.
Nessus Script ID	Entrez l'URL de l'ID du script Nessus que vous souhaitez rechercher. Par exemple, 10123.
News Article	Tapez l'URL de l'ID de l'article d'actualité que vous souhaitez rechercher. Remarque : L'ID d'article d'actualité fait référence à des articles d'actualité sur des vulnérabilités spécifiques.
Niko Item ID	Entrez l'ID de l'élément Niko que vous souhaitez rechercher.
OVAL ID	Entrez l'ID OVAL (Open Vulnerability and Assessment Language) que vous souhaitez rechercher. Par exemple, 5863.

Tableau 9-12 Attributs de vulnérabilité (suite)

Paramètre	Description
Other Advisory URL	Entrez d'autres URL de recommandation que vous souhaitez rechercher.
Other Solution URL	Entrez d'autres URL de solution que vous souhaitez rechercher.
Packet Storm	Entrez la référence Packet Storm que vous souhaitez rechercher.
RedHat RHSA	Entrez l'ID RHSA (RedHat Security Alert) que vous souhaitez rechercher. Par exemple, RHSA-2004:065-05.
Related OSVDB ID	Entrez l'ID OSVDB lié que vous souhaitez rechercher. Les ID sont reliés par des références croisées dans l'OSVDB. En règle générale, les ID OSVDB sont reliés par des références croisées, si la source de l'information est la même.
SCIP VulDB ID	Entrez l'ID VulDB (Vulnerability Database) du SCIP (Secure Communications Interoperability Protocol) que vous souhaitez rechercher.
Secunia Advisory ID	Entrez l'ID de recommandation Secunia que vous souhaitez rechercher. Par exemple : 10123.
Security Tracker	Entrez l'ID Security Tracker que vous souhaitez rechercher. Par exemple, 1009695.
Snort Signature ID	Entrez l'ID Signature Snort que vous souhaitez rechercher. Par exemple, 1324.
Tenable PVS	Entrez l'ID Tenable Passive Vulnerability Scanner (PVS) que vous souhaitez rechercher.
US-CERT Cyber Security Alert	Entrez l'ID de l'alerte de cybersécurité US-CERT que vous souhaitez rechercher. Par exemple, TA06-333A.
VUPEN Advisory	Entrez l'ID de sécurité VUPEN que vous souhaitez rechercher.
Vender Specific Advisory URL	Entrez l'URL de la recommandation spécifique du fournisseur que vous souhaitez rechercher.
Vendor Specific News/Changelog Entry	Entrez l'URL de l'entrée du journal des changements/nouveautés spécifiques du fournisseur que vous souhaitez rechercher.
Vendor Specific Solution URL	Entrez l'URL de la solution spécifique du fournisseur que vous souhaitez rechercher.
Vendor URL	Entrez l'URL du fournisseur que vous souhaitez rechercher.

Etape 4 Cliquez sur **Search**.

Les résultats de la recherche sont affichés. Vous pouvez maintenant rechercher et sélectionner l'actif que vous souhaitez afficher. Voir [Affichage des profils d'actif](#).

10

GESTION DES RAPPORTS

Vous pouvez utiliser l'onglet **Reports** afin de créer, éditer, distribuer et gérer les rapports.

Cette section comprend les rubriques suivantes :

- [Présentation de l'onglet Rapport](#)
- [Utilisation de l'onglet Rapport](#)
- [Création de rapports personnalisés](#)
- [Personnalisation des rapports par défaut](#)
- [Groupement des rapports](#)
- [Générer manuellement un rapport](#)
- [Affichage Generated Reports](#)
- [Dupliquer un rapport](#)
- [Partage d'un rapport](#)
- [Marquer des rapports](#)

Présentation de l'onglet Rapport

L'onglet **Reports** vous fournit :

- Des options de rapports détaillées nécessaires pour satisfaire les diverses normes de réglementation, telles que la conformité PCI.
- La flexibilité dans la présentation et le contenu.

Vous pouvez créer votre propre rapport personnalisé IBM Security QRadar QFlow Collector ou utiliser l'un des rapports par défaut. Vous pouvez personnaliser et renommer chacun des rapports par défaut et les distribuer à d'autres utilisateurs Détection des anomalies QRadar. Les administrateurs peuvent afficher tous les rapports créés par d'autres utilisateurs Détection des anomalies QRadar. Les utilisateurs non administrateurs peuvent uniquement visualiser les rapports qu'ils ont créés ou les rapports qui sont partagés par d'autres utilisateurs.

**ATTENTION**

Si vous utilisez Microsoft® Exchange Server 5.5, les caractères de police non disponibles peuvent être affichés dans la ligne d'objet des rapports envoyés par e-mail. Pour résoudre ce problème, téléchargez et installez le Service Pack 4 de Microsoft Exchange Server 5.5. Pour plus d'informations, contactez Support technique Microsoft.

Pour vous assurer que la fonction Reports utilise la date et l'heure correctes de présentation des données, votre session Détection des anomalies QRadar doit être synchronisée avec votre fuseau horaire. Lors de l'installation et de la configuration de Détection des anomalies QRadar, le fuseau horaire est configuré. Vérifiez auprès de votre administrateur pour s'assurer que votre session Détection des anomalies QRadar est synchronisée avec votre fuseau horaire.

Utilisation de l'onglet Rapport

L'onglet **Reports** affiche une liste de rapports personnalisés par défaut. A partir de l'onglet **Reports**, vous pouvez visualiser des informations statistiques sur le modèle rapports, effectuer des actions sur les modèles de rapport, afficher les rapports générés et supprimer le contenu généré.

Cette section comprend les rubriques suivantes :

- [Affichage des rapports](#)
- [Utilisation de la barre d'outils](#)
- [Affichage des rapports générés](#)
- [Suppression du contenu généré](#)
- [Utilisation de la barre d'état](#)

Affichage des rapports

Dans l'onglet **Reports**, vous pouvez afficher la liste des rapports et des données statistiques pour chaque rapport, tels que la fréquence à laquelle le rapport est généré et la prochaine génération prévue du rapport.

Pour afficher la liste des rapports :

Etape 1 Cliquez sur l'onglet **Reports**.

L'onglet **Reports** fournit les informations suivantes :

Tableau 10-1 Paramètres de l'onglet Reports

Paramètres	Description
Flag Column	Si une erreur se produit, provoquant l'échec de la génération du rapport, l'icône Error s'affiche dans cette colonne.
Report Name	Indique le nom du rapport.
Group	Indique le groupe auquel appartient ce rapport.

Tableau 10-1 Paramètres de l'onglet Reports (suite)

Paramètres	Description
Schedule	Indique la fréquence à laquelle le rapport est généré. Les rapports qui indiquent une planification par intervalle, lorsqu'elle est activée, sont automatiquement générés conformément à l'intervalle spécifié. Si un rapport n'indique pas une planification par intervalle, vous devez générer manuellement le rapport. Voir Générer manuellement un rapport .
Next Run Time	Indique la durée, en heures et en minutes, jusqu'à la génération du prochain rapport.
Last Modification	Indique la date de la dernière modification de ce rapport.
Owner	Indique l'utilisateur Détection des anomalies QRadar qui possède le rapport.
Author	Indique l'utilisateur Détection des anomalies QRadar qui a créé le rapport.
Generated Reports	A partir de cette zone de liste, sélectionnez la date d'émission du rapport généré que vous souhaitez afficher. Lorsque vous sélectionnez la date d'émission, le paramètre Format affiche les formats disponibles pour les rapports générés. Voir Affichage des rapports générés . Si aucun rapport n'est généré, None s'affiche.
Formats	Indique les formats de rapport du rapport sélectionné actuellement dans la colonne Generated Reports . Cliquez sur l'icône du format que vous souhaitez afficher. Les formats de rapport incluent : <ul style="list-style-type: none"> • PDF - Portable Document Format • HTML - Format Hyper Text Markup Language • RTF - Rich Text Format • XML - Extensible Markup Language (only available for tables) • XLS - Format Microsoft Excel (uniquement disponible pour les tableaux)

Etape 2 Déplacez votre souris sur un rapport pour prévisualiser un rapport résumé dans une infobulle.

Le résumé indique la configuration du rapport et le type de contenu que génère le rapport.

REMARQUE

Par défaut, les rapports sont triés par colonne de **Last Modification**. Dans le menu de navigation Reports, les rapports sont triés par intervalle horaire. Afin de filtrer le rapport pour n'afficher que les rapports d'une fréquence spécifique, cliquez sur la flèche à côté de l'élément de menu **Report** dans le menu de navigation et sélectionnez le groupe (frequency) du dossier.

Utilisation de la barre d'outils

Vous pouvez utiliser la barre d'outils pour effectuer un certain nombre d'actions sur les rapports. Le tableau suivant identifie et décrit les options Reports de la barre d'outils.

Tableau 10-2 Options de barre d'outils et d'onglet des rapports

Option	Description
Group	A partir la zone de liste, sélectionnez le groupe que vous souhaitez afficher. le groupe est affiché avec les rapports affectés. Pour plus d'informations, voir Groupement des rapports .
Manage Groups	Cliquez sur Manage Groups afin de gérer le groupe de rapports. En utilisant la fonction Manage Groups, vous pouvez organiser vos rapports en groupes fonctionnels. Pour plus d'informations, voir Groupement des rapports .
Actions	<p>Cliquez sur Actions pour effectuez les options suivantes :</p> <ul style="list-style-type: none"> • Create - Sélectionnez cette option afin de créer un nouveau rapport. Pour plus d'informations, voir Personnalisation des rapports par défaut. • Edit - Sélectionnez cette option afin d'éditer le rapport sélectionné. Vous pouvez également cliquer deux fois sur un rapport afin d'éditer le contenu. • Duplicate - Sélectionnez cette option afin de dupliquer ou de renommer le rapport sélectionné. Pour plus d'informations, voir Dupliquer un rapport. • Assign Groups - Sélectionnez cette option afin d'affecter le rapport sélectionné à un groupe de rapport. Pour plus d'informations, voir Groupement des rapports. • Share - Sélectionnez cette option afin de partager le rapport sélectionné avec d'autres utilisateurs. Vous devez disposer de privilèges administratifs afin de partager des rapports. Pour plus d'informations, voir Partage d'un rapport. • Toggle Scheduling - Sélectionnez cette option afin de basculer du rapport sélectionné à l'état Actif ou Inactif. • Run Report - Sélectionnez cette option afin de générer le rapport sélectionné. Pour plus d'informations, voir Générer manuellement un rapport. Pour générer plusieurs rapports, maintenez la touche de contrôle enfoncée et cliquez sur le rapport que vous souhaitez générer. • Delete Report - Sélectionnez cette option afin de supprimer le rapport sélectionné. Pour supprimer plusieurs rapports, maintenez la touche de contrôle enfoncée et cliquez sur les rapports que vous souhaitez supprimer. • Delete Generated Content - Sélectionnez cette option afin de supprimer tous les contenus générés pour les lignes sélectionnées. Pour supprimer plusieurs rapports générés, maintenez la touche de contrôle enfoncée et cliquez sur les rapports générés que vous souhaitez supprimer.

Tableau 10-2 Options de barre d'outils et d'onglet des rapports (suite)

Option	Description
Hide Inactive Reports	Sélectionnez cette case afin de masquer les modèles de rapport inactifs. L'onglet Reports s'actualise automatiquement et affiche uniquement les rapports actifs. Décochez la case afin d'afficher les rapports inactifs masqués.
Search Reports	Entrez vos critères de recherche dans la zone Search Reports puis cliquez sur l'icône Search Reports . Une recherche est effectuée en fonction des paramètres suivants pour déterminer lequel correspond à vos critères spécifiés : <ul style="list-style-type: none"> • Report Title • Report Description • Report Groups • Report Author User Name

Affichage des rapports générés

Vous pouvez afficher les rapports générés figurant sur l'onglet **Reports**. ces rapports ont été précédemment générés, et peuvent déjà être distribués pour d'autres Détection des anomalies QRadar utilisateurs. Vous pouvez uniquement afficher les rapports auxquels vous avez eu accès de l'administrateur Détection des anomalies QRadar. Les administrateurs peuvent accéder à tous les rapports. Les rapports peuvent être présentés dans l'un des formats suivants :

- **PDF** - Portable Document Format
- **HTML** - Format Hyper Text Markup Language
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (only available for tables)
- **XLS** - Format Microsoft Excel

Les formats XML et XLS sont uniquement disponibles pour les rapports qui utilisent un format tableau de graphique unique (portrait ou paysage).

REMARQUE

Si vous utilisez Mozilla Firefox comme navigateur et que vous sélectionnez le format de rapport RTF, FireFox lance une nouvelle fenêtre de navigateur. Le lancement de cette nouvelle fenêtre est le résultat de la configuration du navigateur FireFox et n'affecte pas Détection des anomalies QRadar. Vous pouvez fermer la fenêtre et continuer votre session Détection des anomalies QRadar.

Pour afficher un rapport généré :

- Etape 1** Cliquez sur l'onglet **Reports**.

REMARQUE

L'onglet **Reports** peut exiger une longue période de temps pour s'actualiser si votre système comporte un grand nombre de rapports.

Etape 2 Dans la zone de liste de la colonne **Generated Reports**, sélectionnez l'horodatage de rapport que vous souhaitez afficher.

Lorsqu'un rapport a généré le contenu, la colonne **Generated Reports** affiche une zone de liste. La zone de liste affiche tout le contenu généré, organisé par l'horodatage du rapport. Les rapports les plus récents sont affichés en haut de la liste. Si un rapport ne génère pas de contenu, la valeur **None** est affichée dans la colonne **Generated Reports**.

Les icônes représentant le format du rapport généré sont affichées dans la colonne **Formats**.

Etape 3 Cliquez sur l'icône du format que vous souhaitez afficher.

Le rapport s'affiche dans le format sélectionné.

Suppression du contenu généré Lorsque vous supprimez le contenu généré, tous les rapports qui ont été générés à partir du modèle de rapport sont supprimés, mais le rapport modèle est conservé.

Pour supprimer un contenu généré d'un rapport :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez les rapports dont vous souhaitez supprimer le contenu généré

Etape 3 A partir de la zone de liste **Actions**, cliquez sur **Delete Generated Content**.

Tout le contenu généré pour le rapport sélectionné est supprimé.

Utilisation de la barre d'état La barre d'état affiche le nombre de résultats de la recherche (**Displaying 1 of 10 items**) qui s'affiche actuellement et le volume de temps (**Elapsed time:**) nécessaire pour traiter les résultats de la recherche.

Création de rapports personnalisés

Dans l'onglet **Reports** vous pouvez accéder au Report Wizard pour créer un nouveau rapport. Le Report Wizard fournit un guide étape par étape sur la conception, la planification et la génération des rapports. L'assistant utilise les éléments clés suivants pour vous aider à créer un rapport :

- **Layout** - La position et la taille de chaque conteneur
- **Container** - Marque de réservation pour le contenu présenté
- **Content** - Définition du graphique placé dans le conteneur

Cette section comprend les rubriques suivantes :

- [Création d'un rapport](#)
- [Configuration des graphiques](#)
- [Sélection d'un type de graphique](#)

Création d'un rapport

Pour créer un rapport :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Dans la zone de liste **Actions**, sélectionnez **Create**.

Etape 3 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 4 Sélectionnez une des options de planification suivantes.

- **Manually** - Génère un rapport une fois. Il s'agit du réglage par défaut, mais vous pouvez générer ce rapport aussi souvent que nécessaire.
- **Hourly** - Planifie le rapport pour générer, à la fin de chaque heure en utilisant les données de la précédente heure.

Si vous sélectionnez l'option **Hourly**, une configuration supplémentaire est requise. Dans les zones de liste, sélectionnez un cadre temporel de début et de fin du cycle de génération. Un rapport est généré pour chaque heure dans ce cadre temporel. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00 pour les deux zones **From** et **To**.

- **Daily** - Planifie le rapport pour générer quotidiennement en utilisant les données de la journée précédente. Pour chaque graphique sur un rapport, vous pouvez sélectionner les 24 dernières heures de la journée, ou sélectionner un cadre temporel précis de la journée précédente.

Si vous sélectionnez l'option **Daily**, une configuration supplémentaire est nécessaire. Cochez la case à côté de chaque jour où vous souhaitez générer un rapport. En outre, vous pouvez utiliser la zone de liste pour sélectionner une heure de début du cycle de génération de rapports. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.

- **Weekly** - Planifie le rapport pour générer hebdomadairement en utilisant les données de la semaine précédente.

si vous sélectionnez l'option **Weekly**, une configuration supplémentaire est nécessaire. Sélectionnez le jour où vous souhaitez générer le rapport. La valeur configurée par défaut est le lundi. Dans la zone de liste, sélectionnez l'heure de début du cycle de génération de rapports. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.

- **Monthly** - Planifie le rapport pour générer mensuellement en utilisant les données du mois précédent.

Si vous sélectionnez l'option **Monthly**, une configuration supplémentaire est nécessaire. A partir de la zone de liste, sélectionnez la date où vous souhaitez générer le rapport. La valeur configurée par défaut est le premier jour du mois. Vous pouvez également utiliser la zone de liste pour sélectionner un temps de commencement pour le cycle de génération de rapports. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.

REMARQUE

Après avoir créé un rapport qui génère hebdomadairement ou mensuellement, la date prévue doit être écoulée avant que le rapport généré renvoie des résultats. Pour un rapport planifié, vous devez attendre l'heure planifiée pour la construction

des résultats. Par exemple, une recherche hebdomadaire nécessite 7 jours pour construire les données. Cette recherche ne renvoie pas de résultats avant l'écoulement de 7 jours.

Etape 5 Pour autoriser ce rapport à générer un panneau manuel, sélectionnez l'une des options suivantes :

- **Yes** - Active la génération manuelle de ce rapport.
- **No** - Désactive la génération manuelle de ce rapport.

Etape 6 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Un rapport peut être constitué de plusieurs éléments de données et peut représenter un réseau et des données de sécurité dans une variété de styles, tels que des tableaux, des graphiques linéaires, des graphiques circulaires et des histogrammes.

Lorsque vous sélectionnez l'agencement d'un rapport, considérez le type de rapport que vous souhaitez créer. Par exemple, ne choisissez pas un petit conteneur de tableau pour un contenu graphique qui affiche un grand nombre d'objets. Chaque graphique comprend une légende et une liste de réseaux dont le contenu est dérivé, choisissez un conteneur assez grand pour contenir les données. Pour prévisualiser comment chaque graphique affiche un ensemble de données, voir [Sélection d'un type de graphique](#).

Etape 7 Configurez la présentation de votre rapport :

- a Dans la zone de liste **Orientation**, sélectionnez la page d'orientation: portrait ou paysage. La valeur configurée par défaut est paysage.
- b Sélectionnez une des six options d'agencement affichées dans le Report Wizard.
- c Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 8 Indiquez des valeurs pour les paramètres suivants :

- **Report Title** - Entrez un titre de rapport. Le titre peut comporter jusqu'à 100 caractères de longueur. N'utilisez pas des caractères spéciaux.
- **Logo** - Dans la zone de liste, sélectionnez un logo. Le logo Détection des anomalies QRadar est le logo configuré par défaut. Pour plus d'informations sur l'image de marque de votre rapport, voir [Marquer des rapports](#).

Etape 9 Pour configurer chaque conteneur dans le rapport :

- a Dans la zone de liste **Chart Type** sélectionnez un type de graphique. Les options incluent :

- **None**

Lorsque vous sélectionnez l'option **None**, le conteneur s'affiche vide dans le rapport. Cette option peut être utile pour créer un espace blanc dans votre rapport. Si vous sélectionnez l'option None pour tout conteneur, aucune configuration supplémentaire n'est nécessaire pour ce conteneur.

- **Asset Vulnerabilities**

- **Event/Logs**

- **Flows**
- **Top Destination IPs**
- **Top Offenses**
- **Top Source IPs**

Après avoir sélectionné un type de graphique, la page suivante de l'Assistant s'ouvre ce qui vous permet de configurer le contenu pour ce conteneur particulier.

- b** Configurez le graphique.
Pour obtenir des informations détaillées sur la configuration de votre graphique, voir [Configuration des graphiques](#).
- c** Cliquez sur **Save Container Details**.
L'assistant revient à la page précédente, vous permettant d'indiquer plus de contenus pour votre rapport.
- d** Si nécessaire, répétez les étapes **a** à **c** pour tous les conteneurs.
- e** Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Les graphiques affichés sur la page d'aperçu n'affichent pas les données réelles. Il ne s'agit que d'une représentation graphique de l'agencement que vous avez configuré.

Etape 10 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 11 Cochez les cases pour les formats de rapport. Vous pouvez sélectionner plus d'une option. Les options sont :

- Portable Document Format (PDF) - Il s'agit du format de rapport configuré par défaut.
- Hypertext Markup Language (HTML)
- Rich Text Format (RTF)
- Extended Markup Language (XML)
- Excel Spreadsheet (XLS)

REMARQUE

La taille de fichier des rapports générés peut être un ou deux mégaoctets, en fonction du format de sortie sélectionné. Nous recommandons l'utilisation du format PDF, le format PDF est de plus petite taille et ne consomme pas une grande quantité d'espace de stockage sur disque.

Etape 12 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 13 Sélectionnez les canaux de distribution que vous souhaitez pour votre rapport.

Tableau 10-3 Options de distribution des rapports générés

Options	Description
Report Console	Cochez cette case pour envoyer le rapport généré à l'onglet Reports . Il s'agit du canal de distribution par défaut.
Sélectionnez les utilisateurs qui devraient être en mesure d'afficher le rapport généré.	<p>Cette option s'affiche uniquement une fois que vous avez coché la case Report Console.</p> <p>Dans la liste des utilisateurs, sélectionnez les utilisateurs Détection des anomalies QRadar auxquels vous souhaitez accorder le droit d'afficher les rapports générés.</p> <p>Remarque : Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs. Pour plus d'informations à propos des autorisations, voir le IBM Security QRadar Network Anomaly Detection Guide d'administration.</p>
Select all users	<p>Cette option s'affiche uniquement une fois que vous avez coché la case Report Console.</p> <p>Cochez cette case si vous voulez accorder le droit à tous les utilisateurs Détection des anomalies QRadar d'afficher les rapports générés.</p> <p>Remarque : Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs. Pour plus d'informations à propos des autorisations, voir le IBM Security QRadar Network Anomaly Detection Guide d'administration.</p>
Email	Cochez cette case si vous voulez distribuer les rapports générés par e-mail.
Entrez le(s) adresse(s) e-mail de distribution de rapport	<p>Cette option s'affiche uniquement une fois que vous avez coché la case Email.</p> <p>Entrez l'adresse e-mail de chaque destinataire des rapports générés; séparez la liste des adresses e-mail avec des virgules. Le nombre maximum de caractères pour ce paramètre est 255.</p> <p>Remarque : Les destinataires reçoivent cet e-mail de <code>no_reply_reports@qradar</code>.</p>
Include Report as attachment (non-HTML only)	<p>Cette option s'affiche uniquement une fois que vous avez coché la case Email.</p> <p>Cochez cette case pour envoyer le rapport généré en tant que pièce jointe.</p>
Include link to Report Console	<p>Cette option s'affiche uniquement une fois que vous avez coché la case Email.</p> <p>Cochez cette case pour inclure un lien vers Report Console dans l'e-mail.</p>

Etape 14 Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 15 Entrez les valeurs pour les paramètres suivants :

Tableau 10-4 Paramètres de finalisation

Paramètre	Description
Report Description	Entrez une description pour ce rapport. La description est affichée dans la page Report Summary et dans l'e-mail de distribution des rapports générés.
Groups	Sélectionnez les groupes auxquels vous voulez affecter ce rapport. Pour plus d'informations à propos des groupes, voir Groupement des rapports .
Voulez-vous exécuter le rapport maintenant ?	Cochez cette case si vous souhaitez générer le rapport lorsque l'assistant est terminé. Par défaut, la case est cochée.

Etape 16 Cliquez sur **Next** afin d'afficher le rapport récapitulatif.

La page Report Summary fournit les détails du rapport. vous pouvez sélectionner les onglets disponibles sur le rapport récapitulatif afin de prévisualiser les sélections du rapport.

Etape 17 Cliquez sur **Finish**.

Le rapport est immédiatement généré. Si vous décochez la case **Would you like to run the report now?** sur la dernière page de l'assistant, le rapport est enregistré et généré comme planifié.

Le titre du rapport est le titre par défaut pour le rapport généré. Si vous reconfigurez un rapport afin d'entrer un nouveau titre de rapport, le rapport est enregistré comme nouveau rapport avec le nouveau nom, mais l'original rapport reste le même.

Configuration des graphiques

Le type de graphique détermine la façon dont le rapport généré présente des données et des objets de réseau. Vous pouvez tracer des données avec plusieurs caractéristiques et créer les graphiques dans un seul rapport généré.

