IBM Security QRadar Network Anomaly Detection
Version 7.1.0 (MR2)

Guide d'utilisation

Note: Avant d'utiliser le présent document et le produit associé, lisez les informations dans “Avis et Marques” à la page 383.

SOMMAIRE

A PROPOS DU PRÉSENT GUIDE

Le *IBM Security QRadar Network Anomaly Detection le guide d'utilisation IBM Security QRadar Network Anomaly Detection* fournit des informations sur la gestion de IBM Security QRadar Network Anomaly Detection notamment sur les onglets **Dashboard**, **Offenses**, **Log Activity**, **Network Activity**, **Assets**, and **Reports**.

Public visé

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:

ATTENTION : 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.*

ATTENTION : *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)

Contacter le service clients

Pour savoir comment contacter le service client, voir la note technique ***Support and Download Technical Note (note technique de prise de prise en charge et de téléchargement)***.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 A PROPOS DE LA DÉTECTION DES ANOMALIES QRADAR

Détection des anomalies QRadar 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.

Navigateurs Web pris en charge

Vous pouvez accéder à la console à partir d'un navigateur Web standard. Détection des anomalies QRadar prend en charge certaines versions de navigateurs Web Mozilla Firefox et Microsoft Internet Explorer.

Lorsque vous accédez au système, une invite s'affiche et demande un nom d'utilisateur et un mot de passe. Le nom d'utilisateur et le mot de passe doivent être configurés 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	10.0 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.
Microsoft® Windows Internet Explorer, avec vue de compatibilité activée	• 8.0 • 9.0 Pour obtenir des instructions sur la façon d'activer la vue Compatibility View, voir **Activation de Compatibility View pour Internet Explorer**.

Activation de Compatibility View pour Internet Explorer

Vous pouvez activer Compatibility View si vous utilisez Microsoft Internet Explorer pour accéder à Détection des anomalies QRadar.

Procédure

Etape 1 Dans votre navigateur Web Microsoft Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre Developer Tools.

Etape 2 Pour configurer le mode navigateur, dans la zone de liste **Browser Mode**, sélectionnez la version de votre navigateur Web.

Etape 3 Pour configurer le mode document, dans la zone de liste **Document Mode**, sélectionnez **Internet Explorer 7.0 Standards**.

Connexion à Détection des anomalies QRadar

Détection des anomalies QRadar est une application basée sur le Web. Pour vous connecter à Détection des anomalies QRadar, vous devez utiliser les navigateurs Web Mozilla Firefox ou Microsoft Internet Explorer.

Pour plus d'informations sur les navigateurs Web pris en charge, voir **Navigateurs Web pris en charge**.

A propos de cette tâche

Si vous utilisez un navigateur Web Mozilla Firefox, alors vous devez y ajouter une exception afin de pouvoir vous connecter à Détection des anomalies QRadar. Pour plus d'informations, voir votre documentation Mozilla Firefox.

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

Procédure

Etape 1 Ouvrez votre navigateur Web.

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

https://<`IP Address`>

Où **<** `IP adress` **>** 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**.

Etape 5 Pour vous déconnecter de Détection des anomalies QRadar, cliquez sur **Log out** dans le coin supérieur droit de l'interface utilisateur.

Result

Une clé de licence par défaut vous permet d'accéder à l'interface utilisateur pendant cinq semaines. Une fenêtre s'affiche et indique la date d'expiration de la clé de licence temporaire. Pour plus d'informations sur l'installation d'une clé de

licence, voir *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

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.

Onglet User interface

Détection des anomalies QRadar divise la fonction en onglet. L'onglet Dashboard est l'onglet par défaut qui s'affiche lorsque vous vous connectez à Détection des anomalies QRadar. Vous pouvez facilement accéder aux onglets afin de localiser les données ou fonctionnalités dont vous avez besoin.

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. Cinq 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**, voir **Gestion des tableaux de bord**.

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**, voir **Gestion des 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 **Etude de l'activité du journal**.

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 vous 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 **Etude de l’activité du réseau**.

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 des rapports**.