Les types de graphiques suivants sont disponibles pour chaque rapport :

- [Asset Vulnerabilities](#)
- [Event/Logs](#)
- [Event/Logs](#)
- [Flows](#)
- [Top Destination IPs](#)
- [Top Offenses](#)
- [Top Source IPs](#)

Asset Vulnerabilities

vous pouvez utiliser le graphique des vulnérabilités de l'actif pour afficher les données de vulnérabilité pour chaque actif défini dans votre déploiement. Vous pouvez générer des graphiques de vulnérabilité de l'actif lorsque les vulnérabilités ont été détectées par une analyse VA. Pour plus d'informations, voir le *IBM Security QRadar Guide de configuration de l'évaluation de la vulnérabilité*

- Pour configurer les détails de conteneur du graphique des vulnérabilités de l'actif, entrez les valeurs pour les paramètres suivants :

Tableau 10-5 Détails du conteneur du graphique des vulnérabilités des actifs

Paramètre	Description
Container Details - Assets	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Assets to Top	Dans la zone de liste, sélectionnez le nombre des actifs que vous souhaitez inclure dans ce rapport.
Graph Type	<p>Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent :</p> <ul style="list-style-type: none"> • Aggregate Table - Affiche les données dans une table d'agrégation qui correspond à une table contenant des sous-tables (sous-rapports). Lorsque vous sélectionnez cette option, vous devez configurer les détails du sous-rapport. L'option Table est uniquement disponible pour le conteneur de largeur pleine page. • Bar - Affiche les données dans un graphique à barres. Lorsque vous sélectionnez cette option, le rapport ne comprend pas les données des sous-rapports. Il s'agit de la configuration par défaut. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée. • Pie - Affiche les données dans un graphique circulaire. Lorsque vous sélectionnez cette option, le rapport ne comprend pas les données du sous-rapport. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée.

Pour afficher des exemples de chaque type de données des graphiques, voir [Sélection d'un type de graphique](#).

Tableau 10-5 Détails du conteneur du graphique des vulnérabilités des actifs (suite)

Paramètre	Description
Order Assets By	<p>Sélectionnez le type de données en fonction duquel vous souhaitez trier le graphique. Les options incluent :</p> <ul style="list-style-type: none"> • Asset Weight - Trie les données en fonction de la pondération d'actif définie dans le profil d'actif. • CVSS Risk - Trie les données par le niveau de risque du Common Vulnerability Scoring System (CVSS). Pour plus d'informations sur CVSS, voir http://www.first.org/cvss/. • Vulnerability Count - Trie les données en fonction du nombre de vulnérabilités des actifs.
Sub-Report Details	
Sub-report	Indique le type d'information affichée dans le sous-rapport.
Order Sub-report By	<p>Sélectionnez le paramètre en fonction duquel vous souhaitez organiser le sous-rapport. Les options incluent :</p> <ul style="list-style-type: none"> • Risk (Base Score) • OSVDB ID • OSVDB Title • Last Modified Date • Disclosure Date • Discovery Date <p>Pour plus d'informations sur la base de données Open Source Vulnerability (OSVDB), voir www.osvdb.org.</p>
Limit Sub-report to Top	Dans la zone de liste, sélectionnez le nombre de vulnérabilités que vous souhaitez inclure dans ce sous-rapport.
Graph Content	
Vulnerabilities	<p>Pour indiquer les vulnérabilités que vous souhaitez signaler :</p> <ol style="list-style-type: none"> 1 Cliquez sur Browse. 2 Dans la zone de liste Search by, sélectionnez l'attribut de vulnérabilité selon lequel vous souhaitez effectuer une recherche. Les options incluent CVE ID, Bugtraq ID, OSVDB ID et OSVDB Title. Pour plus d'informations sur les attributs de vulnérabilité, voir Gestion des actifs - Recherche des actifs par attribut de vulnérabilité. 3 Dans la liste Search Results, sélectionnez les vulnérabilités que vous souhaitez signaler. Cliquez sur Add. 4 Cliquez sur Submit.
IP Address	Tapez l'adresse IP, le CIDR ou une liste des adresses IP séparées par des virgules que vous souhaitez signaler Les CIDR partiels sont autorisés.

Tableau 10-5 Détails du conteneur du graphique des vulnérabilités des actifs (suite)

Paramètre	Description
Networks	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels recueillir des données graphiques.

Event/Logs

Vous pouvez utiliser le graphique Event/Logs afin d'afficher des informations sur l'événement. Vous pouvez baser vos graphiques sur des données provenant des recherches enregistrées à partir de l'onglet **Log Activity**. Ceci vous permet de personnaliser les données que vous souhaitez afficher dans le rapport généré. Vous pouvez configurer le graphique pour tracer des données sur une période de temps configurable. Cette fonctionnalité vous aide à détecter les tendances de l'événement.

Pour plus d'informations sur les recherches enregistrées, voir [Recherche de donnée](#).

- Pour configurer le graphique des détails du conteneur des événements/journaux, entrez des valeurs pour les paramètres suivants :

Tableau 10-6 Détails du conteneur du graphique des événements/journaux

Paramètre	Description
Container Details - Events/Logs	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Events/Logs to Top	Dans la zone de liste, sélectionnez le nombre des événements/journaux à afficher dans le rapport généré.

Tableau 10-6 Détails du conteneur du graphique des événements/journaux (suite)

Paramètre	Description
Graph Type	<p>Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent :</p> <ul style="list-style-type: none"> • Bar - Affiche les données dans un graphique à barres. Il s'agit du type de graphique par défaut. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée. • Line - Affiche les données dans un graphique à courbes. • Pie - Affiche les données dans un graphique circulaire. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée. • Stacked Bar - Affiche les données dans un graphique à barres empilées. • Stacked Line - Affiche les données dans un graphique à courbes empilées. • Table - Affiche les données sous la forme d'un tableau. L'option Table est uniquement disponible pour le conteneur de largeur pleine page seulement. <p>Pour afficher des exemples de chaque type de données des graphiques, voir Sélection d'un type de graphique.</p>

Tableau 10-6 Détails du conteneur du graphique des événements/journaux (suite)

Paramètre	Description
Manual Scheduling	<p>Le panneau Manual Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Manually dans le Report Wizard.</p> <p>En utilisant les options Manual Scheduling, vous pouvez créer une planification manuelle qui peut exécuter un rapport sur une période de temps personnalisée définie, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez. Par exemple, vous pouvez programmer un rapport pour qu'il soit exécuté du 1er au 31 Octobre, incluant uniquement les données générées pendant vos heures de travail, telles que du lundi au vendredi, de 8h00 à 21h00.</p> <p>Pour créer une planification manuelle :</p> <ol style="list-style-type: none"> 1 Dans la zone de liste From, entrez la date de début que vous souhaitez pour le rapport ou sélectionnez la date en utilisant l'icône Calendar. La valeur configurée par défaut est la date actuelle. 2 Dans les zones de liste, sélectionnez l'heure de début que vous souhaitez pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. 3 Dans la zone de liste To entrez la date de fin que vous souhaitez pour le rapport ou sélectionnez la date en utilisant l'icône Calendar. La valeur configurée par défaut est la date actuelle. 4 Dans les zones de liste, sélectionnez l'heure de fin que vous souhaitez pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. 5 Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p>

Tableau 10-6 Détails du conteneur du graphique des événements/journaux (suite)

Paramètre	Description
Hourly Scheduling	<p>Afin d'affiner d'avantage votre planification :</p> <ol style="list-style-type: none"> 1 Cochez la case Targeted Data Selection. Des options supplémentaires s'affichent. 2 Cochez la case Only hours from, puis en utilisant les zones de liste, sélectionnez l'intervalle que vous souhaitez pour votre rapport. Par exemple, vous pouvez sélectionner uniquement les heures de 8h00 à 17h00. 3 Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.
	<p>Le panneau Hourly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Hourly dans le Report Wizard.</p> <p>► Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport.</p> <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p>
	<p>La planification horaire place automatiquement dans des graphiques toutes les données de l'heure précédente.</p>

Tableau 10-6 Détails du contenu du graphique des événements/journaux (suite)

Paramètre	Description
Daily Scheduling	<p>Le panneau Daily Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Daily dans le Report Wizard.</p> <p>1 Sélectionnez une des options suivantes :</p> <ul style="list-style-type: none"> • All data from previous day (24 hours) • Data of previous day from - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. <p>2 Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport.</p> <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p>

Tableau 10-6 Détails du conteneur du graphique des événements/journaux (suite)

Paramètre	Description
Weekly Scheduling	<p>Le panneau Weekly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Weekly dans le Report Wizard.</p> <ol style="list-style-type: none"> Sélectionnez une des options suivantes : <ul style="list-style-type: none"> All data from previous week All Data from previous week from - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut est le dimanche. Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p> <p>Afin d'affiner d'avantage votre planification :</p> <ol style="list-style-type: none"> Cochez la case Targeted Data Selection. Des options supplémentaires s'affichent. Cochez la case Only hours from, puis en utilisant les zones de liste, sélectionnez l'intervalle que vous souhaitez pour votre rapport. Par exemple, vous pouvez sélectionner uniquement les heures de 8h00 à 17h00. Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.

Tableau 10-6 Détails du conteneur du graphique des événements/journaux (suite)

Paramètre	Description
Monthly Scheduling	<p>Le panneau Monthly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Monthly dans le Report Wizard.</p> <ol style="list-style-type: none"> Sélectionnez une des options suivantes : <ul style="list-style-type: none"> All data from previous month Data from previous month from the - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut s'étend du 1er au 31. Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. <p><i>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</i></p> <p>Afin d'affiner d'avantage votre planification :</p> <ol style="list-style-type: none"> Cochez la case Targeted Data Selection. Des options supplémentaires s'affichent. Cochez la case Only hours from, puis en utilisant les zones de liste, sélectionnez l'intervalle que vous souhaitez pour votre rapport. Par exemple, vous pouvez sélectionner uniquement les heures de 8h00 à 17h00. Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.
Graph Content	
Group	<p>Dans la zone de liste, sélectionnez un groupe recherche enregistrée pour afficher les recherches enregistrées appartenant à ce groupe dans la zone de liste Available Saved Searches.</p>

Tableau 10-6 Détails du conteneur du graphique des événements/journaux (suite)

Paramètre	Description
Type Saved Search or Select from List	Pour affiner la liste Available Saved Searches , entrez le nom de la recherche que vous souhaitez localiser dans la zone Type Saved Search or Select from List . Vous pouvez également entrer un mot-clé pour afficher la liste des recherches incluant ce mot clé. Par exemple, entrez Firewall afin d'afficher une liste de toutes les recherches qui incluent Firewall dans le nom de la recherche.

Tableau 10-6 Détails du conteneur du graphique des événements/journaux (suite)

Paramètre	Description
Available Saved Searches	Fournit une liste des recherches enregistrées disponibles. Toutes les recherches enregistrées disponibles s'affichent par défaut. Cependant, vous pouvez filtrer la liste en sélectionnant un groupe dans la zone de liste Group ou en entrant le nom d'une recherche enregistrée connue dans la zone Type Saved Search or Select from List .
Create New Event Search	Cliquez sur Create New Event Search pour créer une nouvelle recherche. Pour plus d'informations sur la création d'une recherche d'événements, voir Etudes d'événements .

Flows

Vous pouvez utiliser le graphique Flows afin d'afficher le flux d'informations. Vous pouvez baser vos graphiques sur des données provenant des recherches enregistrées à partir de l'onglet **Network Activity**. Ceci vous permet de personnaliser les données que vous souhaitez afficher dans le rapport généré. Vous pouvez utiliser les recherches enregistrées pour configurer le graphique afin de tracer un flux de données sur une période de temps configurable. Cette fonctionnalité vous aide à détecter les tendances des flux.

Pour plus d'informations sur les recherches enregistrées, voir [Recherche de données](#).

- Pour configurer les détails de conteneur de flux, entrez des valeurs pour les paramètres suivants :

Tableau 10-7 Détails de conteneur de flux

Paramètre	Description
Container Details - Flows	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Flows to Top	Dans la zone de liste, sélectionnez le nombre de flux qui doivent être affichés dans le rapport généré.

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
Graph Type	<p>Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent :</p> <ul style="list-style-type: none"> • Bar - Affiche les données dans un graphique à barres. Il s'agit du type de graphique par défaut. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée. • Line - Affiche les données dans un graphique à courbes. • Pie - Affiche les données dans un graphique circulaire. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée. • Stacked Bar - Affiche les données dans un graphique à barres empilées. • Stacked Line - Affiche les données dans un graphique à courbes empilées. • Table - Affiche les données sous la forme d'un tableau. <p>Pour afficher des exemples de chaque type de données des graphiques, voir Sélection d'un type de graphique.</p>

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
Manual Scheduling	<p>Le panneau Manual Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Manually dans le Report Wizard.</p> <p>En utilisant les options Manual Scheduling, vous pouvez créer une planification manuelle qui peut exécuter un rapport sur une période de temps personnalisée définie, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez. Par exemple, vous pouvez programmer un rapport pour qu'il soit exécuté du 1^{er} au 31 Octobre, incluant uniquement les données générées pendant vos heures de travail, telles que du lundi au vendredi, de 8 heures à 21 heures.</p> <p>Pour créer une planification manuelle :</p> <ol style="list-style-type: none"> 1 Dans la zone de liste From, entrez la date de début que vous souhaitez pour le rapport ou sélectionnez la date en utilisant l'icône Calendar. La valeur configurée par défaut est la date actuelle. 2 Dans les zones de liste, sélectionnez l'heure de début que vous souhaitez pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. 3 Dans la zone de liste To entrez la date de fin que vous souhaitez pour le rapport ou sélectionnez la date en utilisant l'icône Calendar. La valeur configurée par défaut est la date actuelle. 4 Dans les zones de liste, sélectionnez l'heure de fin que vous souhaitez pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. 5 Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p>

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
	<p>Afin d'affiner d'avantage votre planification :</p> <ol style="list-style-type: none"> 1 Cochez la case Targeted Data Selection. Des options supplémentaires s'affichent. 2 Cochez la case Only hours from, puis en utilisant les zones de liste, sélectionnez l'intervalle que vous souhaitez pour votre rapport. Par exemple, vous pouvez sélectionner uniquement les heures de 8h00 à 17h00.
Hourly Scheduling	<p>Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport. Le panneau Hourly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Hourly dans le Report Wizard.</p> <ul style="list-style-type: none"> ► Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p> <p>La planification horaire place automatiquement dans des graphiques toutes les données de l'heure précédente.</p>

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
Daily Scheduling	<p>Le panneau Daily Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Daily dans le Report Wizard.</p> <p>1 Sélectionnez une des options suivantes :</p> <ul style="list-style-type: none"> • All data from previous day (24 hours) • Data of previous day from - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. <p>2 Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport.</p> <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p>

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
Weekly Scheduling	<p>Le panneau Weekly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Weekly dans le Report Wizard.</p> <ol style="list-style-type: none"> Sélectionnez une des options suivantes : <ul style="list-style-type: none"> All data from previous week All Data from previous week from - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut est le dimanche. Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. <p>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</p> <p>Afin d'affiner d'avantage votre planification :</p> <ol style="list-style-type: none"> Cochez la case Targeted Data Selection. Des options supplémentaires s'affichent. Cochez la case Only hours from, puis en utilisant les zones de liste, sélectionnez l'intervalle que vous souhaitez pour votre rapport. Par exemple, vous pouvez sélectionner uniquement les heures de 8h00 à 17h00. Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
Monthly Scheduling	<p>Le panneau Monthly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification Monthly dans le Report Wizard.</p> <ol style="list-style-type: none"> Sélectionnez une des options suivantes : <ul style="list-style-type: none"> All data from previous month Data from previous month from the - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut s'étend du 1er au 31. Dans la zone de liste Timezone, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. <p><i>Remarque : Lors de la configuration du paramètre Timezone, prenez en compte l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise des données provenant de plusieurs processeurs d'événements couvrant plusieurs fuseaux horaires, le fuseau horaire configuré peut être incorrect. Par exemple, si votre rapport est associé à des données recueillies auprès des processeurs d'événements en Amérique du nord et en Europe, et que vous configurez le fuseau horaire sur GMT -5.00 America/New_York, les données provenant d'Europe indiquent le fuseau horaire de manière incorrecte.</i></p> <p>Afin d'affiner d'avantage votre planification :</p> <ol style="list-style-type: none"> Cochez la case Targeted Data Selection. Des options supplémentaires s'affichent. Cochez la case Only hours from, puis en utilisant les zones de liste, sélectionnez l'intervalle que vous souhaitez pour votre rapport. Par exemple, vous pouvez sélectionner uniquement les heures de 8h00 à 17h00. Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.
Graph Content	
Group	<p>Dans la zone de liste, sélectionnez un groupe recherche enregistrée pour afficher les recherches enregistrées appartenant à ce groupe dans la zone de liste Available Saved Searches.</p>

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
Type Saved Search or Select from List	Pour affiner la liste Available Saved Searches , entrez le nom de la recherche que vous souhaitez localiser dans la zone Type Saved Search or Select from List . Vous pouvez également entrer un mot-clé pour afficher la liste des recherches incluant ce mot clé. Par exemple, entrez Firewall afin d'afficher une liste de toutes les recherches qui incluent Firewall dans le nom de la recherche.

Tableau 10-7 Détails de conteneur de flux (suite)

Paramètre	Description
Available Saved Searches	Fournit une liste des recherches enregistrées disponibles. Toutes les recherches enregistrées disponibles s'affichent par défaut. Cependant, vous pouvez filtrer la liste en sélectionnant un groupe dans la zone de liste Group ou en entrant le nom d'une recherche enregistrée connue dans la zone Type Saved Search or Select from List .
Create New Flow Search	Cliquez sur Create New Flow Search afin de créer une nouvelle recherche. Pour plus d'informations sur la création d'une recherche de flux, voir Etudes des flux .

Top Source IPs

Le graphique de la principale source des espaces de présentation de l'image affiche et trie les principales sources d'infraction (adresses IP) qui attaquent votre réseau ou les actifs de l'entreprise.

- Pour configurer les détails de conteneur de la principale source des espaces de présentation de l'image, entrez des valeurs pour les paramètres suivants :

Tableau 10-8 Détails de conteneur des principales sources de l'espace de présentation de l'image

Paramètre	Description
Container Details - Top Source IPs	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Top	Dans la zone de liste, sélectionnez le nombre de sources à inclure dans les graphiques.
Graph Type	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : <ul style="list-style-type: none"> • Table - Affiche les données sous la forme d'un tableau (uniquement avec conteneur de largeur pleine page). • Horizontal Bar - Affiche les données dans un diagramme à barres.
Order Results By	Dans la zone de liste, sélectionnez le tri des données sur le graphique. Les options incluent : <ul style="list-style-type: none"> • Asset Weight • Risk • Magnitude

Graph Content

Tableau 10-8 Détails de conteneur des principales sources de l'espace de présentation de l'image (suite)

Paramètre	Description
Networks	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels vous pouvez recueillir des données graphiques.

Top Offenses

Le graphique Top Offenses affiche les principales infractions qui se produisent à l'heure actuelle pour les emplacements réseau que vous sélectionnez.

- ▶ Pour configurer les détails de conteneur des principales infractions, entrez des valeurs pour les paramètres suivants :

Tableau 10-9 Détails de conteneur des principales infractions

Paramètre	Description
Container Details - Top Offenses	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Top	Dans la zone de liste, sélectionnez le nombre des infractions à inclure dans les graphiques. La valeur configurée par défaut est 10.
Include	<p>Cochez la case à côté de l'option que vous souhaitez inclure dans le rapport généré. Les options sont :</p> <ul style="list-style-type: none"> • Active Offenses • Inactive Offenses • Hidden Offenses • Closed Offenses <p>Les options Active Offenses et Inactive Offenses sont sélectionnées par défaut.</p> <p>Si vous décochez toutes les cases, aucune restriction n'est appliquée au rapport généré; par conséquent, le rapport généré inclut toutes les infractions.</p>
Offenses Category	<p>A partir de la zone de liste High Level Category, sélectionnez la catégorie de haut niveau que vous souhaitez inclure dans le rapport généré.</p> <p>A partir de la zone de liste Low Level Category, sélectionnez la catégorie de bas niveau que vous souhaitez inclure dans le rapport généré.</p> <p>Pour plus d'informations sur les catégories de haut et de bas niveau, voir le <i>IBM Security QRadar Network Anomaly Detection Guide d'administration</i>.</p>
Graph Type	<p>Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent :</p> <ul style="list-style-type: none"> • Table - Affiche les données sous la forme d'un tableau (uniquement avec conteneur de largeur pleine page). • Horizontal Bar - Affiche les données dans un diagramme à barres.

Tableau 10-9 Détails de conteneur des principales infractions (suite)

Paramètre	Description
Order Results By:	Dans la zone de liste, sélectionnez le tri des données sur le graphique. Les options incluent : <ul style="list-style-type: none"> • Severity • Magnitude • Relevance • Credibility
Graph Content	
Networks	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels vous pouvez recueillir des données graphiques.

Top Destination IPs

Le graphique de la principale destination des espaces de présentation de l'image affiche la principale destination des espaces de présentation de l'image dans les emplacements réseaux que vous sélectionnez.

- Pour configurer les détails de conteneur de la principale destination des espaces de présentation de l'image, entrez des valeurs pour les paramètres suivants :

Tableau 10-10 Détails de conteneur des principales cibles des espaces de présentation de l'image

Paramètre	Description
Container Details - Top Destination IPs	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Top	Dans la zone de liste, sélectionnez le nombre d'éléments à inclure dans les graphiques. La valeur configurée par défaut est 10.
Graph Type	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : <ul style="list-style-type: none"> • Table - Affiche les données sous la forme d'un tableau (uniquement avec conteneur de largeur pleine page). • Horizontal Bar - Affiche les données dans un diagramme à barres.

Tableau 10-10 Détails de conteneur des principales cibles des espaces de présentation de l'image (suite)

Paramètre	Description
Order Results By	Dans la zone de liste, sélectionnez l'affichage des données dans le graphique. Les options incluent : <ul style="list-style-type: none">• Asset Weight• Risk Level• Magnitude
Graph Content	
Networks	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels vous pouvez recueillir des données graphiques.

Sélection d'un type de graphique

Chaque type de graphique prend en charge une variété de types de graphiques que vous pouvez utiliser pour afficher les données. Les fichiers de configuration de réseau déterminent les couleurs que les tableaux utilisent pour représenter le trafic réseau. Chaque adresse IP est représentée à l'aide d'une couleur unique.

Le tableau suivant donne des exemples des graphiques de réseau et des données de sécurité Détection des anomalies QRadar :

Tableau 10-11 Graph Types

Graph Type	Availability
Line Graph	Disponible avec les types de graphiques suivants : <ul style="list-style-type: none"> • Events/Logs • Flows
Stacked Line Graph	Disponible avec les types de graphiques suivants : <ul style="list-style-type: none"> • Events/Logs • Flows
Bar Graph	Disponible avec les types de graphiques suivants : <ul style="list-style-type: none"> • Events/Logs • Flows • Asset Vulnerabilities
Horizontal Bar Graph	Disponible avec les types de graphiques suivants : <ul style="list-style-type: none"> • Top Source IPs • Top Offenses • Top Destination IPs
Stacked Bar Graph	Disponible avec les types de graphiques suivants : <ul style="list-style-type: none"> • Events/Logs • Flows
Pie Graph	Disponible avec les types de graphiques suivants : <ul style="list-style-type: none"> • Events/Logs • Flows • Asset Vulnerabilities
Table Graph	Disponible avec les types de graphiques suivants : <ul style="list-style-type: none"> • Event/Logs • Flows • Top Source IPs • Top Offenses • Top Destination IPs <p>Pour afficher le contenu d'un tableau, vous devez concevoir le rapport avec un conteneur en pleine largeur de page.</p>

Tableau 10-11 Graph Types (suite)

Graph Type	Availability
Aggregate Table	Disponible avec le graphique Asset Vulnerabilities. Pour afficher le contenu d'un tableau, vous devez concevoir le rapport avec un conteneur en pleine largeur de page.

Personnalisation des rapports par défaut

Détection des anomalies QRadar fournit un nombre important de rapports par défaut que vous pouvez utiliser ou personnaliser. L'onglet par défaut **Reports** affiche la liste des rapports. Chaque rapport capture et affiche les données existantes.

Pour personnaliser les rapports par défaut :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Cliquez deux fois sur le rapport que vous souhaitez personnaliser.

L'assistant Report Wizard affiche les paramètres tels qu'ils sont préconfigurés pour le rapport par défaut.

Etape 3 Personnalisez le rapport.

Vous pouvez modifier tout paramètre afin de personnaliser le rapport pour générer le contenu dont vous avez besoin. Voir [Création de rapports personnalisés](#).

Groupement des rapports

Dans l'onglet **Reports**, vous pouvez trier la liste des rapports en groupes fonctionnels. Si vous classez les rapports en groupes, vous pouvez efficacement organiser et trouver des rapports. Par exemple, vous pouvez afficher tous les rapports relatifs à la conformité de la Payment Card Industry Data Security Standard (PCIDSS). Par défaut, l'onglet **Reports** affiche la liste de tous les rapports, Cependant, vous pouvez classer les rapports dans des groupes tels que :

- Compliance
- Executive
- Log Sources
- Network Management
- Security
- VoIP
- Other

Lorsque vous créez un nouveau rapport, vous pouvez affecter le rapport à un groupe existant ou créer un nouveau groupe. Pour plus d'informations sur l'affectation d'un rapport à un groupe en utilisant de l'assistant de rapport, voir [Personnalisation des rapports par défaut](#).

REMARQUE

Vous devez disposer d'un accès administratif afin de créer, modifier ou supprimer des groupes. Pour plus d'informations sur les rôles d'utilisateur, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Cette section comprend les rubriques suivantes :

- **Création d'un groupe**
- **Modification d'un groupe**
- **Affectation d'un rapport à un groupe**
- **Copie d'un rapport vers un autre groupe**
- **Suppression d'un rapport d'un groupe**

Création d'un groupe Pour créer un groupe :

- Etape 1** Cliquez sur l'onglet **Reports**.
- Etape 2** Cliquez sur **Manage Groups**.
- Etape 3** En utilisant l'arborescence de navigation, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.
Après avoir créé le groupe, vous pouvez glisser-déposer les éléments de l'arborescence de navigation pour modifier l'organisation des éléments de l'arborescence.
- Etape 4** Cliquez sur **New Group**.
- Etape 5** Entrez les valeurs pour les paramètres suivants :
 - **Name** - Entrez le nom pour le nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
 - **Description** - Entrez une description pour ce groupe. La description peut comporter jusqu'à 255 caractères. Cette zone est facultative.
- Etape 6** Cliquez sur **OK**.
- Etape 7** Pour modifier l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers le nouvel emplacement sur l'arborescence de navigation.
- Etape 8** Fermez la fenêtre Report Groups.

Modification d'un groupe En utilisant l'icône **Edit**, vous pouvez modifier le nom ou la description d'un groupe de rapports.

Pour modifier un groupe:

- Etape 1** Cliquez sur l'onglet **Reports**.
- Etape 2** Cliquez sur **Manage Groups**.
- Etape 3** Dans l'arborescence de navigation, sélectionnez le groupe que vous souhaitez éditer.

Etape 4 Cliquez sur **Edit**.

Etape 5 Mettez les valeurs des paramètres à jour, si nécessaire :

- **Name** - Entrez le nom pour le nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
- **Description** - Entrez une description pour ce groupe. La description peut comporter jusqu'à 255 caractères. Cette zone est facultative.

Etape 6 Cliquez sur **OK**.

Etape 7 Fermez la fenêtre Report Groups.

Affectation d'un rapport à un groupe En utilisant l'option **Assign Groups**, vous pouvez affecter un rapport à un autre groupe.

Pour affecter un rapport à un groupe :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez le rapport que vous souhaitez affecter à un groupe.

Etape 3 A partir de la zone de liste **Actions**, sélectionnez **Assign Groups**.

Etape 4 Dans la liste **Item Groups**, cochez la case du groupe auquel vous souhaitez attribuer à ce rapport.

Etape 5 Cliquez sur **Assign Groups**.

Copie d'un rapport vers un autre groupe En utilisant l'icône **Copy**, vous pouvez copier un rapport vers un ou plusieurs groupes de rapports.

Pour copier un rapport d'un groupe vers un autre :

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Cliquez sur **Manage Groups**.

Etape 3 Dans l'arborescence de navigation, sélectionnez le rapport que vous souhaitez copier.

Etape 4 Cliquez sur **Copy**.

Etape 5 Sélectionnez le groupe ou les groupes vers lesquels vous souhaitez copier le rapport.

Etape 6 Cliquez sur **Assign Groups**.

Etape 7 Fermez la fenêtre Report Groups.

Suppression d'un rapport d'un groupe Si vous supprimez un rapport d'un groupe, l'action ne supprime pas le rapport. Le rapport existe toujours sur l'onglet **Reports**.

Pour supprimer un rapport d'un groupe:

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Cliquez sur **Manage Groups**.

- Etape 3** Dans l'arborescence de navigation, accédez au dossier qui contient le rapport que vous souhaitez supprimer.
- Etape 4** Dans la liste des groupes, sélectionnez le rapport que vous souhaitez supprimer.
- Etape 5** Cliquez sur **Remove**.
- Etape 6** Cliquez sur **OK**.
- Etape 7** Fermez la fenêtre Report Groups.

Générer manuellement un rapport

Pour générer manuellement un rapport :

- Etape 1** Cliquez sur l'onglet **Reports**.
- Etape 2** Sélectionnez le rapport que vous souhaitez générer.
- Etape 3** Cliquez sur **Run Report**.

Le rapport génère. Alors que le rapport génère, la colonne **Next Run Time** affiche l'un des trois messages suivants :

- **Generating** - Le rapport est en cours de génération.
- **Queued (*position in the queue*)** - Le rapport est mis en attente pour la génération. Le message indique la position du rapport en file d'attente. Par exemple, 1 de 3.
- **(x hour(s) x min(s) y sec(s))** - Le rapport est planifié pour s'exécuter. Le message est un compte à rebours qui indique quand le rapport suivant sera exécuté.

REMARQUE

Vous pouvez sélectionner l'icône **Refresh** pour actualiser l'affichage, y compris les informations dans la colonne **Next Run Time**.

Après la génération d'un rapport, vous pouvez afficher le rapport généré dans la colonne **Generated Reports**. Voir [Affichage des rapports générés](#).

Dupliquer un rapport

Pour dupliquer un rapport :

- Etape 1** Cliquez sur l'onglet **Reports**.
- Etape 2** Sélectionnez le rapport que vous souhaitez dupliquer.
- Etape 3** Dans la zone de liste **Actions**, cliquez sur **Duplicate**.
- Etape 4** Entrez un nouveau nom, sans espaces, pour le rapport.

Partage d'un rapport

Vous pouvez partager des rapports avec d'autres utilisateurs. Lorsque vous partager un rapport, vous devez fournir une copie du rapport sélectionné à un

autre utilisateur pour modifier ou planifier. Toutes les mises à jour effectuées par l'utilisateur sur un rapport partagé n'affectent pas la version originale du rapport.

REMARQUE

Vous devez disposer de privilèges administratifs afin de partager des rapports. En outre, pour qu'un nouvel utilisateur puisse afficher et accéder aux rapports, un administrateur doit partager tous les rapports nécessaires avec le nouvel utilisateur.

Pour partager un rapport :

- Etape 1** Cliquez sur l'onglet **Reports**.
- Etape 2** Sélectionnez le rapport que vous souhaitez partager.
- Etape 3** Dans la zone de liste **Actions**, cliquez sur **Share**.
- Etape 4** Dans la liste des utilisateurs, sélectionnez les utilisateurs avec lesquels vous souhaitez partager ce rapport.
Si aucun utilisateur ayant un accès approprié n'est disponible, un message s'affiche.
- Etape 5** Cliquez sur **Share**.

Marquer des rapports

Pour marquer les rapports, vous pouvez importer des logos et des images spécifiques. Le rapport de marque est bénéfique pour votre entreprise si vous prenez en charge plus d'un seul logo. Lorsque vous importez une image Détection des anomalies QRadar, l'image est automatiquement enregistrée en tant que Portable Network Graphic (PNG). Nous vous recommandons l'utilisation des graphiques 144 x 50 pixels avec un fond blanc.

Pour des rapports de marque avec des logos personnalisés, vous devez télécharger et configurer les logos avant de commencer à utiliser le Report Wizard.

Pour marquer un rapport :

- Etape 1** Cliquez sur l'onglet **Reports**.
- Etape 2** Dans le menu de navigation, cliquez sur **Branding**.
- Etape 3** Cliquez sur **Browse** afin de parcourir les fichiers situés sur votre système.
- Etape 4** Sélectionnez le fichier qui contient le logo que vous souhaitez télécharger.
- Etape 5** Cliquez sur **Open**.

Le nom de fichier s'affiche dans la zone **New Image**.

- Etape 6** Cliquez sur **Upload Image** afin d'importer l'image sur Détection des anomalies QRadar.

REMARQUE

Pour vous assurer que votre navigateur affiche le nouveau logo, désactivez votre cache du navigateur.

Etape 7 Sélectionnez le logo que vous souhaitez utiliser par défaut et cliquez sur **Set Default Image**. Ce logo est affiché comme la première option dans le menu dans la page Specify Content du Report Wizard.

REMARQUE

Lorsque vous téléchargez une nouvelle image et que vous la définissez comme votre image par défaut, la nouvelle image par défaut n'est pas appliquée aux rapports qui ont été précédemment générés. La mise à jour du logo sur les rapports précédemment générés nécessite la génération manuelle d'un nouveau contenu dans le rapport.

REMARQUE

Si vous téléchargez une image dont la longueur ne peut être prise en charge par l'en-tête du rapport, l'image se redimensionne automatiquement pour s'adapter à l'en-tête; Il s'agit approximativement de 50 pixels de hauteur.

A

TESTS DE RÈGLE

Cette section fournit des informations sur les tests que vous pouvez appliquer à la règle notamment :

- [Tests de règles d'événements](#)
- [Tests de règle de flux](#)
- [Tests de règle commune](#)
- [Tests de règle de violation](#)
- [Tests de règle de détection d'anomalie](#)

Tests de règles d'événements

Cette section fournit des informations sur les tests de règle d'événement que vous pouvez appliquer à la règle notamment :

- [Tests de profil d'hôte.](#)
- [Test de port/IP](#)
- [Tests de propriété d'événement](#)
- [Tests de propriété commune](#)
- [Tests de la source du journal](#)
- [Tests de séquence de fonction :](#)
- [Fonction : Tests de compteur](#)
- [Fonction : Tests simple](#)
- [Données/Tests de temps](#)
- [Tests de propriété de réseau](#)
- [Fonction : Tests négatifs](#)

Tests de profil d'hôte

Les tests de profil d'hôte comprennent :

Tableau A-1 Règle d'événement : Tests de profil d'hôte

Test	Description	Nom du test par défaut	Paramètres
Port de profil d'hôte	<p>Validez lorsque le port est ouvert sur une source ou une destination locale configurée. Vous pouvez également spécifier si le statut du port est détecté en utilisant l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Active - QRadar Network Anomaly Detection recherche activement des ports configurés via l'évaluation de la vulnérabilité et de l'analyse. • Passive - QRadar Network Anomaly Detection contrôle passivement le réseau concernant les hôtes déjà détectés. 	Lorsque le port de destination de l'hôte source est ouvert observé de façon active ou passive	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • actively seen passively seen either actively or passively seen - Indiquez si vous souhaitez que ce test considère l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est actively or passively seen.
Host Existence	<p>Validez lorsque l'hôte source ou de destination est connu pour sa présence via l'analyse active ou passive.</p> <p>Vous pouvez également spécifier si le statut de l'hôte est détecté en utilisant l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Active - QRadar Network Anomaly Detection recherche activement l'hôte configuré via l'évaluation de la vulnérabilité et de l'analyse. • Passive - QRadar Network Anomaly Detection contrôle passivement le réseau concernant les hôtes déjà détectés. 	Lorsque l'hôte local source existe either actively or passively seen	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique à l'hôte source ou de destination. La valeur par défaut est source. • actively seen passively seen either actively or passively seen - Indiquez si vous souhaitez que ce test considère l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est either actively or passively seen.

Tableau A-1 Règle d'événement : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Age de profil d'hôte	Validez lorsque la source locale ou de destination est supérieure à la valeur configurée dans les intervalles de temps configurés.	Lorsque l'âge du profil d'hôte source est supérieur au nombre d'intervalles de temps	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique l'hôte source ou de destination. La valeur par défaut est source IP. • greater than less than - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge d'hôte de du profil. • this number of - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • time intervals - Indiquez si ce test doit prendre en considération les minutes ou les heures.
Host Port Age	Validez lorsque l'âge du profil du port source ou de destination est supérieure ou inférieure au temps configuré.	lorsque l'âge du port de profil de l'hôte source (source) est supérieur à ce nombre d'intervalles de temps (greater than this number of time intervals)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • greater than less than - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge du port du profile. La valeur par défaut est greater than. • this number of - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • time intervals - Indiquez si ce test doit prendre en considération les minutes ou les heures.

Tableau A-1 Règle d'événement : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Asset Weight	Validez lorsque l'actif spécifié possède un poids affecté supérieur ou inférieur à la valeur configuré.	Lorsque l'actif cible (destination) a une pondération supérieur à cette pondération	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test considère l'actif source et de destination. La valeur par défaut est destination IP. • greater than less than equal to - Indiquez si vous souhaitez que la valeur soit supérieure, inférieure ou égale à la valeur configurée. • this weight - Indiquez le poids que ce test doit prendre en considération.
Host Vulnerable to Event	Validez lorsque le port de l'hôte spécifié est vulnérable à l'événement en cours.	Lorsque la cible (destination) est vulnérable à l'exploit en cours (current) sur n'importe quel (any) port	Configurez les paramètres suivants : <ul style="list-style-type: none"> • destination source local host remote host - Indiquez si vous souhaitez que ce test considère une destination, une source, un hôte local ou un hôte distant. source, local host, or remote host. La valeur par défaut est destination IP. • current any - Indiquez si vous souhaitez que ce test considère l'exploit en cours ou n'importe quel exploit. Le chemin par défaut est le suivant : current. • any current - Indiquez si vous souhaitez que ce test considère n'importe quel port en cours. La valeur par défaut est any IP.
OSVDB IDs	Validez lorsqu'une adresse IP (source ou destination) est vulnérable aux ID de Open Source Vulnerability Database (OSVDB) configurés.	lorsque l'IP source (source IP) est vulnérable à l'un des ID OSVDB (OSVDB ID) suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est source IP. • OSVDB IDs - Indiquez n'importe quel ID de OSVDB que ce test doit prendre en considération. Pour plus d'informations concernant les ID de OSVDB, consultez http://osvdb.org/.

Test de port/IP Les tests du Port/IP comprennent :**Tableau A-2** Event Rule: IP / Port Test Group

Test	Description	Nom du test par défaut	Paramètres
Source Port	Validez lorsque le port de la source de l'événement fait partie des ports source configurés.	lorsque le port source est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Destination Port	Validez lorsque le port de la destination de l'événement fait partie des ports de destination configurés.	lorsque le port destination est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Local Port	Validez lorsque le port local de l'événement fait partie des ports locaux configurés.	lorsque le port local est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Remote Port	Validez lorsque le port distant de l'événement fait partie des ports distants configurés.	lorsque le port remote est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Adresse IP source	Validez lorsque l'adresse IP source de l'événement est l'une des adresses IP configurées.	lorsque l'IP source est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Destination IP Address	Validez lorsque l'adresse IP de destination de l'événement est l'une des adresses IP configurées.	lorsque l'IP cible fait partie des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Local IP Address	Validez lorsque l'adresse IP local de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP locale est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Remote IP Address	Validez lorsque l'adresse IP distante de l'événement est l'une des adresses IP configurées.	lorsque l'IP distante est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
IP Address	Validez lorsque l'adresse IP source ou cible de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP source ou de destination est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Source or Destination Port	lorsque le port source ou de destination est l'un des ports configurés	lorsque le port source ou de destination est l'un de ces ports	these ports - Indiquez les ports que ce test doit prendre en considération.

Tests de propriété d'événement Le groupe de test de propriété d'événement comprend :

Tableau A-3 Règle d'événement : Tests de propriété d'événement

Test	Description	Nom du test par défaut	Paramètres
Local Network Object	Validez lorsque l'événement se produit dans le réseau spécifié.	Lorsque le réseau de destination est l'un des réseaux suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test considère l'adresse IP source ou de destination. • one of the following networks - Indiquez les zones des réseaux sur lesquelles vous souhaitez appliquer les tests.
IP Protocol	Validez lorsque le protocole IP de l'événement est l'un des protocoles configurés.	lorsque le protocole IP est l'un des protocoles suyvants	protocols - Indiquez les protocoles que vous souhaitez ajouter au test.
Event Payload Search	Chaque événement contient une copie de l'événement non normalisé original. Ce test est valide lorsque la chaîne de recherche entrée est incluse n'importe où dans le contenu de l'événement.	lorsque le contenu de l'événement contient cette chaîne (this string)	this string - Indiquez la chaîne de texte que vous souhaitez inclure dans le test.
QID of Event	Un QID est un identificateur unique pour les événements. Ce test est valide lorsque l'identificateur d'événement est configuré sur QID.	lorsque le QID d'événement de l'un des QID suivants	QIDs - Utilisez l'une des options suivantes pour localiser les QID : <ul style="list-style-type: none"> • Sélectionnez l'option Browse By Category et à partir des zones de liste, sélectionnez les QID de la catégorie supérieure et inférieure que vous souhaitez localiser. • Sélectionnez l'option QID Search et entrez le QID ou le nom que vous souhaitez localiser. Cliquez sur Search.
Event Context	Event Context est la relation entre l'adresse IP source et l'adresse IP de destination de l'événement. Par exemple, une adresse IP source locale vers une adresse IP de destination distante. Validez si le contexte d'événement est l'un des contextes suivants : <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote 	lorsque le contexte d'événement est ce contexte (this context)	this context - Indiquez le contexte que ce test doit prendre en considération. Les options sont : <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Category	Validez lorsque la catégorie d'événement est la même que celle qui est configurée, par exemple, Denial of Service (DoS) attack.	lorsque la catégorie d'événement pour l'événement est l'une des catégories suivantes	categories - Indiquez la catégorie d'événement que ce test doit prendre en considération. Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i> .
Severity	Validez lorsque la gravité de l'événement est supérieure, inférieure ou égale à la valeur configurée.	Lorsque la gravité de l'événement est supérieure à 5 {par défaut}	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si la gravité est supérieure, inférieure ou égale à la valeur configurée. • 5 - Indiquez l'index, qui est une valeur comprise entre 0 et 10. La valeur par défaut est 5.
Credibility	Validez lorsque la crédibilité est supérieure, inférieure ou égale à la valeur configurée.	Lorsque la crédibilité de la valeur est supérieure à 5 {par défaut}	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si la crédibilité est supérieure, inférieure ou égale à la valeur configurée. • 5 - Indiquez l'index, qui est une valeur comprise entre 0 et 10. La valeur par défaut est 5.
Relevance	Validez lorsque la pertinence est supérieure, inférieure ou égale à la valeur configurée.	Lorsque la pertinence est supérieure à 5 (par défaut)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si la pertinence est supérieure, inférieure ou égale à la valeur configurée. • 5 - Indiquez l'index, qui est une valeur comprise entre 0 et 10. La valeur par défaut est 5.
Source Location	Validez lorsque l'adresse IP source de l'événement est locale ou distante.	Lorsque la source est locale ou distante {par défaut : distante}	local remote - Indiquez le trafic local ou distant.
Destination Location	Validez lorsque l'adresse IP de destination de l'événement est locale ou distante.	Lorsque la destination est locale ou distante {par défaut : distante}	local remote - Indiquez le trafic local ou distant.

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Rate Analysis	<p>QRadar Network Anomaly Detection contrôle le taux d'événements de toutes les QID d'adresses IP source et de destination et marque les événements qui annexent le comportement de taux anormaux.</p> <p>Validez lorsque l'événement est marqué pour l'analyse de taux.</p>	Lorsque l'événement est marqué pour l'analyse de taux.	
False Positive Tuning	<p>Lorsque vous ajustez les événements des faux positifs sur l'onglet Log Activity, les valeurs de réglage s'affichent sur ce test. Si vous souhaitez annuler un réglage du faux positif, vous pouvez éditer les valeurs de réglage nécessaires.</p>	Lorsque la signature du faux positif correspond à l'une des signatures suivantes	<p>signatures - Indiquez la signature du faux positif que ce test doit prendre en considération. Entrez la signature dans le format suivant :</p> <p><CAT QID ANY>:<value>:<source IP>:<dest IP></p> <p>Où :</p> <p><CAT QID ANY> - Indiquez si vous souhaitez que cette signature de faux positif considère une catégorie (CAT), QRadar Identificateur (QID) ou une autre valeur.</p> <p><value> - Indiquez la valeur du paramètre <CAT QID ANY>. Par exemple, si vous indiquez QID, vous devez indiquer la valeur QID.</p> <p><source IP> - Indiquez l'adresse IP source que cette signature de faux positif doit prendre en considération.</p> <p><dest IP> - Indiquez l'adresse IP de destination que cette signature de faux positif doit prendre en considération.</p>

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	<p>Validez lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé à une chaîne d'expressions régulières particulières.</p> <p>Remarque : Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez des modèles d'expressions régulières, choisissez des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez consulter les didacticiels des expressions régulières disponibles sur le Web.</p>	lorsque le nom d'utilisateur (username) correspond à l'expression régulière suivante (regex)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • MAC source MAC destination MAC username source username destination username event username hostname source hostname dest hostname OS source OS dest OS event payload - Indiquez la valeur que vous souhaitez associer à ce test. La valeur par défaut est username. • regex - Indiquez la ligne de l'expression régulière que ce test doit prendre en considération.
IPv6	Validez lorsque l'adresse IPv6 de destination ou source correspond à l'adresse IP configurée.	lorsque l'adresse IP source (v6)((v6) source IP) fait partie des adresses IPv6 (IPv6) suivantes	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source IP(v6) destination IP(v6) - Indiquez si vous souhaitez que ce test considère l'adresse IPv6 source ou de destination. • IP(v6) addresses - Indiquez les adresses IPv6 que ce test doit prendre en considération.

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Set	Validez lorsque l'une ou toutes les propriétés d'événements sont comprises dans l'un ou tous les ensembles de références configurés.	Lorsque l'une de ces propriétés d'événement est comprise dans l'un de ces ensemble de référence	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez si vous souhaitez que ce test considère une ou toutes les propriétés d'événement configuré. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération • any all - Indiquez si vous souhaitez que ce test considère l'un ou tous les ensembles de référence configurés. • these reference set(s) - Indiquez les ensembles de référence que ce test doit prendre en considération.
Search Filter	Validez lorsque l'événement correspond au filtre de recherche spécifié.	Lorsque l'événement correspond à ce filtre de recherche	this search filter - Indiquez le filtre de recherche que ce test doit prendre en considération.

Tests de propriété commune

Le groupe de test de propriété commune comprend :

Tableau A-4 Règle d'événement : Tests de propriété commune

Test	Description	Nom du test par défaut	Paramètres
CVSS Risk (Host)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque l'hôte de destination possède une valeur de risque CVSS supérieure à cette valeur	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination either - Indiquez si le test considère l'hôte source ou de destination de l'événement. • greater than less than equal to - Indiquez si vous souhaitez que la valeur du risque CVSS soit supérieure, inférieure ou égale à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.
CVSS Risk (Port)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque le port de destination possède une valeur de risque CVSS supérieure à cette valeur	<ul style="list-style-type: none"> • source destination either - Indiquez si le test prend en considération le port source ou de destination de l'événement. • greater than less than equal to - Indiquez si vous souhaitez que le niveau de menace soit supérieur, inférieur ou égal à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.
Custom Rule Engines	Validez lorsque l'événement est traité par des moteurs de règle personnalisée spécifiée.	Lorsque l'événement est traité par l'un de ces moteurs de règles personnalisées (These Custom Rule Engines)	these - Indiquez le paramètre Custom Rule Engine que ce test doit prendre en considération.

Tableau A-4 Règle d'événement : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	<p>Validez lorsque la propriété configurée est associée à une chaîne d'expressions régulières particulières (regex).</p> <p>Remarque : Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez des modèles d'expressions régulières, choisissez des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez consulter les didacticiels des expressions régulières disponibles sur le Web.</p>	Si l'une de ces propriétés (these properties) correspond à l'expression régulière suivante	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these properties - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événement et de flux normalisées et personnalisées. • regex - Indiquez la ligne de l'expression régulière que ce test doit prendre en considération.
Hexadecimal	Validez lorsque la propriété configurée est associée à une valeur hexadécimale.	lorsque l'une de ces propriétés (these properties) comprend l'une de ces valeurs hexadécimales (these hexadecimal values)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these properties - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événement et de flux normalisées et personnalisées. • these hexadecimal values - Indiquez les valeurs hexadécimales que ce test doit prendre en considération.

Tests de la source du journal Les tests de la source du journal comprennent :

Tableau A-5 Règle d'événement : Log Source Tests

Test	Description	Nom du test par défaut	Paramètres
Source Log Sources	Validez lorsque l'une des sources du journal configurées est la source de l'événement.	Lorsque l'(les) événement (s) sont détectés par un ou plusieurs sources du journal (these log source)	these log sources - Indiquez les sources du journal que ce test doit détecter.