Onglet Admin

Si vous possédez des privilèges d'administration, vous pouvez accéder à l'onglet **Admin**. l'onglet **Admin** fournit aux utilisateurs 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** - Fournit l'accès aux composants plug-in. Cette option s'affiche uniquement si des plug-ins sont installés sur votre console.
- **Deployment Editor** - Vous permet de gérer les composants individuels de votre déploiement Détection des anomalies QRadar.

Toutes les mises à jour de configuration que vous effectuez 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**, voir le *IBM Security QRadar Network Anomaly DetectionGuide d'administration*.

procédures communes Détection des anomalies QRadar

Les diverses commandes sur l'interface utilisateur Détection des anomalies QRadar sont présentes sur la plupart des onglets de l'interface utilisateur. Cette section fournit des informations sur ces procédures communes.

Affichage des messages

Le menu Messages, qui se trouve au coin supérieur droit de l'interface utilisateur donne l'accès à la fenêtre sur laquelle vous pouvez lire et gérer vos notifications système.

Avant de commencer

Pour que les notifications système s'affichent sur la fenêtre Window, l'administrateur doit créer une règle basée sur chaque type de message de notification et cocher la case **Notify** dans Custom Rules Wizard. Pour plus d'informations sur la configuration des notifications d'événements et la création de règles d'événement, voir le *IBM Security QRadar Network Anomaly DetectionGuide d'administratio*n.

A propos de cette tâche

Le menu Messages indique le nombre de notifications systèmes non lues que vous avez dans votre système. Cet indicateur incrémente le nombre jusqu'à que vous rejetiez les notifications système. Pour chaque notification système, la fenêtre Messages fournit un récapitulatif et l'horodatage du moment de création de la notification système.Vous pouvez pointer votre souris sur la notification pour afficher plus de détails. A l'aide des fonctions sur la fenêtre Messages, vous pouvez gérer les notifications système.

Les notifications système sont également disponibles sur l'onglet **Dashboard** et sur la fenêtre contextuelle facultative que peut s'afficher au coin inférieur gauche de l'interface utilisateur. Les actions que vous effectuez dans la fenêtre Messages sont propagées sur l'onglet **Dashboard** et la fenêtre contextuelle. Par exemple, si vous rejetez une notification système de la fenêtre Messages, la notification système est supprimée de tous les affichages de notification système. Pour plus d'informations sur les notifications systèmes Dashboard, voir **Elément de notification système**.

La fenêtre Messages fournit les fonctions suivantes :

Tableau 1-2 Fonctions de la fenêtre Messages

Fonction	Description
All	Cliquez sur **All** pour afficher toutes les notifications système. Il s'agit de l'option par défaut, par conséquent, il vous suffit juste de cliquer sur **All** si vous avez sélectionné une autre option et que vous voulez afficher toutes les notifications système de nouveau.

Tableau 1-2 Fonctions de la fenêtre Messages

Fonction	Description
Health	Cliquez sur **Health** pour afficher uniquement les notifications système qui ont un niveau de gravité de santé.
Errors	Cliquez sur **Errors** pour afficher uniquement les notifications système qui ont un niveau de gravité d'erreur.
Warnings	Cliquez sur **Warnings** pour afficher uniquement les notifications système qui ont un niveau de gravité d'avertissement.
Information	Cliquez sur **Information** pour afficher uniquement les notifications système qui ont un niveau de gravité d'information.
Dismiss All	Cliquez sur **Dismiss All** pour rejeter toutes les notifications système de votre système. Si vous avez filtré la liste des notifications système en utilisant les icônes **Health**, **Errors**, **Warnings**, ou **Information**, le texte sur l'icône **View All** change pour devenir l'une des options suivantes : • Dismiss All Errors • Dismiss All Health • Dismiss All Warnings • Dismiss All Info
View All	Cliquez sur **View All** pour afficher les événements de notification système sur l'onglet **Log Activity**. Si vous avez filtré la liste des notifications système en utilisant les icônes **Health**, **Errors**, **Warnings**, ou **Information**, le texte sur l'icône **View All** change pour devenir l'une des options suivantes : • View All Errors • View All Health • View All Warnings • View All Info
Dismiss	Cliquez sur l'icône **Dismiss** à côté d'une notification système pour rejeter la notification système de votre système.