Tableau A-5 Règle d'événement : Log Source Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Log Source Type	Validez lorsque les types de la source du journal configurées est la source de l'événement.	lorsque l'événement est détecté par un ou plusieurs types de source du journal (these log source)	these log source - Indiquez les sources du journal que ce test doit détecter.
Inactive Log Sources	Validez lorsque l'une des sources du journal configurées n'a pas généré un événement à l'heure configurée.	lorsque l'événement est détecté par une ou plusieurs de ces sources de journal (these log sources) pour ces autant de secondes (this many seconds)	Configurez les paramètres suivants : these log sources - Indiquez les sources du journal que ce test doit détecter. this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération.
Log Source Groups	Validez lorsqu'un événement est détecté par les groupes de sources du journal configurés.	lorsque l'événement est détecté par un ou plusieurs de ces groupes de source du journal (these log source groups)	these log source groups - Indiquez les groupes que cette règle doit prendre en considération.

Tests de séquence de fonction : La fonction : les tests de séquence comprennent :

Tableau A-6 Règle d'événement : Fonctions - Sequence Group

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Event Function	Vous pouvez utiliser les blocs de construction ou d'autres règles de bloc pour effectuer ce test. Cette fonction vous permet de détecter une séquence spécifique de règles sélectionnées relatives à la source et à la destination dans une plage de temps configurée.	lorsque toutes ces règles (rules) sont définies dans l'ordre in in any, de the same any source IP à the same any destination IP , sur this many seconds	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si ce test doit prendre en considération l'ordre in ou in any. • the same any - Indiquez si vous souhaitez que ce test considère les composants same ou any des sources configurées. • username source IP source port destination IP destination port QID event ID log source category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • the same any - Indiquez si vous souhaitez que ce test considère les composants same ou any des destinations configurées. • destination IP username destination port - Indiquez si vous souhaitez que ce test considère une adresse IP de destination, un nom d'utilisateur ou un port de destination. La valeur par défaut est destination IP. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est seconds.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Event Function	Vous permet d'utiliser les blocs de construction ou d'autres règles pour effectuer ce test. Vous pouvez utiliser cette fonction pour détecter un nombre de règles spécifiées, en séquence, concernant une source ou une destination au sein d'un intervalle de temps configuré.	lorsqu'au moins ce nombre (this number) de ces règles (rules), dans un certain dans n'importe quel ordre (in in any) , depuis la même n'importe quelle adresse IP source (the same any source IP) vers la même n'importe quelle adresse IP cible (the same any destination IP), sur ce nombre de secondes (this many seconds)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this number - Indiquez le nombre de règles que cette fonction doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si ce test doit prendre en considération l'ordre in ou in any. • the same any - Indiquez si vous souhaitez que ce test considère les mêmes ou n'importe quelle (same ou any) source configurée. • username source IP source port destination IP destination port QID event ID log sources category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • the same any - Indiquez si vous souhaitez que ce test considère les valeurs same ou any des destinations configurées. • destination IP username destination port - Indiquez si vous souhaitez que ce test considère une adresse IP de destination, un nom d'utilisateur ou un port de destination. La valeur par défaut est destination IP. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Event Sequence Function Between Hosts	Vous permet de détecter une séquence des règles sélectionnées concernant les mêmes hôtes source et de destination dans l'intervalle de temps configuré. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour effectuer ce test.	lorsque cette séquence de rules , concernant le même hôte source et de destination dans this many seconds	Configurez les paramètres suivants : <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est seconds.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Function	Vous permet d'indiquer un nombre de règles spécifiques pour une adresse IP spécifique ou un port suivi par un nombre de règles spécifiques pour une adresse IP ou un port spécifique. Vous pouvez également utiliser des blocs de construction ou des règles existantes pour effectuer ce test.	lorsqu'au moins autant de (this many) de ces règles (rules), dans un certain dans n'importe quel ordre (in in any) , avec le même nom d'utilisateur (username) suivi par au moins autant de (this many) de ces règles (rules) dans un certain dans n'importe quel ordre (in in any) vers/depuis (to/from) la même adresse IP source (destination IP) que la séquence précédente, dans autant de minutes (this many minutes)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre de règles que ce test doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si vous souhaitez que ce test considère les règles dans un ordre spécifique. • username source IP source port destination IP destination port - Indiquez si vous souhaitez que ce test considère le nom d'utilisateur, l'IP source, le port source, l'IP de destination, ou le port de destination. La valeur par défaut est username. • this many - Indiquez le nombre de règles que ce test doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si vous souhaitez que ce test considère les règles dans un ordre spécifique. • to from - Indiquez la direction que ce test doit prendre en considération. • username source IP source port destination IP destination port - Indiquez si vous souhaitez que ce test considère le nom d'utilisateur, l'IP source, le port source, l'IP de destination ou le port de destination. La valeur par défaut est destination IP. • this many - Indiquez le nombre d'intervalles que cette règle doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que cette règle doit prendre en considération. La valeur par défaut est minutes.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et les différentes propriétés d'événement au sein de l'intervalle de temps configuré.	lorsque ces règles (these rules) correspondent à au moins autant de (this many) fois dans autant de minutes (this many minutes) une fois que ces règles (these rules) correspondent	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.
Event Property Function	Vous permet de détecter un nombre configuré de règles spécifiques avec les mêmes propriétés d'événement dans l'intervalle de temps configuré.	lorsque ces règles (these rules) correspondent à au moins autant de (this many) fois avec les mêmes propriétés d'événement (event properties) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées avec les propriétés d'événement identiques et différentes dans un intervalle de temps configuré après une série de règles spécifiques.	lorsque ces règles (these rules) correspondent à au moins autant de (this many) fois avec les mêmes propriétés d'événement (event properties) et des propriétés d'événement (event properties) différentes dans autant de minutes (this many minutes) une fois que ces règles these rules) correspondent	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées dans un intervalle de temps et une fois qu'une série de règles spécifiques s'est produite avec des propriétés d'événement identiques.	lorsque ces règles (these rules) correspondent à au moins autant de (this many) fois dans autant de minutes (this many minutes) une fois que ces règles (these rules) correspondent	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées avec des propriétés d'événement identiques dans un intervalle de temps une fois qu'une série de règles spécifiques s'est produite avec des propriétés d'événement identiques.	Lorsque ces règles (these rules) correspondent à au moins autant de (this many) fois avec les mêmes propriétés d'événement (event properties) autant de minutes (this many minutes) une fois que ces règles (these rules) correspondent avec les mêmes propriétés d'événement (event properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées dans un intervalle de temps après que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événement.	lorsque ces règles (these rules) correspondent à au moins autant de (this many) fois avec les mêmes propriétés d'événement (event properties) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent avec les mêmes propriétés (event properties)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des événements spécifiques qui se produisent avec les mêmes et les différentes propriétés d'événement dans un intervalle de temps après que des séries de règles spécifiques se produisent.	lorsqu'au moins autant de (this many) événements sont affichés avec les mêmes propriétés d'événement (event properties) et des propriétés d'événement (event properties) différentes dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des événements spécifiques qui se produisent avec les mêmes propriétés d'événement dans un intervalle de temps et une fois que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événement.	lorsqu'au moins autant de (this many) événements sont affichés avec les mêmes propriétés d'événement (event properties) dans autant de minutes (this many minutes) après que ces règles (these rules) correspondent avec les mêmes propriétés d'événement (event properties)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-6 Règle d'événement : Fonctions - Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des événements spécifiques qui se produisent avec les mêmes et les différentes propriétés d'événement dans un intervalle de temps et une fois que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événement.	lorsqu'au moins autant de (this many) événement sont observés avec des propriétés d'événement identiques (event properties) et des propriétés d'événement (event properties) différentes dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Fonction : Tests de compteur La fonction : les tests du compteur comprennent :

Tableau A-7 Règle d'événement : Fonctions - Counters Group

Test	Description	Nom du test par défaut	Paramètres
Multi-Event Counter Function	Vous permet de tester le nombre d'événement à partir des conditions configurées, telles que, l'adresse IP source. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour effectuer ce test.	Lorsqu'une adresse IP (source IP) correspond à plus de exactement (more than exactly) autant de règles (of these rules) via plus de exactement (across more than exactly) this many destination IP, over this tant de minutes many minutes	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • username source IP source port destination IP destination port QID event ID log sources category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • more than exactly - Indiquez si vous souhaitez que ce test considère exactement le nombre de règle ou plus. • this many - Indiquez le nombre de règles que ce test doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • more than exactly - Indiquez si vous souhaitez que ce test considère le nombre exacte d'adresses IP de destination, de ports de destination, de QID, d'ID d'événement source ou de sources log que vous sélectionnez dans la source précédente. • this many - Indiquez le nombre d'adresse IP, de ports, de QID, d'événements, de source de journal ou des catégories que ce test doit prendre en considération. • username destination IP source IP source port destination port QID event ID log sources category - Indiquez la destination que ce test doit prendre en considération. La valeur par défaut est destination IP. • this many - Indiquez le temps de la valeur que vous souhaitez affecter à ce test. • seconds minutes hours days - Indiquez l'intervalle de temps que cette règle doit prendre en considération. La valeur par défaut est minutes.

Tableau A-7 Règle d'événement : Fonctions - Counters Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Function	Vous permet de détecter une série de règles pour une adresse IP spécifique par des séries de règles spécifiques pour une adresse IP ou un port spécifique. Vous pouvez également utiliser les blocs de construction ou des règles existantes pour effectuer ce test.	Lorsqu'une de ces règles (rules) avec la même adresse IP source (source IP) plus de autant fois (this many) times, via le nombre exacte ou plus d'adresse IP de destination (more than exactly this many destination IP) dans autant de minutes (this many minutes)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • username source IP source port destination IP destination port QID event ID log sources category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • more than exactly - Indiquez si vous souhaitez que ce test considère le nombre exacte d'adresses IP de destination, de ports de destination, de QID, d'ID d'événement source ou de sources log que vous sélectionnez dans la source précédente. • this many - Indiquez le nombre que ce test doit prendre en considération selon l'option configurée dans le paramètre IP source. • username destination IP source IP source port destination port QID event ID log sources category - Indiquez la destination que ce test doit prendre en considération. La valeur par défaut est destination IP. • this many - Indiquez l'intervalle de temps que vous souhaitez affecter à ce test. • seconds minutes hours days - Indiquez l'intervalle de temps que cette règle doit prendre en considération. La valeur par défaut est minutes.

Tableau A-7 Règle d'événement : Fonctions - Counters Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Username Function	Vous permet de détecter les différentes mises à jour des noms d'utilisateurs sur un hôte unique.	Lorsque le nom d'utilisateur (username) change plus d'autant de fois (this many times) dans autant d'heures (this many hours) sur un hôte unique (sigle host).	Configurez les paramètres suivants : <ul style="list-style-type: none"> • MAC username hostname - Indiquez si vous souhaitez que ce test considère le nom d'utilisateur, l'adresse MAC ou le nom de l'hôte. La valeur par défaut est username. • this many - Indiquez le nombre de changements que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est hours.
Event Property Function	Vous permet de détecter des séries d'événements avec les mêmes propriétés d'événement dans l'intervalle de temps configuré. Par exemple, si vous pouvez utiliser ce test lors 100 événements avec la même adresse IP source se produisent dans 5 minutes.	Lorsque au moins autant d'événements (this many events) sont affichés avec les mêmes propriétés (event properties) dans autant de minutes (this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Tableau A-7 Règle d'événement : Fonctions - Counters Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	<p>1Allows you to detect a series of events with the same event properties and different event properties within the configured time interval.</p> <p>Par exemple, si vous pouvez utiliser ce test pour détecter lorsque 100 événements avec la même adresse IP source et une adresse IP de destination différente se produisent dans 5 minutes.</p>	Lorsqu'au moins autant d'événements (this many) sont affichés avec les mêmes propriétés d'événements (event properties) et des propriétés d'événements différentes (event properties) dans autant de minutes (this many minutes)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes propriétés d'événement dans l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à ce temps (this many times) dans autant de minutes (this many minutes)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Tableau A-7 Règle d'événement : Fonctions - Counters Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes propriétés d'événement dans l'intervalle de temps configuré.	Lorsque (these rules) correspondent au moins à ce temps (this many times) avec les mêmes propriétés d'événements (event properties) dans autant de minutes (this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.
Event Property Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et les différentes propriétés d'événement au sein de l'intervalle de temps configuré.	Lorsque es règles (these rules) correspondent au moins autant de (this many) fois avec les mêmes propriétés et des propriétés d'événement (event properties) dans autant de minutes (in this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Fonction : Tests simple La fonction - les tests simple :

Tableau A-8 Règle d'événement : Simple Group

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Event Function	Vous permet d'utiliser les blocs de construction sauvegardés ou d'autres règles pour effectuer ce test. L'événement doit correspondre à toutes ou l'une des règles sélectionnées. Si vous souhaitez créer une instruction OR pour le test de cette règle, spécifiez le paramètre any .	Lorsqu'un événement correspond à l'une ou à toutes (any all) les règles suivantes	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez soit l'une (any) ou toutes (all) les règles configurées qui devraient s'appliquer à ce test. • rules - Indiquez les règles que ce test doit prendre en considération.

Données/Tests de temps Les données et les tests de temps comprennent :

Tableau A-9 Event Rule: Date/Time Tests

Test	Description	Nom du test par défaut	Paramètres
Event Day	Lorsque l'événement se produit à la date configurée.	lorsque le(s) événement(s) se produit à (on) la date sélectionnée selected	Configurez les paramètres suivants : <ul style="list-style-type: none"> • on after before - Indiquez si vous souhaitez que ce test considère avant, après ou à la date configurée. La valeur par défaut est on IP. • selected - Indiquez le jour du mois que ce test doit prendre en considération.
Event Week	Validez lorsque l'événement se produit pendant les jours du mois configurés.	lorsque le ou les événements se produisent dans l'un de ces jours de la semaine (these days of the week)	these days of the week - Indiquez les jours de la semaine que ce test doit prendre en considération.
Event Time	Validez lorsque l'événement se produit avant, après ou à l'heure configurée.	lorsque l'événement se produit après cette heure (after this time)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • after before at - Indiquez si ce test doit prendre en considération avant, après ou à la date configuré. La valeur par défaut est after IP. • this time - Indiquez l'heure que ce test doit prendre en considération.

Tests de propriété de réseau

Le test de la propriété du réseau comprend :

Tableau A-10 Règle d'événement : Tests de propriété de réseau

Test	Description	Nom du test par défaut	Paramètres
Local Networks	Validez lorsque l'événement se produit dans le réseau spécifié.	lorsque le réseau local est one of the following	one of the following networks - Indiquez les zones de réseaux sur lesquelles vous souhaitez appliquer les tests.
Remote Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux distants.	lorsque l' IP source fait partie de l'un des emplacements de réseaux distants suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • remote network locations - Indiquez les emplacements de réseau que ce test doit prendre en considération.
Remote Services Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux des services distants configurés.	lorsque l' IP source fait partie de l'un des emplacements réseau de service distants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • remote services network locations - Indiquez les emplacements de réseau de services que ce teste doit prendre en considération.
Geographic Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements des réseaux géographiques configurés.	lorsque Source IP fait partie de l'un des emplacements géographiques de réseaux	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • geographic network locations - Indiquez les emplacements réseau que ce test doit prendre en considération.

Fonction : Tests négatifs La fonction - les tests négatifs comprennent :

Tableau A-11 Règle d'événement : Negative Group

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter lorsqu'aucune des règles spécifiées dans un intervalle de temps configuré après que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événements	Lorsqu'aucune de ces règles (these rules) correspondent dans autant de minutes (this many minutes) après ces règles (these rules) correspondent avec les mêmes propriétés d'événement (event properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.
Rule Function	Vous permet de détecter lorsqu'aucune de ces règles spécifiées dans un intervalle de temps configuré après que des séries de règles se sont produites.	Lorsqu'aucune de ces règles (these rules) ne correspondent dans autant de minutes (this many minutes) après ces règles (these rules) correspondent	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tests de règle de flux

Cette section fournit des informations sur les tests de règle de flux que vous pouvez appliquer à la règle notamment :

- [Tests de profil d'hôte](#)

- **Test de port/IP**
- **Tests de propriété de flux**
- **Tests de propriété commune**
- **Fonction - Tests de séquence**
- **Fonction - Tests de compteur**
- **Fonction : Tests simple**
- **Données/Tests de temps**
- **Tests de propriété de réseau**
- **Fonction : Tests négatifs**

Tests de profil d'hôte Les tets de profil d'hôte comprennent :

Tableau A-12 Règle dE FLUX : Tests de profil d'hôte

Test	Description	Nom du test par défaut	Paramètres
Port de profil d'hôte	<p>Validez lorsque le port est ouvert sur une source ou une destination locale configurée. Vous pouvez également spécifier si le statut du port est détecté en utilisant l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Active - QRadar Network Anomaly Detection recherche activement des ports configurés via l'évaluation de la vulnérabilité et de l'analyse. • Passive - QRadar Network Anomaly Detection contrôle passivement le réseau concernant les hôtes déjà détectés. 	<p>lorsque le port de destination de l'hôte source est ouvert activement ou passivement seen</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • actively seen passively seen either actively or passively seen - Indiquez si vous souhaitez que ce test considère l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est either actively or passively seen.

Tableau A-12 Règle dE FLUX : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Host Existence	<p>Validez lorsque l'hôte source ou de destination est connu pour sa présence via l'analyse active ou passive.</p> <p>Vous pouvez également spécifier si le statut du host est détecté en utilisant l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Active - QRadar Network Anomaly Detection recherche activement des ports configurés via l'évaluation de la vulnérabilité et de l'analyse. • Passive - QRadar Network Anomaly Detection contrôle passivement le réseau concernant les hôtes déjà détectés. 	Lorsque l'hôte local source existe either actively or passively seen	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • actively seen passively seen either actively or passively seen - Indiquez si vous souhaitez que ce test considère l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est either actively or passively seen.
Age de profil d'hôte	Validez lorsque la source locale ou de destination est supérieure à la valeur configurée dans les intervalles de temps configurés.	Lorsque l'âge du profil d'hôte source est supérieur au nombre d'intervalles de temps	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique l'hôte source ou de destination. La valeur par défaut est source IP. • greater than less than - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge d'hôte de du profil. • this number of - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • time intervals - Indiquez si ce test doit prendre en considération les minutes ou les heures.

Tableau A-12 Règle dE FLUX : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Host Port Age	Validez lorsque l'âge du profil du port source ou de destination est supérieure ou inférieure au temps configuré.	lorsque l'âge du port de profil de l'hôte source (source) est supérieur à ce nombre d'intervalles de temps (greater than this number of time intervals)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • greater than less than - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge du port du profile. La valeur par défaut est greater than. • this number of - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • time intervals - Indiquez si ce test doit prendre en considération les minutes ou les heures.
Asset Weight	Validez lorsque l'unité (destination) est attaquée ou l'hôte est l'attaquant (source) a une pondération assignée supérieure ou inférieure à la valeur configurée.	Lorsque l'actif cible (destination) a une pondération supérieur à cette pondération	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test considère l'actif source et de destination. La valeur par défaut est destination IP. • greater than less than equal to - Indiquez si vous souhaitez que la valeur soit supérieure, inférieure ou égale à la valeur configurée. • this weight - Indiquez le poids que ce test doit prendre en considération.
OSVDB IDs	Validez lorsqu'une adresse IP (source ou destination) est vulnérable aux ID de Open Source Vulnerability Database (OSVDB) configurés.	lorsque l'IP source (source IP) est vulnérable à l'un des ID OSVDB (OSVDB ID) suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est source IP. • OSVDB IDs - Indiquez n'importe quel ID de OSVDB que ce test doit prendre en considération. Pour plus d'informations concernant les ID de OSVDB, consultez http://osvdb.org/.

Test de port/IP Les tests du Port/IP comprennent :**Tableau A-13** Flow Rules: IP / Port Test Group

Test	Description	Nom du test par défaut	Paramètres
Source Port	Validez lorsque le port de la source du flux est l'un des ports source configurée.	lorsque le port source est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Destination Port	Validez lorsque le port de destination du flux est l'un des ports de destination configurés.	lorsque le port destination est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Local Port	Validez lorsque le port local du flux est l'un des ports locaux configurés.	lorsque le port local est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Remote Port	Validez lorsque le port distant du flux est l'un des ports distants configurés.	lorsque le port distant est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Adresse IP source	Validez lorsque l'adresse IP source du flux est l'une des adresses IP configurées.	lorsque l'IP source est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Destination IP Address	Validez lorsque l'adresse IP de destination du flux est l'une des adresses IP configurées.	lorsque l'IP cible fait partie des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Local IP Address	Validez lorsque l'adresse IP local du flux est l'une des adresses IP configurées.	lorsque l'adresse IP locale est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Remote IP Address	Validez lorsque l'adresse IP distante du flux est l'une des adresses IP configurées.	lorsque l'IP distante est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
IP Address	Validez lorsque l'adresse IP source du flux est l'une des adresses IP de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP source ou de destination est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Source or Destination Port	lorsque le port source ou de destination est l'un des ports configurés	lorsque le port source ou de destination est l'un de ces ports	these ports - Indiquez les ports que ce test doit prendre en considération.

Tests de propriété de flux Le test de propriété de flux comprend :**Tableau A-14** Règles de flux : Flow Property Tests

Test	Description	Nom du test par défaut	Paramètres
IP Protocol	Validez lorsque le protocole IP du flux est l'un des protocoles configurés.	lorsque le protocole IP est l'un des protocoles suivants	protocols - Indiquez les protocoles que vous souhaitez ajouter au test.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Context	<p>Le contexte du flux est la relation entre l'adresse IP source et l'adresse IP de destination du flux. Par exemple, une adresse IP source locale vers une adresse IP de destination distante.</p> <p>Validez si le contexte du flux est l'un des suivants :</p> <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote 	Lorsque le contexte du flux est this context	<p>this context - Indique le contexte que ce test doit prendre en considération. Les options sont :</p> <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Validez lorsque l'adresse IP source de l'événement est locale ou distante.	Lorsque la source est locale ou distante {par défaut : distante}	local remote - Indiquez le trafic local ou distant. La valeur par défaut est remote IP .
Destination Location	Validez lorsque l'adresse IP de destination du flux est locale ou distante.	Lorsque la destination est locale ou distante {par défaut : distante}	local remote - Indiquez le trafic local ou distant. La valeur par défaut est remote IP .
Regex	<p>Validez lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé avec une ligne d'expressions régulières particulières</p> <p>Remarque : <i>Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez des modèles d'expressions régulières, choisissez des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez consulter les didacticiels des expressions régulières disponibles sur le Web.</i></p>	lorsque le nom d'utilisateur (username) correspond à l'expression régulière suivante (regex)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • hostname source hostname destination hostname source payload destination payload - Indiquez la valeur que vous souhaitez associer avec ce test. La valeur par défaut est username. • regex - Indiquez la ligne de l'expression régulière que ce test doit prendre en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
IPv6	Validez lorsque l'adresse IPv6 de destination ou source correspond à l'adresse IP configurée.	Lorsque l'adresse IP source (v6) fait partie des adresses IP (v6) suivantes	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP(v6) destination IP(v6) - Indiquez si vous souhaitez que ce test considère l'adresse IPv6 source ou de destination. • IP(v6) addresses - Indiquez les adresses IPv6 que ce test doit prendre en considération.
Reference Set	Validez lorsque l'une ou toutes les propriétés du flux sont comprises dans l'un ou tous les ensembles de références configurés.	Lorsque l'une de ces propriétés du flux est comprise dans l'un de ces ensembles de références	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez si vous souhaitez que ce test considère une ou toutes les propriétés d'événement configuré. • these flow properties - Indiquez les propriétés du flux que ce test doit prendre en considération • any all - Indiquez si vous souhaitez que ce test considère l'un(any) ou tous (all) les ensembles de référence configurés. • these reference set(s) - Indiquez les ensembles de référence que ce test doit prendre en considération.
Flow Bias	Validez lorsque la direction du flux correspond à la tendance du flux configuré.	Lorsque la tendance du flux est l'une des tendances suivantes :	inbound outbound mostly inbound mostly outbound balanced - Indiquez la tendance du flux que ce test doit prendre en considération. La valeur par défaut est inbound IP .