Lorsque vous cliquez sur une notification, les détails de notifications système suivants s'affichent dans une fenêtre contextuelle :

Tableau 1-3 Détails de notification système

Paramètre	Description
Flag	Affiche un symbole 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 Information (i) • Icône Error (X) • Icône Warning (!) • Icône Health
Host IP	Indique l'adresse IP de l'hôte qui a créé la notification système.
Gravité	Indique le niveau de gravité de l'incident qui a créé cette notification.
Low Level Category	Indique la catégorie à faible niveau associée à l'incident qui a généré cette notification système. Par exemple : interruption service. Pour plus d'informations sur les catégories, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
Payload	Indique le contenu de la charge utile associée à l'incident qui a généré cette notification système.
Created	Indique la quantité de temps qui s'est écoulée depuis la création de la notification.

Procédure

Etape 1 Connectez-vous à Détection des anomalies QRadar.

Etape 2 Au coin supérieur droit de l'interface utilisateur, cliquez sur **Messages**.

Etape 3 Sur la fenêtre Messages, affichez les détails de notification système.

Etape 4 Facultatif. Pour affiner la liste des notifications système, cliquez sur l'une des options suivantes :

- Errors
- Warnings
- Information

Etape 5 Facultatif. Pour rejeter des notifications système, choisissez l'une des options suivantes :

- Pour rejeter toutes les notifications système, cliquez sur **Dismiss All**.
- Pour rejeter une notification système, cliquez sur l'icône **Dismiss** près de la notification système que vous souhaitez rejeter.

Etape 6 Facultatif. Pour afficher les détails de notification système, survolez la notification de système à l'aide de la souris.

Tri de résultats Sur les onglets **Log Activity**, **Offenses**, **Network Activity** et **Reports**, vous pouvez trier les tableaux en cliquant sur un en-tête de colonne. Une flèche au dessus de la colonne indique la direction du tri.

Procédure

Etape 1 Connectez-vous à Détection des anomalies QRadar.

Etape 2 Cliquez sur l'onglet que vous souhaitez afficher :

Etape 3 Sélectionnez l'une des options suivantes :

- Cliquez sur l'en-tête de colonne une fois pour trier l'ordre descendant du tableau
- Cliquez sur l'en-tête de colonne deux fois pour trier l'ordre ascendant du tableau.

Actualisation et pause de l'interface utilisateur

Les onglets **Dashboard**, **Log Activity**, **Offenses**, et **Network Activity** vous permettent d'actualiser, de mettre en pause et de lire les données qui s'affichent sur l'onglet.

A propos de cette tâche

Les onglets **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). L'horloge, situé au coin supérieur droit de l'interface indique le volume de temps jusqu'à ce que l'onglet soit automatiquement actualisé.

Lorsque vous affichez les onglets **Log Activity** ou **Network Activity** en mode Real Time (streaming) ou Last Minute (actualisation automatique), vous pouvez utiliser l'icône **Pause** pour mettre en pause l'affichage actuel.

Vous pouvez également mettre en pause l'affichage actuel sur l'onglet **Dashboard**. 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.

Procédure

Etape 1 Connectez-vous à Détection des anomalies QRadar.

Etape 2 Cliquez sur l'onglet que vous souhaitez afficher.

Etape 3 Sélectionnez l'une des options suivantes :

- Afin d'actualiser l'onglet, cliquez sur l'icône **Refresh** située sur le coin supérieur droit de l'onglet.
- Pour mettre en pause l'affichage sur l'onglet, cliquez sur l'icône **Pause**.
- Si le temps est en pause, cliquez sur l'icône **Play** pour redémarrer le minuteur.

Etude des adresses IP

Les onglets **Dashboard**, **Log Activity**, **Offenses**, et **Network Activity** fournissent plusieurs méthodes pour étudier une adresse IP à partir de l'interface utilisateur.

A propos de cette tâche

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

Le menu contextuel vous fournit des options vous permettant d'étudier une adresse IP. Vous pouvez ajouter des options de menu contextuel personnalisées au menu. Pour plus d'informations sur la manière de personnaliser le menu contextuel, voir *Customizing the Right-Click Menu Technical Note*.

Procédure

Etape 1 Connectez-vous à Détection des anomalies QRadar.