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Byte / Packet Count	Validez lorsque le nombre d'octets ou de paquets correspond au montant configuré.	Lorsque les octets de la source sont supérieurs à ce montant	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination local remote - Indiquez si ce test doit prendre en considération les paquets ou les octets locaux ou distants de la source ou de la destination. La valeur par défaut est source IP. • bytes packets- Indiquez si ce test doit prendre en considération les paquets ou les octets. La valeur par défaut est bytes IP. • greater than less than equal to - Indiquez si le nombre d'octets ou de paquets est supérieure, inférieure ou égal à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.
Host Count	Validez lorsque le nombre des hôtes correspondent au montant configuré.	Lorsque le numéro des hôtes source est supérieur à ce montant .	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination local remote - Indiquez si vous souhaitez que ce test considère les hôtes locaux ou distant source ou de destination. La valeur par défaut est source IP. • greater than less than equal to - Indiquez si le nombre d'hôte est supérieure, inférieure ou égale à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Packet Rate	Validez lorsque le taux de paquets correspond au montant configuré.	Lorsque le taux de paquets source est supérieure à la valeur paquet/seconde	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination local remote - Indiquez si vous souhaitez que ce test considère le taux de paquets locaux ou distants source ou de destination. La valeur par défaut est source IP. • greater than less than equal to - Indiquez si le taux de paquets est supérieure, inférieure ou égale à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.
Flow Duration	Validez lorsque la durée du flux correspond à l'intervalle de temps configuré.	Lorsque la durée du flux est supérieure à la valeur par seconde	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si la durée du flux est supérieure, inférieure ou égale à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.
Flow Payload Search	Chaque flux contient une copie de l'événement d'origine non normalisé. Ce test est valide lorsque la ligne de recherche entrée est incluse n'importe où dans le contenu de l'événement.	lorsque le contenu de la source correspond à la ligne d'expressions régulières	Configurez les paramètres suivants : <ul style="list-style-type: none"> • testsource destination local remote - Indiquez si vous souhaitez que ce critère considère le contenu local ou distant de source et destination. La valeur par défaut est source IP. • matches the regex matches the hexadecimal - Indiquez si vous souhaitez faire correspondre à une expression régulière ou une chaîne hexadécimale. La valeur par défaut est regex. • string - Indiquez la ligne du texte que vous souhaitez inclure dans le test.
Flow Source Name	Validez lorsque le nom de la source de flux correspond aux valeurs configurées.	Lorsque le nom de la source de flux est l'un de these source	these sources - Indiquez les noms de la source que ce test doit prendre en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Interface	Validez lorsque l'interface de flux correspond aux valeurs configurées.	Lorsque l'interface du flux est l'une des these interfaces	these interfaces - Indiquez l'interface de flux que ce test doit prendre en considération.
Flow Type	Validez lorsque le type de flux correspond aux valeurs configurées.	Lorsque le type du flux est l'un des these flow types	these flow types - Indiquez le type de flux que ce test doit prendre en considération.
Byte/Packet Ratio	Validez lorsque le rapport octet/paquet correspond à la valeur configurée.	lorsque le rapport byte/packet source est supérieure à la valeur bytes/packet	Configurez les paramètres suivants : <ul style="list-style-type: none"> source destination local remote - Indiquez si vous souhaitez que ce critère considère le rapport byte/packet local ou distant source ou de destination. La valeur par défaut est source IP. greater than less than equal to - Indiquez si la durée du flux est supérieure, inférieure ou égale à la valeur configurée. value - Indiquez le rapport que ce test doit prendre en considération.
ICMP Type	Validez lorsque le type Internet Control Message Protocol (ICMP) correspond aux valeurs configurées.	lorsque le type ICMP est l'un des these types	these types - Indiquez les types ICMP que ce test doit prendre en considération.
ICMP Code	Validez lorsque le code ICMP correspond aux valeurs configurées.	lorsque le code ICMP est l'un de these codes	these codes - Indiquez les codes ICMP que ce test doit prendre en considération.
DSCP	Validez lorsque le code de services différenciés (DSCP) corresponde aux valeurs configurées.	lorsque le DSCP destination est l'un de these values	Configurez les paramètres suivants : <ul style="list-style-type: none"> source destination local remote either - Indiquez si vous souhaitez que ce test considère soit le DSCP source, destination, local, ou distant. La valeur par défaut est destination IP. these values - Indiquez les valeurs DSCP que ce test doit prendre en considération.
IP Precedence	Validez lorsque la priorité IP correspond aux valeurs configurées	lorsque la priorité IP destination est l'une de these values	Configurez les paramètres suivants : <ul style="list-style-type: none"> source destination local remote either - Indiquez si vous souhaitez que ce test considère soit le DSCP source, destination, local, ou distant. La valeur par défaut est destination IP. these values - Indiquez les valeurs de priorité IP que ce test doit prendre en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Packet Ratio	<p>Validez lorsque le ratio du paquet configuré correspond à la valeur configurée.</p> <p>Ce test vous permet de spécifier les valeurs dans le rapport du paquet.</p>	<p>lorsque le rapport de paquet source/destination est supérieure à cette valeur</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination local remote - Spécifiez la direction que ce test doit prendre en considération en tant que valeur précédente du rapport. La valeur par défaut est source IP. • greater than less than equal to - Indiquez si le rapport du paquet est supérieur, inférieur ou égal à la valeur configurée. • value - Indiquez le rapport que ce test doit prendre en considération.
TCP Flags	<p>Validez lorsque les indicateurs TCP correspondent aux valeurs configurées.</p>	<p>lorsque les indicateurs TCP destination sont exactement these flags</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination local remote - Indiquez si vous souhaitez que ce critère considère les indicateurs TCP source, destination, variables locaux ou distants. La valeur par défaut est destination IP. • are exactly includes all of includes any of - Indiquez si vous souhaitez que ce test considère exactement soit tous ou aucun des indicateurs TCP configurés. La valeur par défaut est are exactly. • these flags - Indiquez les indicateurs TCP que ce test doit prendre en considération.
IF Index	<p>Validez lorsque IF Index correspond aux valeurs configurées</p>	<p>lorsque la liste des indexes (interface) IF input comprend all de these values</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • input output either - Indiquez la direction que ce test doit prendre en considération. La valeur par défaut est input. • all any - Indiquez si vous souhaitez que ce test considère tout ou n'importe quelle valeur IF Index configurée.. • these values - Indiquez les indexes IF que ce test doit prendre en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
TCP Flag Combination	Validez lorsque les indicateurs TCP correspondent aux combinaisons d'indicateur configurées.	lorsque les indicateurs TCP de destination sont des these flag combinations	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination local remote - Indiquez si vous souhaitez que ce critère considère les indicateurs TCP source, destination, variables locaux ou distants. La valeur par défaut est destination IP. • these flag combinations - Indiquez les combinaisons d'indicateurs que ce test doit prendre en considération. Indicateurs séparés par des virgules.
Search Filter	Validez lorsque le flux correspond au filtre de recherche spécifié.	Lorsque le flux correspond à ce filtre de recherche	this search filter - Indiquez le filtre de recherche que ce test doit prendre en considération.
Flow Payload	Validez lorsque la partie spécifiée du flux possède ou ne possède pas un contenu.	lorsque la partie de destination du flux has des données de contenu	Configurez les paramètres suivants : <ul style="list-style-type: none"> • the source the destination the local the remote either - Indiquez si vous souhaitez que ce test le flux source, de destination, local, distant ou de chaque côté. La valeur par défaut est destination IP. • has has not - Indiquez si vous souhaitez que ce test considère les flux qui ont ou n'ont pas de contenu.

Tests de propriété commune Les données et les tests de temps comprennent :

Tableau A-15 Règles de flux : Tests de propriété commune

Test	Description	Nom du test par défaut	Paramètres
CVSS Risk (Host)	Validez lorsque l'hôte spécifié possède une valeur du risque CVSS qui correspond à la valeur configurée.	lorsque l'hôte de destination possède une valeur de risque CVSS supérieure à cette valeur	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination either - Indiquez si le test prend en considération l'hôte source ou de destination du flux. • greater than less than equal to - Indiquez si vous souhaitez que la valeur du risque CVSS est supérieure, inférieure ou égale à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.
CVSS Risk (Port)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque le port de destination possède une valeur de rique CVSS supérieure à cette valeur	<ul style="list-style-type: none"> • source destination either - Indiquez si le test prend en considération le port source ou de destination du flux. • greater than less than equal to - Indiquez si vous souhaitez que le niveau de menace soit supérieur, inférieur ou égal à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.
Custom Rule Engine	Validez lorsque le flux est traité par des moteurs de règle personnalisée spécifiée.	lorsque le flux est traité par l'un de These Custom Rule Engines	these - Indiquez l'ID Custom Rule Engine que ce test doit prendre en considération.

Tableau A-15 Règles de flux : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	<p>Validez lorsque la propriété configurée est associée avec une ligne des expressions régulières particulières (regex).</p> <p>Remarque : <i>Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez des modèles d'expressions régulières, choisissez des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez consulter les didacticiels des expressions régulières disponibles sur le Web.</i></p>	lorsque ces propriétés (these properties) correspondent à l'expression régulière suivante	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these properties - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événement et de flux normalisées et personnalisées. • regex - Indiquez la ligne de l'expression régulière que ce test doit prendre en considération.
Hexadecimal	Validez lorsque la propriété configurée est associée avec une valeur hexadécimale.	lorsque l'une de ces propriétés (these properties) comprend l'une de ces valeurs hexadécimales (these hexadecimal values)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these properties - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événement et de flux normalisées et personnalisées. • these hexadecimal values - Indiquez les valeurs hexadécimales que ce test doit prendre en considération.

Fonction - Tests de séquence

La fonction : les tests de séquence comprennent :

Tableau A-16 Règles de flux : Fonctions du groupe de séquence

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Flow Function	Vous permet d'utiliser les blocs de construction ou d'autres règles pour effectuer ce test. Cette fonction vous permet de détecter une séquence spécifique des règles sélectionnées relatives à la source et à la destination au sein d'une période de temps configurée.	lorsque toutes ces règles, in in any order, from the same any source IP to the same any destination IP, over this many seconds	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si ce test doit prendre en considération dans ou dans n'importe quel ordre. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source configurée. • 1 source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source destination. • destination IP destination port - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est destination IP. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est seconds.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Flow Function	Vous permet d'utiliser les blocs de construction ou d'autres règles pour effectuer ce test. Vous pouvez utiliser cette fonction pour détecter un nombre de règles spécifiées, en séquence, concernant une source ou une destination au sein d'un intervalle de temps configuré.	lorsqu'au moins ce nombre (this number) de ces règles (rules), dans cette ordre n'importe quel ordre (in in any order), à partir de la même n'importe quelle adresse IP source (the same any source IP) vers la même n'importe quelle adresse IP de destination (the same any destination IP) sur autant de secondes (this many seconds)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this number - Indiquez le nombre de règles que cette fonction doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si ce test doit prendre en considération dans ou dans n'importe quel ordre. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source configurée. • 1source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source destination. • destination IP destination port - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est destination IP. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Flow Sequence Function Between Hosts	Vous permet de détecter une séquence des règles sélectionnées concernant les mêmes hôtes source et de destination dans l'intervalle de temps configuré. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour effectuer ce test.	lorsque cette séquence de rules , concernant le même hôte source et de destination dans ce many seconds	Configurez les paramètres suivants : <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalle que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est seconds.
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et les différentes propriétés de flux au sein de l'intervalle de temps configuré.	lorsque ces règles (these rules) correspondent à au moins autant de fois (this many times) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter un nombre configuré de règles spécifiques avec des propriétés de flux identiques dans l'intervalle de temps configuré.	lorsque ces règles (these rules) correspondent à au moins autant de fois (this many times) avec des propriétés de flux identiques (flow properties) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées avec des propriétés de flux identiques et différentes dans un intervalle de temps configuré après une série de règles spécifiques.	lorsque ces règles (these rules) correspondent à au moins autant de fois (this many times) avec des propriétés de flux identiques (propriétés de flux) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées dans un intervalle de temps une fois qu'une série de règles spécifiques s'est produite avec des propriétés de flux similaires.	lorsque ces règles (these rules) correspondent à au moins autant de fois (this many times) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent avec les mêmes propriétés de flux (flow properties)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées avec les mêmes propriétés de flux dans un intervalle de temps et une fois que des séries de règles spécifiques se produisent avec les mêmes propriétés de flux.	lorsque ces règles (these rules) correspondent à au moins autant de fois (this many times) avec des propriétés de flux identiques (flow properties) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent avec des propriétés de flux identiques (flow properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these - Indiquez les règles que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées avec les mêmes ou différentes propriétés de flux dans un intervalle de temps configuré et une fois que des séries des règles spécifiques produisent avec les mêmes propriétés de flux.	lorsque ces règles (these rules) correspondent à au moins autant de fois (this many times) avec les mêmes propriétés de flux (flow properties) et des propriétés de flux différentes (flow properties) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent avec les mêmes propriétés de flux (flow properties)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter des flux spécifiques qui se produisent avec les mêmes et les différentes propriétés de flux dans un intervalle de temps configuré après que des séries de règles spécifiques se produisent.	lorsqu'au moins autant de flux (this many flows) sont observés avec les mêmes propriétés de flux (flow properties) et des propriétés de flux différentes (flow properties) dans autant de minutes (thismany o minutes) une fois ces règles (these rules) correspondent.	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this many - Indiquez le nombre de flux que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter un nombre spécifique de flux qui se produisent avec les mêmes propriétés de flux dans un intervalle de temps configuré une fois que des séries des règles spécifiques se produisent avec les mêmes propriétés de flux.	Lorsque au moins autant de flux (this many) flows sont observés avec les mêmes propriétés de flux (flow properties) dans autant de minutes (many minutes) une fois ces règles (these rules) correspondent avec les mêmes propriétés de flux (flow properties)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre de flux que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions du groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter des flux spécifiques qui se produisent avec des propriétés identique et différentes dans un intervalle de temps configuré une fois qu'une série de règles spécifiques s'est produite avec les mêmes propriétés de flux.	Lorsqu'au moins autant de (this many) flux sont affichés avec les mêmes propriétés de flux (flow properties) et des propriétés de flux (flow properties) différentes dans autant de minutes (this many minutes) après ces règles (< after these rules) correspondent avec les mêmes propriétés de flux (flow properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this many - Indiquez le nombre de flux que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Fonction - Tests de compteur

Les fonctions : les tests de compteur comprennent

Tableau A-17 Règles de flux : Fonctions - groupe de compteurs

Test	Description	Nom du test par défaut	Paramètres
Multi-Flow Counter Function	Vous permet de tester le nombre d'événement à partir des conditions configurées, telles que, l'adresse IP source. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour effectuer ce test.	Lorsqu'une adresse IP (source IP) correspond à plus de exactement (more than exactly) autant de règles (of these rules) via plus de exactement (across more than exactly) this many destination IP, over this tant de minutes many minutes	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • 1 source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • more than exactly - Indiquez si vous souhaitez que ce test considère exactement le nombre de règle ou plus. • this many - Indiquez le nombre de règles que ce test doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • more than exactly - Indiquez si vous souhaitez que ce test considère le nombre exacte d'adresses IP de destination, de ports de destination, de QID, d'ID d'événement source ou de sources log que vous sélectionnez dans la source précédente. • this many - Indiquez le nombre d'adresses IP, ports ou noms d'utilisateur que ce test doit prendre en considération. • username destination IP source IP source port destination port QID event ID log sources category - Indiquez la destination que ce test doit prendre en considération. La valeur par défaut est destination IP. • this many - Indiquez le temps de la valeur que vous souhaitez affecter à ce test. • seconds minutes hours days - Indiquez l'intervalle de temps que cette règle doit prendre en considération. La valeur par défaut est minutes.

Tableau A-17 Règles de flux : Fonctions - groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Function	Vous permet de détecter une série de règles pour une adresse IP spécifique par des séries de règles spécifiques pour une adresse IP ou un port spécifique. Vous pouvez également utiliser les blocs de construction ou des règles existantes pour effectuer ce test.	Lorsqu'une de ces règles (rules) avec la même adresse IP source (source IP) plus d'autant de fois (this many) times, via le nombre exacte ou plus d'adresse IP de destination (more than exactly this many destination IP) dans autant de minutes (this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • 1source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • more than exactly - Indiquez si vous souhaitez que ce test considère le nombre exacte d'adresses IP de destination, de ports de destination, de QID, d'ID d'événement source ou de sources log que vous sélectionnez dans la source précédente. • this many - Indiquez le nombre que ce test doit prendre en considération selon l'option configurée dans le paramètre IP source. • username destination IP source IP source port destination port QID event ID log sources category - Indiquez la destination que ce test doit prendre en considération. La valeur par défaut est destination IP. • this many - Indiquez l'intervalle de temps que vous souhaitez affecter à ce test. • seconds minutes hours days - Indiquez l'intervalle de temps que cette règle doit prendre en considération. La valeur par défaut est minutes.

Tableau A-17 Règles de flux : Fonctions - groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	<p>Vous permet de détecter des séries d'événements avec les mêmes propriétés d'événement dans l'intervalle de temps configuré.</p> <p>Par exemple, si vous pouvez utiliser ce test pour détecter lorsque 100 événements avec la même adresse IP source se produisent dans 5 minutes.</p>	<p>Lorsque au moins autant d'événements (this many flows) sont affichés avec les mêmes propriétés (flow properties) dans autant de minutes (this many minutes)</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre de flux que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.
Flow Property Function	<p>Vous permet de détecter des séries d'événements avec les mêmes propriétés d'événements et des propriétés d'événement différentes dans l'intervalle de temps configuré.</p> <p>Par exemple, si vous pouvez utiliser ce test pour détecter lorsque 100 événements avec la même adresse IP source et une adresse IP de destination différente se produisent dans 5 minutes.</p>	<p>Lorsqu'au moins autant d'événements (this many) sont affichés avec les mêmes propriétés d'événements (flow properties) et des propriétés d'événements différentes (flow properties) dans autant de minutes (this many minutes)</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre de flux que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Tableau A-17 Règles de flux : Fonctions - groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet de détecter un nombre configuré de règles spécifiques avec les mêmes propriétés de flux dans l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times in) dans autant de minutes this many minutes	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.
Flow Property Function	Vous permet de détecter un nombre configuré de règles spécifiques avec les mêmes propriétés de flux dans l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times) avec les mêmes propriétés de flux (flow properties) dans autant de minutes (this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Tableau A-17 Règles de flux : Fonctions - groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et les différentes propriétés de flux au sein de l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à ce nombre de fois (this many) times avec les mêmes propriétés de flux (flow properties) et des propriétés de flux différentes (flow properties) dans autant de minutes (this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Fonction : Tests simple La fonction - les tests simple :

Tableau A-18 Règles de flux : Fonctions - groupe de compteurs

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Flow Function	Vous permet d'utiliser les blocs de construction sauvegardés ou d'autres règles pour effectuer ce test. La violation doit correspondre à toutes ou l'une des règles sélectionnées. Si vous souhaitez créer une instruction OR pour le test de cette règle, spécifiez le paramètre any .	Lorsqu'un flux correspond à l'une ou à toutes (any all) les règles (rules) suivantes	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez soit l'une (any) ou toutes (all) les règles configurées qui devraient s'appliquer à ce test. • rules - Indiquez les règles que ce test doit prendre en considération.

Données/Tests de temps

Les données et les tests de temps comprennent :

Tableau A-19 Règles de flux : Tests Heure / Date

Test	Description	Nom du test par défaut	Paramètres
Flow Day	Validez lorsque le flux se produit au jour du mois configuré.	lorsque le(s) flux se produisent sur (on) le jour du mois sélectionné (selected)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • on after before - Indiquez si vous souhaitez que ce test considère avant, après ou à la date configurée. La valeur par défaut est on IP. • selected - Indiquez le jour du mois que ce test doit prendre en considération.
Flow Week	Validez lorsque le flux se produit pendant les jours du mois configurés.	lorsque le(s) flux se produit à l'un de ces jours de la semaine	these days of the week - Indiquez les jours de la semaine que ce test doit prendre en considération.
Flow Time	Validez lorsque le flux se produit avant, après ou à l'heure configurée.	Lorsque le(s) flux se produit après cette heure	Configurez les paramètres suivants : <ul style="list-style-type: none"> • after before at - Indiquez si ce test doit prendre en considération avant, après ou à la date configuré. La valeur par défaut est after IP. • this time - Indiquez l'heure que ce test doit prendre en considération.

Tests de propriété de réseau

Le test de la propriété du réseau comprend :

Tableau A-20 Règles de flux : Network Property Tests

Test	Description	Nom du test par défaut	Paramètres
Local Network Object	Validez lorsque le flux se produit dans le réseau spécifié.	lorsque le réseau local est one of the following	one of the following networks - Indiquez les zones des réseaux sur lesquelles vous souhaitez appliquer les tests.
Remote Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux distants.	lorsque l'adresse fait partie de l'un des emplacements de réseaux distants suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est source IP. • remote network locations - Indiquez les emplacements de réseau que souhaitez que le test considère.

Tableau A-20 Règles de flux : Network Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Services Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux des services distants configurés.	lorsque l'adresse IP fait partie de l'un de remote services network locations	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est source IP. • remote services network locations - Indiquez les emplacements de réseau de services que le test doit prendre en considération.
Geographic Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements des réseaux géographiques configurés.	lorsque source IP fait partie de l'un des emplacements géographiques de réseaux suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est source IP. • geographic network locations - Indiquez les emplacements de réseau que souhaitez que le test considère.

Fonction : Tests négatifs

La fonction - les tests négatifs comprennent :

Tableau A-21 Règles de flux : Fonctions : groupe négatif

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter des règles spécifiques qui se produisent dans un intervalle de temps configuré après que des séries de règles spécifiques se produisent avec les mêmes propriétés de flux.	Lorsqu'aucune de ces règles (these rules) ne correspond dans autant de minutes (this many minutes) après que ces règles (these rules) correspondent avec les mêmes propriétés de flux (flow properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • 1flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.
Rule Function	Vous permet de détecter lorsqu'aucune de ces règles spécifiées ne se produisent dans un intervalle de temps configuré après que des séries de règles se sont produites.	Lorsqu'aucune de ces règles (these rules) ne correspondent dans autant de minutes (this many minutes) après ces règles (these rules) correspondent	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tests de règle commune

Cette section fournit des informations sur les tests de règle commune que vous pouvez appliquer à l'événement et à l'enregistrement de flux à la fois notamment :

- [Tests de profil d'hôte](#)

- Tests IP/Port
- Tests de propriété commune
- Fonctions - Tests de séquence
- Fonction : tests de compteur
- Fonction : Tests simple
- Données/Tests de temps
- Tests de propriété de réseau
- Tests négatifs de fonctions

Tests de profil d'hôte Les tests de profil d'hôte comprennent :

Tableau A-22 Règle commune : Tests du profil d'hôte

Test	Description	Nom du test par défaut	Paramètres
Port de profil d'hôte	<p>Validez lorsque le port est ouvert sur une source ou une destination locale configurée. Vous pouvez également spécifier si le statut du port est détecté en utilisant l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Active - QRadar Network Anomaly Detection recherche activement des ports configurés via l'évaluation de la vulnérabilité et de l'analyse. • Passive - QRadar Network Anomaly Detection contrôle passivement le réseau concernant les hôtes déjà détectés. 	<p>lorsque le port de destination de l'hôte source est ouvert activement ou passivement seen</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • actively seen passively seen either actively or passively seen - Indiquez si vous souhaitez que ce test considère l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est either actively or passively seen.
Host Existence	<p>Validez lorsque l'hôte source ou de destination est connu pour sa présence via l'analyse active ou passive.</p> <p>Vous pouvez également spécifier si le statut du host est détecté en utilisant l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Active - QRadar Network Anomaly Detection recherche activement des ports configurés via l'évaluation de la vulnérabilité et de l'analyse. • Passive - QRadar Network Anomaly Detection contrôle passivement le réseau concernant les hôtes déjà détectés. 	<p>Lorsque l'hôte local source existe either actively or passively seen</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • actively seen passively seen either actively or passively seen - Indiquez si vous souhaitez que ce test considère l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est either actively or passively seen.

Tableau A-22 Règle commune : Tests du profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Age de profil d'hôte	Validez lorsque la source locale ou de destination est supérieure à la valeur configurée dans les intervalles de temps configurés.	Lorsque l'âge du profil d'hôte source est supérieur au nombre d'intervalles de temps	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiques si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • greater than less than - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge du port du profile. • this number of - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • time intervals - Indiquez si ce test doit prendre en considération les minutes ou les heures.
Host Port Age	Validez lorsque l'âge du profil du port d'hôte source ou cible est supérieure ou inférieure au temps configuré.	lorsque l'âge du port de profil de l'hôte source (source) est supérieur à ce nombre d'intervalles de temps (greater than this number of time intervals)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiques si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est source IP. • greater than less than - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge du port du profile. La valeur par défaut est greater than. • this number of - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • time intervals - Indiquez si ce test doit prendre en considération les minutes ou les heures.

Tableau A-22 Règle commune : Tests du profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Asset Weight	Validez lorsque l'unité (cible) est attaquée ou l'hôte est l'attaquant (source) a une pondération assignée supérieure ou inférieure à la valeur configurée.	Lorsque l'actif cible (destination) a une pondération supérieur à cette pondération	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination - Indiquez si vous souhaitez que ce test considère l'actif source et de destination. La valeur par défaut est destination IP. • greater than less than equal to - Indiquez si vous souhaitez que la valeur soit supérieure, inférieure ou égale à la valeur configurée. • this weight - Indiquez le poids que ce test doit prendre en considération.
OSVDB IDs	Validez lorsqu'une adresse IP (source ou destination) est vulnérable aux ID de Open Source Vulnerability Database (OSVDB) configurés.	lorsque l'IP source (source IP) est vulnérable à l'un des ID OSVDB (OSVDB ID) suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est source IP. • OSVDB IDs - Indiquez n'importe quel ID de OSVDB que ce test doit prendre en considération. Pour plus d'informations concernant les ID de OSVDB, consultez http://osvdb.org/.

Tests IP/Port Les tests IP/Port comprennent :

Tableau A-23 Règle commune : IP / Groupe de test du port

Test	Description	Nom du test par défaut	Paramètres
Source Port	Validez lorsque le port source de l'événement ou du flux fait partie des ports source configurés.	lorsque le port source est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Destination Port	Validez lorsque le port cible de l'événement ou du flux fait partie des ports cibles configurés.	lorsque le port destination est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Local Port	Validez lorsque le port local de l'événement ou du flux fait partie des ports locaux configurés.	lorsque le port local est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.

Tableau A-23 Règle commune : IP / Groupe de test du port (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Port	Validez lorsque le port cible de l'événement ou du flux fait partie des ports distants configurés.	lorsque le port distant est l'un des ports suivants	ports - Indiquez les ports que ce test doit prendre en considération.
Adresse IP source	Validez lorsque l'adresse IP source de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'IP source est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Destination IP Address	Validez lorsque l'adresse IP cible de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'IP cible fait partie des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Local IP Address	Validez lorsque l'adresse IP locale de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'adresse IP locale est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Remote IP Address	Validez lorsque l'adresse IP distante de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'IP distante est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
IP Address	Validez lorsque l'adresse IP source ou cible de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'adresse IP source ou de destination est l'une des adresses IP suivantes	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération.
Source or Destination Port	lorsque le port source ou de destination est l'un des ports configurés	lorsque le port source ou de destination est l'un de ces ports	these ports - Indiquez les ports que ce test doit prendre en considération.

Tests de propriété commune Les tests de propriété commune comprennent :

Tableau A-24 Règles communes : Tests de propriété commune

Test	Description	Nom du test par défaut	Paramètres
IP Protocol	Validez lorsque le protocole IP de l'événement ou du flux et l'un des protocoles configurés.	lorsque le protocole IP est l'un des protocoles suivants	protocols - Indiquez les protocoles que vous souhaitez ajouter au test.
Payload Search	Ce test est valide lorsque la ligne de recherche entrée est incluse n'importe où dans le contenu source ou cible de l'événement ou du flux.	lorsque le flux source ou le contenu cible contient cette ligne (this string)	this string - Indiquez la ligne du texte que vous souhaitez inclure dans le test.

Tableau A-24 Règles communes : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
Context	<p>Le contexte est la relation entre la source et la cible de l'événement ou le flux. Par exemple, une source locale vers une destination distante.</p> <p>Validez si le contexte et l'un des suivants :</p> <ul style="list-style-type: none"> Local to Local Local to Remote Remote to Local Remote to Remote 	lorsque le contexte est ce contexte (this context)	<p>this context - Indique le contexte que ce test doit prendre en considération. Les options sont :</p> <ul style="list-style-type: none"> Local to Local Local to Remote Remote to Local Remote to Remote
Source Location	Validez lorsque la source est soit locale ou distante.	lorsque la source est locale ou distante {par défaut : distante}{ remote {default: Remote }	local remote - Indiquez si vous souhaitez que la source soit locale ou distante. La valeur par défaut est distante (remote)
Destination Location	Validez lorsque l'adresse IP cible du flux ou de l'événement est locale ou distante.	Lorsque la destination est locale ou distante {par défaut : distante }	local remote - Indiquez le trafic local ou distant.
Regex	<p>Validez lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé avec une ligne d'expressions régulières particulières</p> <p>Remarque : <i>Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez des modèles d'expressions régulières, choisissez des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez consulter les didacticiels des expressions régulières disponibles sur le Web.</i></p>	lorsque le nom d'utilisateur (username) correspond à l'expression régulière suivante (regex)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> hostname source hostname destination hostname source payload destination payload - Indiquez la valeur que vous souhaitez associer avec ce test. La valeur par défaut est username. regex - Indiquez la ligne de l'expression régulière que ce test doit prendre en considération.

Tableau A-24 Règles communes : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
IPv6	Validez lorsque l'adresse IPv6 de destination ou source correspond à l'adresse IP configurée.	lorsque l'adresse IP source (v6)((v6)source IP) fait partie des adresses IPv6 (IPv6) suivantes	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP(v6) destination IP(v6) - Indiquez si vous souhaitez que ce test considère l'adresse IPv6 source ou de destination. • IP(v6) addresses - Indiquez les adresses IPv6 que ce test doit prendre en considération.
Reference Set	Validez lorsque l'une ou toutes les propriétés du flux ou de l'événement sont comprises dans l'un ou tous les ensembles de références configurés.	Lorsque l'une (any) des propriétés de ces propriétés (these properties) sont comprises dans l'une de ces ensemble de référence (any of these reference set(s))	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez si vous souhaitez que ce test considère une ou toutes les propriétés d'événement configuré. • these properties - Indiquez les propriétés d'événement ou de flux que ce test doit prendre en considération. • any all - Indiquez si vous souhaitez que ce test considère l'un(any) ou tous (all)les ensembles de référence configurés. • these reference set(s) - Indiquez les ensembles de référence que ce test doit prendre en considération.
CVSS Risk (Host)	Validez lorsque l'hôte spécifié possède une valeur du risque CVSS qui correspond à la valeur configurée.	lorsque l'hôte de destination possède une valeur de risque CVSS supérieure à cette valeur	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source destination either - Indiquez si le test prend en considération l'hôte source ou de destination du flux. • greater than less than equal to - Indiquez si vous souhaitez que la valeur du risque CVSS est supérieure, inférieure ou égale à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.

Tableau A-24 Règles communes : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
CVSS Risk (Port)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque le port de destination possède une valeur de risque CVSS supérieure à cette valeur	<ul style="list-style-type: none"> • source destination either - Indiquez si le test prend en considération le port source ou de destination du flux. • greater than less than equal to - Indiquez si vous souhaitez que le niveau de menace soit supérieur, inférieur ou égal à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0.
Search Filter	Validez lorsque l'événement ou le flux correspond au filtre de la recherche spécifiée.	lorsque l'événement ou le flux correspond à ce filtre de recherche (this search filter)	this search filter - Indiquez le filtre de recherche que ce test doit prendre en considération.
Regex	Validez lorsque la propriété configurée est associée avec une ligne des expressions régulières particulières (regex). <i>Remarque : Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez des modèles d'expressions régulières, choisissez des règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez consulter les didacticiels des expressions régulières disponibles sur le Web.</i>	lorsque ces propriétés (these properties) correspondent à l'expression régulière suivante	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these properties - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événement et de flux normalisées et personnalisées. • regex - Indiquez la ligne de l'expression régulière que ce test doit prendre en considération.
Custom Rule Engines	Validez l'événement ou le flux est traité par les moteurs de règle personnalisé spécifié.	lorsque l'événement ou le flux est traité par l'un de ces (these) moteurs de règle personnalisé	these - Indiquez le paramètre Custom Rule Engine que ce test doit prendre en considération.

Tableau A-24 Règles communes : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
Hexadecimal	Validez lorsque la propriété configurée est associée avec une valeur hexadécimale.	lorsque l'une de ces propriétés (these properties) comprend l'une de ces valeurs hexadécimales (these hexadecimal values)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these properties - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événement et de flux normalisées et personnalisées. • these hexadecimal values - Indiquez les valeurs hexadécimales que ce test doit prendre en considération.

Fonctions - Tests de séquence

Les fonctions - les tests de séquence comprennent :

Tableau A-25 Commun: Fonctions - Groupe de séquence

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Event Function	Vous permet d'utiliser les blocs de construction ou d'autres règles pour effectuer ce test. Cette fonction vous permet de détecter une séquence spécifique des règles sélectionnées relatives à la source et à la destination au sein d'une période de temps configurée.	lorsque toutes ces règles, in in any commencent de the same any source IP à the same any destination IP , sur this many seconds	Configurez les paramètres suivants : <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si ce test doit prendre en considération dans ou dans n'importe quel ordre. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source configurée. • 1 source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source destination. • destination IP destination port - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est destination IP. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est seconds.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Event Function	Vous permet d'utiliser les blocs de construction ou d'autres règles pour effectuer ce test. Vous pouvez utiliser cette fonction pour détecter un nombre de règles spécifiées, en séquence, concernant une source ou une destination au sein d'un intervalle de temps configuré.	lorsqu'au moins ce nombre (this number) de ces règles (rules), dans cette ordre n'importe quel ordre (in in any order), à partir de la même n'importe quelle adresse IP source (the same any source IP) vers la même n'importe quelle adresse IP de destination (the same any destination IP) sur autant de secondes (this many seconds)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this number - Indiquez le nombre de règles que cette fonction doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • in in any - Indiquez si ce test doit prendre en considération dans ou dans n'importe quel ordre. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source configurée. • 1source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • the same any - Indiquez si vous souhaitez que ce test considère certaines ou n'importe quelle source destination. • destination IP destination port - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est destination IP. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est seconds.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Event Sequence Function Between Hosts	Vous permet de détecter une séquence des règles sélectionnées concernant les mêmes hôtes source et de destination dans l'intervalle de temps configuré. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour effectuer ce test.	lorsque cette séquence de rules , concernant le même hôte source et de destination dans ce many seconds	Configurez les paramètres suivants : <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalle que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est seconds.
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et les différentes propriétés d'événement au sein de l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times) dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent.	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter un nombre configuré de règles spécifiques avec les mêmes propriétés d'événement qui se produisent dans l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent à au moins autant de fois (this many times) avec les mêmes propriétés d'événement (event properties) dans autant de minutes (this many minutes) une fois ces règles correspondent (after these rules)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées avec les mêmes et les différentes propriétés d'événement produisent dans un intervalle de temps configuré après une série de règles spécifiques.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times) avec les mêmes propriétés d'événement (event properties) et des propriétés d'événement différents (event properties) dans autant de minutes (this many minutes) après que ces règles(these rules) correspondent	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées dans un intervalle de temps configuré et une fois que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événement.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times in this many minutes) après que ces (these rules) correspondent avec les mêmes propriétés d'événements (event properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées avec les mêmes propriétés d'événement dans un intervalle de temps configuré après que les séries des règles spécifiques produisent avec les mêmes propriétés d'événement.	Lorsque ces règles (these rules) correspondent à au moins (this many) fois avec les mêmes propriétés d'événement (event properties) autant de minutes (this many minutes) une fois que ces règles (these rules) correspondent avec les mêmes propriétés d'événement (event properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des règles spécifiques qui se produisent à plusieurs reprises configurées dans un intervalle de temps après que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événement.	Lorsque ces règles (these rules) correspondent à au moins autant de (this many) fois avec les mêmes propriétés d'événement (event properties) et des propriétés d'événement différentes (event properties) dans this many minutes after these rules match les mêmes propriétés d'événement (event properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des événements spécifiques qui se produisent avec les mêmes et les différentes propriétés d'événement dans un intervalle de temps après que des séries de règles spécifiques se produisent.	lorsqu'au moins autant de (this many) événements sont affichés avec les mêmes propriétés d'événement (event properties) et des propriétés d'événement (event properties) différentes dans autant de minutes (this many minutes) une fois ces règles (these rules) correspondent	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des événements spécifiques qui se produisent avec les mêmes propriétés d'événement dans un intervalle de temps et une fois que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événement.	lorsqu'au moins autant de (this many) événements sont affichés avec les mêmes propriétés d'événement (event properties) dans autant de minutes (this many minutes) après que ces règles (these rules) correspondent avec les mêmes propriétés d'événement (event properties)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tableau A-25 Commun: Fonctions - Groupe de séquence (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter des événements spécifiques qui se produisent avec les mêmes et les différentes propriétés d'événement dans un intervalle de temps et une fois que des séries de règles spécifiques se produisent avec les mêmes propriétés d'événement.	Lorsqu'au moins autant (this many) d'événements sont affichés avec les mêmes propriétés d'événement (event properties) et des propriétés d'événement différentes (event properties) dans autant (this many) de fois ces règles (these rules) correspondent avec les mêmes propriétés d'événement (event properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Fonction : tests de compteur La fonction - les tests de compteur comprennent :

Tableau A-26 Règles communes: Fonctions - Counter Test Group

Test	Description	Nom du test par défaut	Paramètres
Multi-Event Counter Function	Vous permet de tester le nombre d'événement ou de flux à partir des conditions configurées, telles que, l'adresse IP source. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour effectuer ce test.	Lorsqu'une adresse IP (source IP) correspond à plus de exactement (more than exactly) autant de règles (of these rules) via plus de exactement (across more than exactly) this many destination IP, over this tant de minutes many minutes	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • 1 source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • more than exactly - Indiquez si vous souhaitez que ce test considère exactement le nombre de règle ou plus. • this many - Indiquez le nombre de règles que ce test doit prendre en considération. • rules - Indiquez les règles que ce test doit prendre en considération. • more than exactly - Indiquez si vous souhaitez que ce test considère le nombre exacte d'adresses IP de destination, de ports de destination, de QID, d'ID d'événement source ou de sources log que vous sélectionnez dans la source précédente. • this many - Indiquez le nombre d'adresse IP, de ports, de QID, d'événements, de source de journal ou des catégories que ce test doit prendre en considération. • username destination IP source IP source port destination port QID event ID log sources category - Indiquez la destination que ce test doit prendre en considération. La valeur par défaut est destination IP. • this many - Indiquez le temps de la valeur que vous souhaitez affecter à ce test. • seconds minutes hours days - Indiquez l'intervalle de temps que cette règle doit prendre en considération. La valeur par défaut est minutes.

Tableau A-26 Règles communes: Fonctions - Counter Test Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Function	Vous permet de détecter une série de règles pour une adresse IP spécifique par des séries de règles spécifiques pour une adresse IP ou un port spécifique. Vous pouvez également utiliser les blocs de construction ou des règles existantes pour effectuer ce test.	Lorsqu'une de ces règles (rules) avec la même adresse IP source (source IP) plus d'autant de fois (this many) times, via le nombre exacte ou plus d'adresse IP de destination (more than exactly this many destination IP) dans autant de minutes (this many minutes)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • rules - Indiquez les règles que ce test doit prendre en considération. • 1 source IP source port destination IP destination port QID category - Indiquez la source que ce test doit prendre en considération. La valeur par défaut est source IP. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • more than exactly - Indiquez si vous souhaitez que ce test considère le nombre exacte d'adresses IP de destination, de ports de destination, de QID, d'ID d'événement source ou de sources log que vous sélectionnez dans la source précédente. • this many - Indiquez le nombre que ce test doit prendre en considération selon l'option configurée dans le paramètre IP source. • username destination IP source IP source port destination port QID event ID log sources category - Indiquez la destination que ce test doit prendre en considération. La valeur par défaut est destination IP. • this many - Indiquez l'intervalle de temps que vous souhaitez affecter à ce test. • seconds minutes hours days - Indiquez l'intervalle de temps que cette règle doit prendre en considération. La valeur par défaut est minutes.

Tableau A-26 Règles communes: Fonctions - Counter Test Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	<p>Vous permet de détecter des séries d'événements avec les mêmes propriétés d'événement dans l'intervalle de temps configuré.</p> <p>Par exemple, si vous pouvez utiliser ce test lors 100 événements avec la même adresse IP source se produisent dans 5 minutes.</p>	<p>Lorsque au moins autant d'événements (this many events) sont affichés avec les mêmes propriétés (event properties) dans autant de minutes (this many minutes)</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.
Event Property Function	<p>1Allows you to detect a series of events with the same event properties and different event properties within the configured time interval.</p> <p>Par exemple, si vous pouvez utiliser ce test pour détecter lorsque 100 événements avec la même adresse IP source et une adresse IP de destination différente se produisent dans 5 minutes.</p>	<p>Lorsqu'au moins autant d'événements (this many) sont affichés avec les mêmes propriétés d'événements (event properties) et des propriétés d'événements différentes (event properties) dans autant de minutes (this many minutes)</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this many - Indiquez le nombre d'événements que ce test doit prendre en considération. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Tableau A-26 Règles communes: Fonctions - Counter Test Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet de détecter un nombre configuré de règles spécifiques avec les mêmes propriétés d'événement qui se produisent dans l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times in) dans autant de minutes this many minutes	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.
Event Property Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes propriétés d'événement dans l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times) avec les mêmes propriétés de flux (event properties) dans autant de minutes (this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Tableau A-26 Règles communes: Fonctions - Counter Test Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et les différentes propriétés d'événement au sein de l'intervalle de temps configuré.	Lorsque ces règles (these rules) correspondent au moins à autant de fois (this many times) avec les mêmes propriétés d'événements (event properties) et des propriétés d'événement différentes (event properties) dans autant de minutes (this many minutes)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • these event properties - Indiquez les propriétés d'événement que ce test doit prendre en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes.

Fonction : Tests simple La fonction - les tests simple :

Tableau A-27 Règles communes: Fonctions - Simple Test Group

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Event Function	Vous permet d'utiliser les blocs de construction sauvegardés ou d'autres règles pour effectuer ce test. L'événement doit correspondre à toutes ou l'une des règles sélectionnées. Si vous souhaitez créer une instruction OR pour le test de cette règle, spécifiez le paramètre any .	Lorsqu'un flux ou un événement correspond à une ou toutes (any all) les règles suivantes (rules)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez soit l'une (any) ou toutes (all) les règles configurées qui devraient s'appliquer à ce test. • rules - Indiquez les règles que ce test doit prendre en considération.

Données/Tests de temps

Les données et les tests de temps comprennent :

Tableau A-28 Règle commune : Tests Date/Heure

Test	Description	Nom du test par défaut	Paramètres
Jour d'événement / flux	Validez lorsque l'événement ou le flux se produit sur les jours du mois configurés.	Lorsque les flux ou les événements se produisent sur le jour du mois sélectionné	Configurez les paramètres suivants : <ul style="list-style-type: none"> • on after before - Indiquez si vous souhaitez que ce test considère avant, après ou à la date configurée. La valeur par défaut est on IP. • selected - Indiquez le jour du mois que ce test doit prendre en considération.
Semaine d'événement / flux	Validez lorsque l'événement ou le flux se produit sur les jours de la semaine configurés.	Lorsque les flux ou les événements se produisent dans l'un de ces jours de la semaine	these days of the week - Indiquez les jours de la semaine que ce test doit prendre en considération.
Heure d'Événement/Flux	Validez lorsque l'événement ou le flux se produit dans, après ou avant l'heure configurée.	Lorsque les flux ou les événements se produisent après ce temps	Configurez les paramètres suivants : <ul style="list-style-type: none"> • after before at - Indiquez si ce test doit prendre en considération avant, après ou à la date configurée. La valeur par défaut est after IP. • this time - Indiquez l'heure que ce test doit prendre en considération.

Tests de propriété de réseau

Le test de la propriété du réseau comprend :

Tableau A-29 Règles commune : Tests de propriété du réseau

Test	Description	Nom du test par défaut	Paramètres
Local Network Object	Validez lorsque l'événement se produit dans le réseau spécifié.	lorsque le réseau local est one of the following	one of the following networks - Indiquez les zones des réseaux sur lesquelles vous souhaitez appliquer les tests.

Tableau A-29 Règles commune : Tests de propriété du réseau (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux distants.	lorsque source IP fait partie de l'un des emplacements de réseaux distants suivants	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • remote network locations - Indiquez les emplacements de réseau que souhaitez que le test considère.
Remote Services Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux des services distants configurés.	lorsque l'adresse IP fait partie de l'un de remote services network locations	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • remote services network locations - Indiquez les emplacements de réseau de services distants que le test doit prendre en considération.
Geographic Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements des réseaux géographiques configurés.	lorsque Source IP fait partie de l'un des emplacements géographiques de réseaux	Configurez les paramètres suivants : <ul style="list-style-type: none"> • source IP destination IP any IP - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • geographic network locations - Indiquez les emplacements de réseau que souhaitez que le test considère.

Tests négatifs de fonctions

Les tests négatifs de fonction comprennent :

Tableau A-30 Règles communes: Fonctions - Negative Test Group

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter des règles spécifiques qui se produisent dans un intervalle de temps configuré après que des séries de règles spécifiques se produisent avec les mêmes propriétés de flux.	Lorsqu'aucune de ces règles (these rules) ne correspond dans autant de minutes this many minutes) après que ces règles (these rules) correspondent avec les mêmes propriétés de flux (flow properties)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these - Indiquez les règles que ce test doit prendre en considération. • flow properties - Specify the flow properties you want this test to consider. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.
Rule Function	Vous permet de détecter lorsqu'aucune de ces règles spécifiées ne se produisent dans un intervalle de temps configuré après que des séries de règles se sont produites.	Lorsqu'aucune de ces règles (these rules) ne correspondent dans autant de minutes (this many minutes) après ces règles (these rules) correspondent	Configurez les paramètres suivants : <ul style="list-style-type: none"> • these rules - Indiquez les règles que ce test doit prendre en considération. • this many - Indiquez le nombre d'intervalles que ce test doit prendre en considération. • seconds minutes hours days - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est minutes. • these rules - Indiquez les règles que ce test doit prendre en considération.

Tests de règle de violation

Cette section fournit des informations sur les tests que vous pouvez appliquer aux règles de violation notamment :

- [Tests IP/Port](#)
- [Test de fonction](#)

- **Données/Tests de temps**
- **Tests de la source du journal**
- **Tests de propriété de violation**

Tests IP/Port Les tests IP/Port comprennent :

Tableau A-31 Règles de violation : Groupe de test IP/Port

Test	Description	Nom du test par défaut	Paramètres
Offense Index	Validez lorsque l'adresse IP source est l'une des adresses IP configurées.	lorsque la violation est indexée par l'une des adresses IP (IP addresses) suivantes.	IP addresses - Indiquez les adresses IP que ce test doit prendre en considération. Vous pouvez saisir plusieurs entrées à l'aide d'une liste séparée par des virgules.
Destination IP Address	Validez lorsque la liste cible est l'une des adresses IP configurées.	lorsque la liste cible comprend l'une (any) des adresses IP (IP addresses) suivantes	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez si vous souhaitez que ce test considère l'une (any) ou toutes (all) les destinations listées. La valeur par défaut est any. • IP addresses - Indiquez les adresses IP que ce test doit prendre en considération. Vous pouvez saisir plusieurs entrées à l'aide d'une liste séparée par des virgules.

Test de fonction Les tests de fonction comprennent :

Tableau A-32 Règles de violation : Groupe de fonctions des violations

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Offense Function	Vous permet d'utiliser les blocs de construction sauvegardés ou d'autres règles pour effectuer ce test. La violation doit correspondre à toutes ou l'une des règles sélectionnées. Si vous souhaitez créer une instruction OR pour le test de cette règle, spécifiez le paramètre any .	lorsque la violation correspond à l'une (any) des règles de violation (offense rules) suivantes.	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez soit l'une (any) ou toutes (all) les règles configurées qui devraient s'appliquer à ce test. La valeur par défaut est any. • offense rules - Indiquez les règles que ce test doit prendre en considération.

Données/Tests de temps Les données et les tests de temps comprennent :

Tableau A-33 Règles de violation : Tests Date/Heure

Test	Description	Nom du test par défaut	Paramètres
Offense Day	Validez lorsque la violation se produit au jour configuré du mois.	Lorsque la (les) violation(s) se produit sur (on) le jour sélectionné (selected) du mois	Configurez les paramètres suivants : <ul style="list-style-type: none"> • on after before - Indiquez si vous souhaitez que cette règle considère dans, avant ou après la date sélectionnée. La valeur par défaut est on IP. • selected - Indiquez la date que ce test doit prendre en considération.
Offense Week	Validez lorsque la violation se produit au jour configuré de la semaine.	lorsque la (les) violation(s) se produit sur (on) ces jours de la semaine	Configurez les paramètres suivants : <ul style="list-style-type: none"> • on after before - Indiquez si vous souhaitez que cette règle considère sur, avant ou après le jour sélectionné. La valeur par défaut est on IP. • these days of the week - Indiquez les jours que ce test doit prendre en considération.
Offense Time	Validez lorsque la violation se produit avant, après ou sur l'heure configurées.	lorsque la (les) violation(s) se produit avant cette heure (after this time)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • on after before - Indiquez si vous souhaitez que ce test considère avant, après ou à l'heure spécifiée. La valeur par défaut est after IP. • this time - Indiquez l'heure que ce test doit prendre en considération.

Tests de la source du journal

Les tests de la source du journal comprennent :

Tableau A-34 Règles de violation : Tests de la source du journal

Test	Description	Nom du test par défaut	Paramètres
Log Source Types	Validez lorsque la source du journal configuré est la source de la violation.	lorsque le (les) type(s) qui a détecté la violation est l'un des types de la source du journal (log source types) suivants	log source types - Indiquez les types de la source du journal que vous souhaitez que ce test détecte.
Number of Log Source Type	Validez lorsque le nombre des types de source du journal est supérieur à la valeur configurée.	lorsque le nombre des types de source du journal qui a détecté la violation est supérieur à ce nombre (greater than this number)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than equal to - Indiquez si vous souhaitez que le niveau de menace devienne supérieur ou égal à la valeur configurée. • this number - Indiquez le nombre des types de la source du journal que ce test doit prendre en considération.