Etape 2 Cliquez sur l'onglet que vous souhaitez afficher.

Etape 3 Survolez une adresse IP à l'aide du pointeur de votre souris afin d'afficher l'emplacement de l'adresse IP.

Etape 4 Effectuez un clic droit sur l'adresse IP ou le nom d'actif et sélectionnez l'une des options suivantes :

Option	Description
Navigate > View by Network	Affiche la fenêtre List of Networks, qui affiche tous les réseaux associés à l'adresse IP sélectionnée.
Navigate > View Source Summary	Affiche la fenêtre List of offenses, qui affiche toutes les violations associées à l'adresse IP source sélectionnée.
Navigate > View Destination Summary	Affiche la fenêtre List of Offenses, qui affiche toutes les violations associées avec l'adresse IP cible sélectionnée.
Information > DNS Lookup	Recherche les entrées DNS en fonction de l'adresse IP.
Information > WHOIS Lookup	Recherche le propriétaire enregistré d'une adresse IP distante. Le serveur WHOIS par défaut est whois.arin.net.
Information > Port Scan	Effectue une analyse Network Mapper (NMAP) 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, voir la documentation de votre fournisseur.
Information > 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, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Information > Search Events	Sélectionnez l'option **Search Events** afin de rechercher les événements associés à cette adresse IP. Pour plus d'informations, voir **Recherche d'événements ou de flux**.
Information > Search Flows	Sélectionnez l'option **Search Flows** afin de rechercher les événements associés à cette adresse IP. Pour plus d'informations, voir **Recherche d'événements ou de flux**..

Etude des noms d'utilisateur

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 de menu incluent :

Option	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, voir **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, voir **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, voir **Surveillance de l'activité du journal**.

Remarque : Pour plus d'informations sur la personnalisation du menu contextuel, voir *Customizing the Right-Click Menu* Technical Note.

Heure du système

A droite deDétection 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. Lorsque vous appliquez des filtres et recherches basés sur le temps sur les onglets **Log Activity Network Activity**, vous devez utiliser Console System Time lorsque vous spécifiez l'intervalle de temps.

Mise à jour des détails d'utilisateur

Vous pouvez mettre à jour vos détails d'utilisateur via l'interface utilisateur Détection des anomalies QRadar.

Procédure

Etape 1 Pour accéder à vos informations utilisateur, cliquez sur **Preferences**.

Etape 2 Si nécessaire, mettez à jour les paramètres suivants :

Options	Description
Username	Affiche votre nom d'utilisateur. Cette zone n'est pas modifiable
Password	Entrez un nouveau mot de passe. Le mot de passe doit répondre aux critères suivants : • Doit contenir six caractères au minimum • Doit contenir 255 caractères au maximum • Doit contenir au moins un caractère spécial • Doit contenir un caractère en majuscule

Options	Description
Password (Confirm)	Entrez le mot de passe à nouveau pour confirmation.
Email Address	Entrez votre adresse e-mail. L'adresse e-mail doit répondre aux conditions suivantes : • 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'interface utilisateur Détection des anomalies QRadar Online Help through the main Détection des anomalies QRadar. Pour accéder à l'aide en ligne, cliquez sur **Help > Help Contents.**

Redimensionnement des colonnes

Plusieurs onglets 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 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 le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

2 GESTION DU TABLEAU DE BORD

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

Présentation des tableaux de bord

Les tableaux de bord vous permettent d'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.

Tableaux de bord par défaut

L'onglet **Dashboard** fournit cinq tableaux de bord par défaut axés sur la sécurité, sur l'activité et l'application réseau, le contrôle du système et la conformité. Chaque tableau de bord affiche un ensemble d'éléments de tableau de bord par défaut. 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	Le tableau de bord **Application Overview** inclut les éléments par défaut suivants : • Inbound Traffic by Country (Total Bytes) • Outbound Traffic by Country (Total Bytes) • Top Applications (Total Bytes) • Top Applications Inbound from Internet (Total Bytes) • Top Applications Outbound to the Internet (Total Bytes) • DSCP - Precedence (Total Bytes)