Tests de propriété de violation

Les tests de propriété de violation comprennent :

Tableau A-35 Règles de violation : Tests des propriétés de violation

Test	Description	Nom du test par défaut	Paramètres
Network Object	Validez lorsque le réseau est affecté par tous ou l'un (any or all) des réseaux configurés.	lorsque le réseau affecté est l'un (any) des réseaux suivants (the following networks)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • any all - Indiquez si vous souhaitez que ce test considère l'un (any) ou tous (all) les réseaux. La valeur par défaut est any. • the following networks - Indiquez les réseaux que ce test doit prendre en considération.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Offense Category	Validez lorsque la catégorie de l'événement est l'une ou toutes les catégories de l'événement configuré.	lorsque les catégories des violations incluent l'une (any) des catégories de liste (list of categories) suivantes	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • any all - Indiquez si vous souhaitez que ce test considère l'une (any) ou toutes (all) les catégories. La valeur par défaut est any. • list of categories - Indiquez les catégories que vous souhaitez que ce test considère. <p>Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>
Severity	Validez lorsque la gravité est supérieure, inférieure ou égale aux valeurs configurées.	lorsque la gravité de violation est supérieure à 5 (par défaut) (greater than 5 {default})	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si vous souhaitez que la gravité de violation soit supérieure, inférieure ou égale à la valeur configurée. • 5 - Indiquez la valeur que vous souhaitez que le test considère. La valeur par défaut est 5.
Credibility	Validez lorsque la crédibilité est supérieure, inférieure ou égale à la valeur configurée.	lorsque la crédibilité de violation est supérieure à 5 (greater than 5) (par défaut)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si vous souhaitez que la crédibilité de violation soit supérieure, inférieure ou égale à la valeur configurée. • 5 - Indiquez la valeur que vous souhaitez que le test considère.
Relevance	Validez lorsque la pertinence est supérieure, inférieure ou égale à la valeur configurée.	lorsque la pertinence de violation est supérieure à 5 (greater than 5) (par défaut)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si vous souhaitez que la pertinence de violation soit supérieure, inférieure ou égale à la valeur configurée. • 5 - Indiquez la valeur que vous souhaitez que le test considère.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Offense Context	<p>Le contexte de violation est la relation entre la source et la cible de la violation. Par exemple, un agresseur informatique local vers une cible distante.</p> <p>Validez si le contexte de violation est l'un des suivants :</p> <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote 	lorsque le contexte de violation est ce contexte (this context)	<p>this context - Indique le contexte que ce test doit prendre en considération. Les options sont :</p> <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Validez lorsque la source est soit locale ou distante.	lorsque la source est locale ou distante (local or remote) {Par défaut : remote }	local remote - Indiquez si vous souhaitez que la source soit locale ou distante. La valeur par défaut est remote IP .
Destination Location	Validez lorsque la cible est soit locale ou distante.	lorsque la liste cible comprend des adresses IP locales ou distantes (par défaut : remote) (local or remote IP addresses {default: remote })	locate IPs remote IPs - Indiquez si vous souhaitez que la cible devienne locale ou distante. La valeur par défaut remote IPs .
Destination Count in an Offense	Validez lorsque le nombre des cibles pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre des cibles sous attaque est supérieur à ce nombre (greater than this number)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • greater than equal to - Indiquez si vous souhaitez que le nombre des cibles soit supérieur ou égal à la valeur configurée. • this number - Indiquez la valeur que ce test doit prendre en considération.
Event Count in an Offense	Validez lorsque le nombre des événements pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre des événements qui composent la violation est supérieur à ce nombre (greater than this number)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si vous souhaitez que le comptage d'événement est supérieur, inférieur ou égal à la valeur configurée. • this number - Indiquez la valeur que ce test doit prendre en considération.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Count in an Offense	Validez lorsque le nombre des flux pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre des flux qui composent la violation est supérieur à ce nombre (greater than this number)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si vous souhaitez que le comptage de flux est supérieur, inférieur ou égal à la valeur configurée. • this number - Indiquez la valeur que ce test doit prendre en considération.
Total Count in an Offense	Validez lorsque le nombre total des événements et des flux pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre des événements et flux composent la violation est supérieur à ce nombre (greater than this number)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than less than equal to - Indiquez si vous souhaitez que le comptage d'événement et de flux est supérieur, inférieur ou égal à la valeur configurée. • this number - Indiquez la valeur que ce test doit prendre en considération.
Category Count in an Offense	Validez lorsque le nombre des catégories d'événement pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre des catégories impliquées dans la violation est supérieur à ce nombre (greater than this number)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • greater than equal to - Indiquez si vous souhaitez que le nombre des catégories est supérieur ou égal à la valeur configurée. • this number - Indiquez la valeur que ce test doit prendre en considération. <p>Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration <i>IBM Security QRadar Network Anomaly Detection</i>.</p>
Offense ID	Validez lorsque l'ID de violation est la valeur configurée.	lorsque l'ID de violation est cet ID (this ID)	this ID - Indiquez l'ID de violation que ce test doit prendre en considération.
Offense Creation	Validez lorsqu'une nouvelle violation est créée.	lorsqu'une nouvelle violation est créée	

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Offense Change	Validez lorsque la propriété de la violation configurée a augmenté au-dessus de la valeur configurée.	lorsque la propriété de la violation (offense property) a augmenté par au moins ce pourcentage (this percent)	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • Magnitude Severity Credibility Relevance Destination count Source count Category count Annotation count Event count - Indiquez la propriété que ce test doit prendre en considération. La valeur par défaut Magnitude. • this - Indiquez le pourcentage Specify the percent or unit value you want this test to consider. • percent unit(s) - Indiquez si vous souhaitez que ce test considère le pourcentage ou les unités.

Tests de règle de détection d'anomalie

Cette section fournit des informations sur les tests que vous pouvez appliquer aux règles de détection d'anomalie notamment :

- [Test de règles d'anomalie](#)
- [Test de règle de comportement](#)
- [Tests de règle de seuil](#)

Test de règles d'anomalie

Cette section fournit des informations sur les tests de règle d'événement que vous pouvez appliquer aux règles notamment :

- [Tests d'anomalie](#)
- [Tests de seuil de temps](#)

Tests d'anomalie

Le groupe de test d'anomalie comprend :

Tableau A-36 Règles d'anomalie : Tests d'anomalie

Test	Description	Nom du test par défaut	Paramètres
Anomaly	<p>Validez lorsque la propriété accumulée a augmenté ou diminué selon le pourcentage spécifié pendant une courte période de temps lorsque comparée à la plus grande période spécifiée.</p> <p>Par exemple, si votre moyenne d'octets cible pour les 24 dernières heures est de 100.000.000 octets pour chaque minute, puis au cours d'une période de 5 minutes, les octets en moyenne augmentent de 40%, ce test est valide.</p> <p>Remarque : L'accumulateur envoie des données au moteur de règle de détection d'anomalie à intervalles d'une minute. Pour plus d'information sur l'accumulateur, consultez le guide d'administration IBM Security QRadar Network Anomaly Detection.</p>	<p>Lorsque la valeur moyenne (par intervalle) de cette propriété accumulée (this accumulated property) au cours de la dernière minute (1 min) est au moins un pourcentage % (percentage) différent de la valeur moyenne (par intervalle de la même propriété au cours de la dernière minute (1 min))</p>	<p>Configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • this accumulated property - Indiquez la propriété accumulée que ce test doit prendre en considération. • 1 min - Indiquez l'intervalle de temps que ce test doit prendre en considération. La valeur par défaut est 1 min. • 40 - Indiquez le pourcentage que ce test doit prendre en considération. Le pourcentage par défaut est 40. • 1 min - Indiquez l'intervalle de temps qu'utilise ce test pour comparer la durée de l'intervalle. L'intervalle par défaut est 1 min.
Minimum Value	<p>Validez lorsque la valeur testée pour l'intervalle accumulé dépasse la valeur configurée.</p>	<p>lorsque les intervalles d'accumulation sont uniquement considérés si la valeur testée pour cet intervalle dépasse certaines valeurs (some value)</p>	<p>some value - Indiquez la valeur que vous souhaitez considérée pour l'intervalle d'accumulation configuré.</p>

Tests de seuil de temps

Le groupe de tests de seuil de temps comprend :

Tableau A-37 Règles d'anomalie : Tests de seuil de temps

Test	Description	Nom du test par défaut	Paramètres
Date Range	Validez lorsqu'une activité anormale est détectée dans la plage de dates spécifiée.	lorsque la date est entre cette date (this date) et cette date (this date)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this date - Indiquez la date de début de votre plage de dates. • this date - Specify the end date for your date range.
Day of the Week	Validez lorsqu'une activité anormale est détectée dans un jour spécifié de la semaine.	lorsque le jour de la semaine est l'un des jours sélectionné (these selected days)	these selected days - Indiquez les jours que ce test doit prendre en considération.
Time Range	Validez lorsqu'une activité anormale est détectée dans la plage de temps spécifiée.	lorsque l'heure du jour est entre cette heure (this time) et cette heure (this time)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this time - Indiquez le temps de début de votre plage de dates. • this time - Indiquez la date de fin de votre plage de dates.

Test de règle de comportement

Cette section fournit des informations sur les tests de règle de comportement que vous pouvez appliquer aux règles notamment :

- [Tests de comportement](#)
- [Tests de seuil de temps](#)

Tests de comportement

Le groupe de tests de comportement comprend :

Tableau A-38 Règles de comportement : Tests de comportement

Test	Description	Nom du test par défaut	Paramètres
Propriétés accumulées	Indique la propriété accumulée considérée par cette règle.	Lorsque cette propriété accumulée est la propriété testée	this accumulated property - Indiquez la propriété accumulée que ce test doit prendre en considération.
Current Traffic Level	Validez lorsque le niveau du trafic courant représente un changement saisonnier spécifié dans des données la plage de temps spécifiée dans cette durée de test de saison. Par exemple, le test de niveau de trafic courant peut comparer les données en cours avec les données de la même plage de temps qu'hier.	Lorsque l'importance du niveau de trafic en cours (sur une échelle de 0 à 100) est l'importance comparée au comportement et aux tendances du trafic étudié	70 - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que ce test doit prendre en considération. La valeur par défaut est 70 .

Tableau A-38 Règles de comportement : Tests de comportement (suite)

Test	Description	Nom du test par défaut	Paramètres
Current Traffic Trend	<p>Validez lorsque la tendance du trafic représente un effet saisonnier spécifique dans les données pour chaque intervalle de temps.</p> <p>Par exemple, la tendance de trafic en cours peut tester lorsque les données augmente le même amount increases the same amount from week 2 to week 3 as it did from week 1 to week 2.</p>	<p>Lorsque l'importance de la tendance du trafic en cours (sur une échelle de 0 à 100) est l'importance comparée au comportement et aux tendances du trafic étudié</p>	<p>30 - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que ce test doit prendre en considération. Le pourcentage par défaut est 30.</p>
Current Traffic Behavior	<p>Validez lorsque le comportement du trafic change dans les données pour chaque intervalle de temps.</p> <p>Par exemple, le test de trafic en cours peut tester pour que les données changent lors de la comparaison de cette minute à la minute précédente.</p>	<p>Lorsque l'importance du niveau de trafic en cours (sur une échelle de 0 à 100) est l'importance comparée au comportement et aux tendances du trafic étudié</p>	<p>30 - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que ce test doit prendre en considération. Le pourcentage par défaut est 30.</p>
Deviation	<p>Validez lorsque la propriété accumulée s'écarte du modèle du trafic prévu.</p>	<p>Lorsque la valeur de la zone actuelle s'écarte avec une marge d'au moins dérivation (deviation%) de l'extrapolé (valeur de la zone prévue).</p>	<p>50 - Indiquez le pourcentage de déviation que ce test doit prendre en considération. La valeur par défaut est 50.</p>
Season Length	<p>Validez lorsque la durée de la saison représente l'intervalle de temps que vous souhaitez tester.</p> <p>Typiquement, pour le trafic de réseau, vous pouvez définir la durée de la saison sur semaine. Lors du contrôle du trafic à partir des systèmes automatisés, nous recommandons de définir la durée de la saison sur un jour.</p>	<p>Lorsque la durée de la saison est un jour</p>	<p>a day a week a month - Indiquez la durée de la saison que ce test doit prendre en considération.</p>

Tableau A-38 Règles de comportement : Tests de comportement (suite)

Test	Description	Nom du test par défaut	Paramètres
Minimum Value	Validez lorsque la valeur testée pour l'intervalle accumulé dépasse la valeur configurée.	lorsque les intervalles d'accumulation sont uniquement considérés si la valeur testée pour cet intervalle dépasse certaine valeurs (0 value)	0 - Indiquez la valeur que vous souhaitez considérer pour l'intervalle d'accumulation configuré.

Tests de seuil de temps

Le groupe de tests de seuil de temps comprend :

Tableau A-39 Règles d'anomalie : Tests de seuil de temps

Test	Description	Nom du test par défaut	Paramètres
Date Range	Validez lorsqu'une activité anormale est détectée dans la plage de dates spécifiée.	lorsque la date est entre cette date (this date) et cette date (this date)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this date - Indiquez la date de début de votre plage de dates. • this date - Specify the end date for your date range.
Day of the Week	Validez lorsqu'une activité anormale est détectée dans un jour spécifié de la semaine.	lorsque le jour de la semaine est l'un des jours sélectionné (these selected days)	these selected days - Indiquez les jours que ce test doit prendre en considération.
Time Range	Validez lorsqu'une activité anormale est détectée dans la plage de temps spécifiée.	lorsque l'heure du jour est entre cette heure (this time) et cette heure (this time)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this time - Indiquez le temps de début de votre plage de dates. • this time - Indiquez la date de fin de votre plage de dates.

Tests de règle de seuil Cette section fournit des informations sur les tests de règle de seuil que vous pouvez appliquer aux règles notamment :

- [Tests de seuil de zone](#)
- [Tests de seuil de temps](#)

Tests de seuil de zone

Le groupe de tests de seuil de zone comprend :

Tableau A-40 Règles de seuil : Tests de seuil de la zone

Test	Description	Nom du test par défaut	Paramètres
Valeur de seuil	Validez lorsque la gravité est supérieure, inférieure ou égale aux valeurs configurées. Vous pouvez indiquer l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété.	Lorsque cette propriété accumulée (this accumulated property) est supérieur à cette valeur (accumulée dans un intervalle de 1 minute)	<ul style="list-style-type: none"> • this accumulated property - Indiquez la propriété accumulée que ce test doit prendre en considération. • greater than less than equal to - Indiquez si la valeur de la propriété accumulée est supérieure, inférieure ou égale à la valeur configurée. • 0 - Indiquez la valeur que ce test doit prendre en considération. La valeur par défaut est 0. • 1 min - Indiquez l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété. La valeur par défaut est 1 min.
Threshold Range	Validez lorsque la propriété accumulée est dans un intervalle spécifié. Vous pouvez indiquer l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété.	Lorsque cette propriété accumulée (this accumulated property) est entre cette valeur ' this value) et cette valeur (this value)(accumulée dans 1 minute d'intervalle)	<ul style="list-style-type: none"> • this accumulated property - Indiquez la propriété accumulée que ce test doit prendre en considération. • 0 - Indiquez la valeur que ce test doit prendre en considération en tant que début d'intervalle. La valeur par défaut est 0. • 0 - Indiquez la valeur que ce test doit prendre en considération en tant que fin d'intervalle. La valeur par défaut est 0. • 1 min - Indiquez l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété. La valeur par défaut est 1 min.

Tests de seuil de temps

Le groupe de tests de seuil de temps comprend :

Tableau A-41 Règles de seuil : Tests de seuil de l'heure

Test	Description	Nom du test par défaut	Paramètres
Date Range	Validez lorsqu'une activité anormale est détectée dans la plage de dates spécifiée.	lorsque la date est entre cette date (this date) et cette date (this date)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this date - Indiquez la date de début de votre plage de dates. • this date - Specify the end date for your date range.

Tableau A-41 Règles de seuil : Tests de seuil de l'heure (suite)

Test	Description	Nom du test par défaut	Paramètres
Day of the Week	Validez lorsqu'une activité anormale est détectée dans un jour spécifié de la semaine.	lorsque le jour de la semaine est l'un des jours sélectionné (these selected days)	these selected days - Indiquez les jours que ce test doit prendre en considération.
Time Range	Validez lorsqu'une activité anormale est détectée dans la plage de temps spécifiée.	lorsque l'heure du jour est entre cette heure (this time) et cette heure (this time)	Configurez les paramètres suivants : <ul style="list-style-type: none"> • this time - Indiquez le temps de début de votre plage de dates. • this time - Indiquez la date de fin de votre plage de dates.

B

GLOSSAIRE

accumulateur	L'accumulateur réside sur l'hôte qui contient un processeur d'événements pour aider à l'analyse des flux, des événements, des rapports, à l'écriture des données de bases de données et à l'alerte d'un DSM.
amplitude	Indique l'importance relative de la violation et constitue une valeur pondérée calculée à partir de la pertinence, de la gravité et de la crédibilité. La barre d'amplitude de l'onglet Offenses et le tableau de bord offrent une représentation visuelle de toutes les variables comparées de la violation, de la source, de la destination ou du réseau. L'amplitude d'une violation est déterminée par plusieurs tests réalisés sur une violation à chaque fois que cette dernière a été planifiée pour une ré-évaluation, en général parce que des événements ont été ajoutés ou que le délai minimal de planification s'est écoulé.
anomalie	Ecart du comportement attendu du réseau.
ARP	Voir Protocole de résolution d'adresse.
ASN	Voir Numéro de système autonome (ASN).
Base de données OSVDB (Open Source Vulnerability Database)	Une base de données OSVDB (Open Source Vulnerability Database) est une base de données open source créée par et pour la communauté de la sécurité du réseau. La base de données fournit des informations techniques sur les vulnérabilités de sécurité réseau.
capture de contenu	QRadar QFlow Collector capture une quantité configurable de contenu et stocke les données dans les journaux de flux. Vous pouvez consulter ces données en utilisant l'onglet Network Activity .
CIDR	Voir Classless Inter-Domain Routing.
Classless Inter-Domain Routing (CIDR)	Schéma d'adressage Internet qui permet d'affecter et de préciser les adresses Internet utilisées dans le routage interne au domaine. Grâce au composant CIDR, une adresse IP unique peut être utilisée pour désigner plusieurs adresses IP uniques.
chiffrement	Le chiffrement offre une plus grande sécurité à l'intégralité du trafic QRadar Network Anomaly Detection entre les hôtes gérés. Lorsque le chiffrement est

activé pour un hôte géré, des tunnels de chiffrement sont créés pour toutes les applications client d'un hôte géré afin de fournir un accès protégé aux serveurs.

Cible hors site	Périphérique hors site qui reçoit des données d'événement ou des données de flux. Une cible hors site ne peut recevoir des données qu'à partir d'un collecteur d'événements.
client	L'hôte qui est à l'origine de la communication.
Collecteur d'événement	Recueille les événements de sécurité et les flux à partir des différents types de périphériques de votre réseau. Le collecteur d'événements rassemble les événements et les flux à partir de sources locales, distant et de périphérique. Le collecteur d'événements normalise ensuite les événements et les flux et envoie les informations au processeur d'événements.
comportement	Indique les conditions normales dans lesquelles le système ou réseau fonctionne.
Console	Interface Web pour QRadar Network Anomaly Detection. QRadar Network Anomaly Detection est accessible depuis un navigateur Web standard (Internet Explorer 7.0/8.0 ou Mozilla Firefox 3.6 et plus). Lorsque vous accédez au système, une invite s'affiche et demande le nom d'utilisateur et un mot de passe, qui doivent être configurés à l'avance par l'administrateur QRadar Network Anomaly Detection.
Conversion d'adresses réseau (NAT)	La conversion d'adresses réseau traduit l'adresse IP dans un réseau en une adresse IP différente dans un autre réseau.
couche réseau	Couche 3 dans l'architecture de l'interconnexion de systèmes ouverts (OSI) ; la couche qui établit un chemin entre des systèmes ouverts.
crédibilité	Indique l'intégrité d'un événement ou d'une violation telle que déterminée par l'évaluation de la crédibilité qui est configurée dans la source du journal. La crédibilité augmente lorsque plusieurs sources signalent le même événement.
destination d'acheminement	QRadar Network Anomaly Detection vous permet de transmettre les données de journal brutes provenant de sources de journal et de données d'événements normalisés QRadar Network Anomaly Detection à un ou plusieurs systèmes de fournisseur, tels que des systèmes de billetterie ou d'alerte. Sur l'interface utilisateur QRadar Network Anomaly Detection, ces systèmes des fournisseurs sont appelés des destinations d'acheminement.
Device Support Module (DSM)	Les modules de support de périphérique (DSMs) vous permettent d'intégrer QRadar Network Anomaly Detection avec des sources de journaux.
Distant-Local (R2L)	Trafic externe entre un réseau distant et un réseau local.
Distant-Distant (R2R)	Trafic externe provenant d'un réseau distant vers un autre réseau distant.

DNS	Voir Domain Name System.
données utiles	Données d'application réelles (excluant les informations d'en-tête ou administratives) contenues dans un flux IP.
Domain Name System (DNS)	Base de données répartie en ligne utilisée pour mapper les noms de machines lisibles par l'homme vers une adresse IP afin de résoudre les noms de machines dans les adresses IP.
données de flux	Caractéristiques d'un flux comprenant : les adresses IP, les ports, le protocole, les octets, la paquets, les balises, la direction, l'ID d'application et les donnée de contenu (facultatif).
DSM	Voir Device Support Module (DSM).
élément	Option du tableau de bord qui crée un portail personnalisé affichant toutes les vues possibles pour le contrôle.
événement	Enregistrement d'un périphérique décrivant une action sur un réseau ou un hôte.
faux positif	Lorsqu'un événement est paramétré sur faux positif, il ne contribue plus aux règles personnalisées, c'est pourquoi les violations ne sont pas générées en fonction de l'événement de faux positif. L'événement reste stocké dans la base de données et contribue à la génération de rapports.
feuilles	Enfants ou objets qui font partie d'un groupe parent.
flux	Session de communication entre deux hôtes. Décrit le mode de communication du trafic, les éléments communiqués (si l'option de capture du contenu a été sélectionnée) et contient des détails tels que quand, qui, combien, les protocoles, les priorités ou les options.
flux double	Lorsqu'un QRadar QFlow Collector détecte le même flux, ce dernier est appelé un flux double. Cependant, dans ce cas, le QRadar QFlow Collector écarte le flux comme un doublon de sorte que le processeur d'événements ne reçoive qu'un seul rapport sur le flux.
Fournisseur d'accès Internet (ISP)	Un Fournisseur d'accès Internet (ISP) fournit aux utilisateurs un accès à Internet et à d'autres services connexes.
FQDN	Voir Nom de domaine complet.
FQNN	Voir Nom de réseau complet.
gravité	Indique la menace que représente une source par rapport au niveau de préparation de la cible contre l'attaque. Cette valeur est mappée vers une catégorie d'événement de la mappe QID qui est comparée à la violation.

Heure système	Dans l'angle droit de l'interface utilisateur s'affiche l'heure du système qui correspond à l'heure de la console QRadar Network Anomaly Detection. C'est l'heure qui détermine l'heure des événements et des violations.
hiérarchie de réseau	Comprend chaque composant de votre réseau et identifie les objets appartenant à d'autres objets. L'exactitude et l'exhaustivité de cette hiérarchie sont des éléments essentiels pour les fonctions d'analyse du trafic. La hiérarchie de réseau permet de stocker les journaux de flux, les bases de données et les fichiers TopN.
Host Context	Surveille tout les composants QRadar Network Anomaly Detection pour s'assurer que chaque composant fonctionne comme prévu.
ICMP	Voir ICMP (Protocole de message de gestion inter-réseau).
identité	QRadar Network Anomaly Detection recueille des informations d'identité, si disponibles, à partir des messages de source de journal. Les informations d'identité fournissent des détails supplémentaires sur les actifs de votre réseau. Les sources de journal génèrent uniquement des informations d'identité si le message de journal envoyé à QRadar Network Anomaly Detection contient une adresse IP et au moins un des éléments suivants : nom d'utilisateur ou adresse MAC. Toutes les sources de journal ne génèrent pas des informations d'identité.
IDS	Voir Système de détection d'intrusion.
indicateurs TCP	Type de marqueur qui peut être ajouté à un paquet pour alerter le système en cas d'activité anormale. Seules quelques combinaisons spécifiques d'indicateurs sont valides et caractéristiques, dans un trafic normal. Des combinaisons anormales d'indicateurs indiquent souvent une attaque ou une condition anormale du réseau.
Interconnexion de systèmes ouverts (OSI)	Cadre général des normes ISO pour la communication entre différents systèmes réalisés par différents fournisseurs, dans lesquels le processus de communication est organisé en sept catégories différentes qui sont placées dans une séquence stratifiée en fonction de leur relation avec l'utilisateur. Chaque couche utilise la couche immédiatement inférieure et fournit un service à la couche au-dessus. Les couches 7 à 4 traitent la communication de bout en bout entre la source et la destination du message, et les couches 3 à 1 se chargent des fonctions réseau.
intervalle	Période par défaut dans le système. Affecte les intervalles de mise à jour des graphiques et la durée contenue dans chaque fichier journal de flux.
intervalle de coalescence	L'intervalle de coalescence (groupage) des événements est de 10 secondes, en commençant par le premier événement qui ne correspond à aucun événement en cours de coalescence. Dans l'intervalle, les trois premiers événements correspondants sont immédiatement publiés dans le processeur d'événements et le quatrième événement et les suivants sont fusionnés afin que le contenu et d'autres caractéristiques ne soient pas inclus dans le quatrième événement. Chaque arrivée d'un événement correspondant pendant l'intervalle incrémente le comptage d'événements du quatrième événement. A la fin de l'intervalle,

l'événement fusionné est publié dans le processeur d'événements et l'intervalle suivant commence pour événements correspondants des. Si aucun événement correspondant n'arrive pendant cet intervalle, le processus redémarre. Dans le cas contraire, la coalescence continue avec tous les événements comptés et publiés selon des intervalles de 10 secondes.

intervalle de rapport	Intervalle de temps configurable selon lequel le processeur d'événement doit envoyer la totalité des événements capturés et des données de flux vers la console.
IP	Voir protocole IP.
IPS	Voir Système de prévention contre les intrusions.
journaux de flux	Enregistrement des flux permettant au système de comprendre le contexte d'une transmission précise via le réseau. Les flux sont stockés dans les journaux de flux.
L2L	Voir Local to Local.
L2R	Voir Local to Remote.
LAN	Voir réseau local.
LDAP	Voir protocole LDAP.
Local to Local (L2L)	Trafic interne d'un réseau local vers un autre réseau local.
Local to Remote (L2R)	Trafic interne d'un réseau local vers un réseau distant.
Magistrate	Fournit les composants de traitement de base de l'option SIEM. Magistrate fournit des rapports, des alertes et une analyse du trafic réseau et des événements de sécurité. Magistrate traite l'événement par rapport aux règles personnalisées définies pour créer une violation.
masque de sous-réseau	Masque de bits qui est combiné de manière logique à l'aide de l'opération ET avec l'adresse IP de destination d'un paquet IP afin de déterminer l'adresse réseau. Un routeur achemine les paquets en utilisant l'adresse réseau.
minuteur d'actualisation	Les onglets Dashboard , Log Activity et Network Activity disposent d'une barre d'état dynamique qui affiche la durée restante avant que QRadar Network Anomaly Detection n'actualise automatiquement les données d'activité du réseau actuel, l'actualisation intégrée peut être effectuée manuellement à tout moment.
multidiffusion IP	La multidiffusion IP réduit le trafic sur un réseau en délivrant un flux unique d'informations à plusieurs utilisateurs en même temps.
NAT	Voir Conversion d'adresses réseau (NAT).

NetFlow	Technologie exclusive de compatibilité développée par Cisco Systems® Inc. qui surveille les flux de trafic à travers un commutateur ou un routeur, interprète le client, le serveur, le protocole et le port utilisé, compte le nombre d'octets et de paquets et envoie ces données à un collecteur NetFlow. Vous pouvez configurer QRadar Network Anomaly Detection pour accepter NDE's et ainsi devenir un collecteur NetFlow.
Nom de domaine complet (FQDN)	Partie d'une adresse URL Internet qui identifie complètement le programme serveur auquel une demande Internet est adressée.
Nom de réseau complet (FQNN)	Chemin d'accès complet d'un point spécifique dans la hiérarchie du réseau. Par exemple, la hiérarchie de la société A contient un objet de service qui contient un objet marketing. Par conséquent, le nom de réseau FQNN est CompanyA.Department.Marketing.
Numéro de système autonome	Un système autonome est un ensemble de tous les réseaux IP qui adhèrent à la même politique de routage spécifique et clairement définie. Un numéro de système autonome (ASN) est un numéro d'identification unique attribué à chaque système autonome.
objets de feuille de base de données	Objets de point final dans une hiérarchie. Au niveau de chaque point dans la hiérarchie au dessus de ce point, se trouve un objet parent qui contient les valeurs agrégées de tous les objets de feuille en dessous.
objets réseau	Composants de la hiérarchie de réseau. Vous pouvez ajouter des couches à la hiérarchie en ajoutant des objets du réseau supplémentaires et en les associant à des objets déjà définis. (Les objets qui contiennent d'autres objets sont appelés groupes.)
OSI	Voir interconnexion des systèmes ouverts.
Packeteer	Les périphériques Packeteer collectent, regroupent et stockent les données de performances du réseau. Lorsque vous configurez une source de flux externe pour Packeteer, vous pouvez envoyer les informations de flux d'un périphérique Packeteer vers QRadar Network Anomaly Detection.
passerelle	Périphérique qui communique avec deux protocoles et traduit les services entre eux.
pertinence	La pertinence détermine l'impact d'un événement, d'une catégorie ou d'une violation sur votre réseau. Par exemple, si un port spécifique est ouvert, la pertinence est élevée.
point de données	Tout point sur les graphiques QRadar Network Anomaly Detection où des données sont extraites.
pondération de réseau	Valeur numérique appliquée à chaque réseau qui témoigne de l'importance du réseau. La pondération de réseau est définie par l'utilisateur.

Processeur d'événements	Traite les événements collectés à partir d'un ou de plusieurs collecteurs d'événements. Les événements sont à nouveau regroupés pour préserver l'utilisation du réseau. Lors de la réception, le processeur d'événements met en corrélation les informations provenant de QRadar Network Anomaly Detection et distribuées dans la zone appropriée, en fonction du type d'événement.
protocole	Ensemble de règles et de formats déterminant le comportement de communication des entités de couche en matière de performances des fonctions de couche. Il peut continuer à requérir un échange d'autorisations avec un module de règles ou un serveur de règles externes avant la validation.
protocole de message de gestion inter-réseau(ICMP)	protocole de couche réseau Internet entre un hôte et une passerelle.
Protocole de résolution d'adresse (ARP)	Protocole de mappage d'une adresse IP (Internet Protocol) à une adresse hôte physique reconnue dans le réseau local. Par exemple, dans une IP Version 4, une adresse a une longueur de 32 bits. Toutefois, dans un réseau local Ethernet, les adresses des périphériques connectés ont une longueur de 48 bits.
Protocole DHCP	Voir Protocole DHCP.
Protocole DHCP	Un protocole qui permet l'attribution dynamique d'adresses IP pour l'équipement installé chez le client.
Protocole IP	Méthode ou protocole grâce à laquelle/auquel les données sont envoyées d'un ordinateur à un autre sur Internet. Chaque ordinateur (appelé hôte) sur Internet possède au moins une adresse IP l'identifiant de manière unique parmi tous les autres systèmes Internet. Une adresse IP comprend une adresse réseau et une adresse hôte. Une adresse IP peut également être divisée par un adressage ou une création de sous-réseau sans classe.
Protocole LDAP (Lightweight Directory Access Protocol)	Ensemble de protocoles pour accéder aux annuaires d'informations. Le protocole LDAP est basé sur les normes contenues dans la norme X.500, mais il est nettement plus simple. Et contrairement à la norme X.500, le protocole LDAP prend en charge le protocole TCP/IP, qui est nécessaire pour tout type d'accès Internet à un serveur d'annuaire.
protocole SOAP	Voir protocole SOAP.
protocole SOAP (Simple Object Access Protocol)	Protocole qui permet à un programme en cours d'exécution sur un type de système d'exploitation de communiquer avec un programme sur le même ou sur un autre type de système d'exploitation.
QRadar QFlow Collector	Recueille des données à partir de périphériques et de divers flux de données en direct ou enregistrés, tels que des TAP réseau, des ports SPAN/miroir, NetFlow et des journaux de flux QRadar Network Anomaly Detection.

QID	QRadar Identificateur. Mappage d'un événement unique d'un périphérique externe à un identificateur unique QRadar.
R2L	Voir Remote to Local.
R2R	Voir Remote to Remote.
rapports	Fonction permettant de créer des représentations graphiques du niveau d'exécution ou de fonctionnement de l'activité du réseau en fonction du temps, des sources, des violations, de la sécurité et des événements.
Redirection du protocole de résolution d'adresse	Le protocole de résolution d'adresse permet à un hôte de déterminer l'adresse des autres périphériques sur le réseau local ou le réseau local virtuel. Un hôte peut utiliser le protocole de résolution d'adresse pour identifier la passerelle par défaut (routeur) ou se rediriger vers le réseau local virtuel. Le protocole de résolution d'adresse permet à IBM Security QRadar Network Anomaly Detection d'indiquer à un hôte s'il existe un problème avec l'envoi de trafic à un système. Cela rend l'hôte et le réseau inutilisable jusqu'à ce que l'utilisateur intervienne.
règle	Collecte des conditions et des actions qui en découlent. Vous pouvez configurer les règles qui permettent à QRadar Network Anomaly Detection de capturer des séries d'événements précises et d'y répondre. Les règles vous permettent de détecter des événements précis et spécialisés et de transférer les notifications vers l'onglet Offenses ou le fichier journal, ou d'envoyer un email à un utilisateur.
règles de routage	Collection de conditions et de routage qui en découle qui sont exécutés lorsque les données d'événement correspondent à chaque règle.
réinitialisations TCP	Pour les applications basées sur le protocole TCP, QRadar Network Anomaly Detection peut émettre une réinitialisation TCP vers le client ou le serveur dans une conversation. Cela arrête la communication entre le client et le serveur.
Réseau IP	Groupe de routeurs IP qui achemine les datagrammes IP. Ces routeurs sont parfois appelés passerelles Internet. Les utilisateurs accèdent au réseau IP à partir d'un hôte. Chaque réseau Internet comprend des combinaisons d'hôtes et de routeurs IP.
réseau local (LAN)	Réseau de données non public dans lequel la transmission en série est utilisée pour la communication de données directe entre des stations de données situées dans les locaux de l'utilisateur.
Séries temporelles	Type de graphique qui représente graphiquement les données dans le temps. Ce graphique met en évidence les réseaux ou les informations de données d'adresse IP provenant des réseaux sélectionnés.
signature d'application	Ensemble unique de caractéristiques ou de propriétés, obtenu par l'examen du contenu du paquet, utilisé pour identifier une application spécifique.

Simple Network Management Protocol (SNMP)	Protocole de gestion de réseau utilisé pour contrôler les routeurs IP, les autres périphériques réseau et les réseaux auxquels ils sont associés.
SNMP	Voir Simple Network Management Protocol.
sources de flux	Source de flux reçue par QRadar QFlow Collector. Grâce à l'éditeur de déploiement, vous pouvez ajouter des sources de flux internes et externes provenant du système ou de l'élément Event Views de l'éditeur de déploiement.
Source hors site	Périphérique hors site qui transmet des données normalisées à un collecteur d'événements. Vous pouvez configurer une source hors site pour recevoir des flux ou des événements et permettre aux données d'être cryptées avant d'être transmises.
source de journal	Les sources de journaux sont des sources de journaux d'événements externes telles que le matériel de sécurité (par exemple les pare-feux et les IDS) et le matériel de réseau (par exemple, les commutateurs et les routeurs).
sous-recherche	Vous permet d'effectuer des recherches dans un ensemble de résultats de recherche terminée. La fonction de sous-recherche vous permet d'affiner vos résultats de recherche sans avoir besoin de rechercher à nouveau dans la base de données à nouveau.
sous-réseau	Un réseau subdivisé en réseaux ou sous-réseaux. Lorsqu'un sous-réseau est utilisé, la partie hôte de l'adresse IP est divisée en un numéro de sous-réseau et un numéro d'hôte. Les hôtes et les routeurs identifient les bits utilisés pour le réseau et le numéro de sous-réseau grâce à l'utilisation d'un masque de sous-réseau.
stratégie de marque	Une option de rapport qui permet à un utilisateur QRadar Network Anomaly Detection de télécharger des logos personnalisés pour des rapports personnalisés.
superflux	Plusieurs flux ayant les mêmes propriétés sont combinés en un seul flux pour augmenter le traitement en réduisant le stockage.
système de détection d'intrusion (IDS)	Application ou dispositif qui identifie une activité suspecte sur le réseau.
Système de prévention contre les intrusions (IPS)	Application qui réagit aux intrusions sur le réseau.
système TACACS (Terminal Access Controller Access Control System)	Le système TACACS (Terminal Access Controller Access Control System) est un protocole d'authentification qui permet un accès au serveur distant afin de transférer un mot de passe d'ouverture de session utilisateur à un serveur

d'authentification pour déterminer si l'accès peut être autorisé pour un système donné. TACACS+ utilise le protocole TCP.

TCP	Voir Transmission Control Protocol.
TopN	Affiche les <i>N</i> premiers réseaux ou informations d'adresse IP pour les données que vous consultez. Par exemple, en utilisant la fonctionnalité de graphique, vous pouvez afficher les cinq premiers réseaux générant un trafic aux Etats-Unis.
Transmission Control Protocol (TCP)	Service de flux fiable fonctionnant sur le protocole IP de la couche transport, ce qui assure la bonne livraison de bout-en-bout des paquets de données sans erreur.
violation	Comprend une violation de la politique d'entreprise.
violation	Message envoyé ou événement généré en réponse à une condition contrôlée. Par exemple, une violation vous informe si une politique a été violée ou si le réseau est attaqué.
Vue du système	Vous permet d'attribuer des composants logiciels, tels que QRadar QFlow Collector, à des systèmes (hôtes gérés) dans votre déploiement. La vue du système inclut tous les hôtes gérés dans votre déploiement. Un hôte géré est un système dans votre déploiement sur lequel le logiciel QRadar Network Anomaly Detection est installé.
Whois	Vous permet de rechercher des informations sur les noms et les numéros enregistrés sur Internet.

C

AVIS ET MARQUES

Dans cette annexe :

- [Avis](#)
- [Marques](#)

Cette section décrit quelques avis et marques importants et fournit des informations sur la conformité.

Avis

Ces informations étaient destinées aux produits et services offerts aux Etats-Unis.

IBM peut ne pas offrir les produits, les services ou les fonctions décrits dans ce document dans d'autres pays. Contactez votre interlocuteur IBM habituel pour obtenir des informations sur les produits et services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre produit, programme ou service fonctionnellement équivalent peut être utilisé, s'il n'enfreint pas les droits de propriété intellectuelle d'IBM. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier le fonctionnement de tout produit, programme ou service non IBM.

IBM peut détenir des brevets ou des demandes de brevet en instance couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Vous pouvez soumettre des demandes de licences par écrit à l'adresse suivante :

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.*

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues auprès du service IBM Intellectual Property Department de votre pays ou par écrit à l'adresse suivante :

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : INTERNATIONAL BUSINESS MACHINES CORPORATION LIVRE LE PRESENT DOCUMENT "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER, TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties explicites ou implicites pour certaines transactions, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Ces informations peuvent contenir des inexactitudes techniques ou des erreurs typographiques. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

*IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA*

Ces informations peuvent être soumises à des dispositions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions d'IBM Customer Agreement, d'IBM International Program License Agreement ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via

d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les prix IBM indiqués sont des prix de détail suggérés par IBM, sont à jour et peuvent être modifiés sans préavis. Les prix distributeurs peuvent donc varier.

Ces informations contiennent des exemples de données et de rapports utilisés dans les opérations métier habituelles. Pour les illustrer aussi complètement que possible, les exemples incluent les noms des personnes, des sociétés, des marques et des produits. Tous ces noms sont fictifs et toute ressemblance avec des noms et adresses utilisés par une société réelle serait purement fortuite.

Si vous visualisez la copie électronique de ces informations, les photographies et illustrations en couleur peuvent ne pas apparaître.

Marques

IBM, le logo IBM et [ibm.com](http://www.ibm.com) sont des marques ou des marques déposées d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse <http://www.ibm.com/legal/copytrade.shtml>.

Les noms suivants sont des marques ou des marques déposées d'autres sociétés :

Java et toutes les marques et tous les logos Java sont des marques ou des marques déposées d'Oracle et/ou de ses filiales.



Linux est une marque de Linus Torvalds aux Etats-Unis, dans d'autres pays ou les deux.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis, dans d'autres pays ou les deux.

UNIX est une marque de The Open Group aux États-Unis et dans d'autres pays.

INDEX

A

accéder à l'aide en ligne 11
onglet admin
 présentation 11
toutes les violations 29
règles de détection des anomalies
 règles des anomalies
 à propos de 182, 195
 tests d'anomalie 340
 tests du seuil de temps 340
 règles de comportement
 à propos de 182, 196
 tests de comportement 341
 tests du seuil de temps 342
 règles de seuil
 à propos de 182, 195
 tests de seuil de champs 343
 tests du seuil de temps 344
onglet d'actifs 207
 ajout de profils d'actifs 216
 suppression d'un profil d'actif 217
 modification d'un profil d'actif 216
 exportation d'un profil d'actif 218
 importation de profils d'actif 218
 gestion de profils d'actif 215
 présentation 6
 recherche
 profils d'actif 219
 actifs par attribut de vulnérabilité 222
 utilisation de la fonction de recherche 219
 affichage des profils d'actif 208

B

rapports de marque 258
éléments structurants
 à propos de 183
 modification 205
par catégorie 65

C

fonction de graphique 153
règles communes
 à propos de 182, 187
 tests de propriété communs 316
 tests date/heure 332
 tests de compteur de fonction 327
 tests négatifs de fonction 333
 tests de séquence de fonction 319
 tests simples de fonction 331
 tests de profil d'hôte 313
 test d'IP/port 315

 tests de propriété de réseau 332
configuration de la taille de page 11
conventions 1
tableaux de bord personnalisés
 création 16
propriétés d'événement personnalisées 114
 copie 121
 création 115, 118
 suppression 122
 modification 119
propriétés de flux personnalisées
 copie 149
 création 143
 suppression 150
 modification 148
règles personnalisées 181

D

éléments de tableau de bord
 événement de recherche 22
 événement par gravité 22
 activité du journal 21
 violations les plus récentes 21
 violations les plus graves 21
 mes violations 21
 activité du réseau 20
 violations 20
 rapports 22
 sources et destinations 21
 notifications du système 23
 récapitulatif du système 23
 premiers types de catégorie 21
 premières destinations locales 21
 premières sources de journal 22
 premières sources 21
onglet de tableau de bord
 présentation 5
tableau de bord
 à propos de 13
 ajout d'éléments 16
 éléments disponibles 20
 configuration des graphiques 17
 création d'un tableau de bord 16
 suppression d'un tableau de bord 20
 détacher des éléments 19
 modification d'un tableau de bord 19
 gestion 15
 suppression d'éléments 19
 affichage d'un tableau de bord 15
suppression des critères de recherche enregistrés 174

E

modification de rapports par défaut 254
 règles d'événement
 à propos de 182, 187
 tests de propriété communs 267
 tests date/heure 283
 tests de propriété d'événement 263
 tests de compteur de fonction 278
 tests négatifs de fonction 285
 tests de séquence de fonction 269
 tests simples de fonction 283
 tests de profil d'hôte 260
 test d'IP/port 262
 tests de source de journal 268
 tests de propriété de réseau 284
 événements
 propriétés d'événement personnalisées 114
 exportation 126
 réglage des faux positifs 122
 groupé 109
 étude 95, 159
 mappage 112
 normalisé 101
 brut 107
 flux 101
 affichage 100
 affichage des violations associées 112
 exportation
 événements 126
 flux 151
 violations 62

F

faux positifs (événements)
 réglage 122
 faux positifs (flux)
 réglage 150
 règles de flux
 à propos de 182, 187
 tests de propriété communs 295
 tests date/heure 310
 tests de propriété de flux 289
 tests de compteur de fonction 305
 tests négatifs de fonction 311
 tests de séquence de fonction 297
 tests simples de fonction 309
 tests de profil d'hôte 286
 test d'IP/port 288
 tests de propriété de réseau 310
 flux
 exportation 151
 réglage des faux positifs 150
 groupé 139
 normalisé 133
 diffusion en flux 132
 affichage 132
 suivi des violations 65
 fonctions 183

G

rapports générés 231
 génération d'un rapport 257
 balises géographiques 7
 glossaire 345
 événement regroupés 109
 flux regroupés 139

H

catégorie de haut niveau 65

I

utilisateurs concernés 1
 étude des adresses IP 7
 étude des noms d'utilisateurs 10
 Adresses IP
 étude 7

L

onglet log activity
 propriétés d'événement personnalisées 114
 mappage d'événements 112
 navigation des graphiques de séries temporelles
 (événements) 158
 présentation 5
 options de menu contextuel 100
 barre d'état 100
 barre d'outils 96
 affichage
 violations associées 112
 événements 100
 événement regroupés 109
 événements normalisés 101
 événements bruts 107
 événements de diffusion 101
 connection 4

M

gestion
 profils d'actif 215
 actifs 207
 violations 29
 modification de mappage d'événement 112
 mes violations 29

N

onglet network activity
 propriétés de flux personnalisés 142
 présentation 5
 clic droit 131
 barre d'outils 128
 utilisation 127
 utilisation de la fonction graphique 142
 affichage
 flux 132
 flux regroupés 139

flux normalisés 133
 flux de diffusion 132
 événements normalisés 101
 flux normalisés 133

O

règles de violations
 à propos de 182, 187
 tests date/heure 335
 tests de fonction 335
 test d'IP/port 334
 tests de source de journal 336
 tests de propriété de violation 336

violations
 à propos de 27
 ajout de notes 57
 attribution aux utilisateurs 63
 fermeture
 violations listées 60
 violations sélectionnées 59
 exportation 62
 suivi 65
 masquage 58
 gestion
 violations 29
 mes violations 29
 menu de navigation 28
 récapitulatif de source de violation
 options 49
 protéger
 violations listées 61
 violations protégées 60
 violations sélectionnées 61
 déprotection listée 62
 déprotection sélectionnée 62
 suppression 58
 fonction de recherche
 recherche des IP de destination 169
 recherche de réseau 170
 recherche d'IP source 168
 envoi de notification par courrier électronique 64
 affichage des violations masquées 58
 page de synthèse
 à propos de 33
 type de violation 43
 utilisation de l'onglet des violations 28
 affichage
 toutes les violations 29
 par catégorie 65
 par IP de destination 76
 par réseau 85
 par IP source 68

onglet offenses
 présentation 5

P

mise en pause de l'interface utilisateur 7
 PCAP data
 à propos de 123

affichage des colonnes 123
 téléchargement 125
 affichage 124
 préférences 10
 violations protégées 60

Q

Détection des anomalies QRadar
 présentation 3
 syntaxe de filtrage rapide 99

R

événements bruts 107
 actualisation de l'interface utilisateur 7
 types de graphiques 237
 vulnérabilités d'actif 237
 connexions 239
 événement/journaux 239
 flux 245
 premiers IP de destination 252
 premières violations 251
 premiers IP source 250

onglet reports
 à propos de 227
 attribution d'un rapport à un groupe 256
 image de marque 258
 type de graphique 237
 configuration des graphiques 237
 conteneurs 232
 contenu 232
 création d'un modèle 232
 création de rapports personnalisés 232
 rapports par défaut 254
 suppression du contenu généré 232
 canaux de distribution 235
 modification de rapports par défaut 254
 génération d'un rapport 257
 types de graphique 253
 regroupement de rapports 254
 attribution d'un rapport 256
 copie d'un rapport 256
 création d'un groupe 255
 modification d'un groupe 255
 suppression d'un rapport 256
 prévisualisation de disposition 235
 présentation 6
 formats de rapport 23
 présentation de rapport 232
 récapitulatif de rapport 236
 options de planification 232
 sélection d'un conteneur 234
 sélection d'une présentation 233
 partage d'un rapport 257
 barre d'outils 230
 utilisation de l'onglet des rapports 228
 utilisation de la barre d'état 232
 affichage
 rapports générés 231
 rapports 228

redimensionnement des colonnes 11

règles

à propos de 181

copie 202

création de règles de détection des anomalies 195

création de règles personnalisées 187

suppression 202

activation/désactivation 201

groupes 202

 affectation 205

 copie 204

 création 203

 suppression 204

 modification 204

affichage 184

S

critères de recherche enregistrée

 suppression 174

recherche

 profils d'actif 219

 actifs par attribut de vulnérabilité 222

tri des résultats 7

Système 23

T

tests

 à propos de 183

réglage des faux positifs (événements) 122

réglage des faux positifs (flux) 150

U

mise à jour des détails d'utilisateur 10

utilisation de la détection des anomalies QRadar 6

V

affichage

 toutes les violations 29

 profils d'actif 208

 violations associées 112

 tableaux de bord 15

 événements 100

 événements de diffusion 101

 heure système 10

 détails de vulnérabilité 213

détails de vulnérabilité 213