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

Tableau de bord par défaut	Eléments
Network Overview	Le tableau de bord **Network Overview** inclut les éléments par défaut suivants : • Top Talkers (real time) • ICMP Type/Code (Total Packets) • Top Networks by Traffic Volume (Total Bytes) • Firewall Deny by DST Port (Event Count) • Firewall Deny by DST IP (Event Count) • Firewall Deny by SRC IP (Event Count) • Top Applications (Total Bytes) • Link Utilization (real-time) • DSCP - Precedence (Total Bytes)
System Monitoring	Le tableau de bord **System Monitoring** inclut les éléments par défaut suivants : • Top Log Sources (Event Count) • Link Utilization (real-time) • System Notifications • Event Processor Distribution (Event Count) • Event Rate (Events per Second Coalesced - Average 1 Min) • Flow Rate (Flows per Second - Peak 1 Min)
Threat and Security Monitoring	Le tableau de bord **Threat and Security Monitoring** inclut les éléments par défaut suivants : • Default-IDS/IPS-All: Top Alarm Signatures (real-time) • Top Systems Attacked (Event Count) • Top Systems Sourcing Attacks (Event Count) • My Offenses • Most Severe Offenses • Most Recent Offenses • Outbound Events by Country (real time) • Internet Threat Information Center • Flow Bias (Total Bytes) • Top Category Types • Top Sources • Top Local Destinations

Tableaux de bord personnalisés

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

Pour personnaliser votre onglet **Dashboard**, vous pouvez effectuer les tâches suivantes :

- Créez les tableaux de bord qui sont adaptés à vos responsabilités. QRadar Network Anomaly Detection prend en charge plus de 255 tableaux de bord par utilisateur ; cependant, des problèmes de performance peuvent se produire lorsque vous créez plus de 10 tableaux de bord.
- Ajoutez et supprimez des éléments de tableau de bord à partir des tableaux de bord personnalisés ou par défaut.
- Déplacez puis positionnez les éléments selon vos exigences. Lors du positionnement devos éléments, chaque élément se redimensionne automatiquement en fonction du tableau de bord.
- Ajoutez des éléments du tableau de bord basés sur toutes les données.

  Par exemple, vous pouvez ajouter un élément du tableau de bord qui fournit un graphique de série temporelle ou un graphique à barres qui représente les 10 activités réseau supérieures.

  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.

Eléments disponibles du tableau de bord

QRadar Network Anomaly Detection vous permet d'ajouter des éléments de tableau de bord à vos tableaux de bord personnalisés ou par défaut.

Les catégories d'élément du tableau de bord sont disponibles :

- **Eléments de recherche de flux**
- **Eléments de violation**
- **Eléments de l’activité du journal**
- **Eléments de rapports les plus récents**
- **Eléments de récapitulatif du système**
- **Eléments de notification système**
- **Centre de documentation Menace Internet**
- **Ajout d'éléments du tableau de bord basés sur la recherche à la liste Add Items**

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.

QRadar Network Anomaly Detection 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. **Ajout d'éléments du tableau de bord basés sur la recherche à la liste Add Items**.

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 types de graphiques pris en charge sont les séries temporelles, les tableaux, les graphiques circulaires et les barres. Le type de graphique par défaut est bar. Ces graphiques sont configurables. Pour plus d'informations sur la configuration des graphiques, voir **Configuration des graphiques**.

Les graphiques de série temporelle sont interactifs. Vous pouvez agrandir et parcourir un calendrier pour étudier l'activité réseau.

Eléments de violation

Vous pouvez ajouter plusieurs éléments de violation à votre tableau de bord.

Remarque : Les violations masquées 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 **Gestion des violations**.

Le tableau suivant décrit les éléments Offense :

Tableau 2-2 Offense items

Eléments du tableau de bord	Description
Most Recent Offenses	Les cinq violations les plus récentes sont identifiées par une barre d'amplitude pour vous informer son importance. Pointez votre souris sur le nom de la violation pour afficher des informations détaillées sur l'adresse IP.
Most Severe Offenses	Les cinq violations les plus graves sont identifiées par une barre d'amplitude pour vous informer de son importance. Pointez votre souris sur le nom de la violation pour afficher des informations détaillées sur l'adresse IP.
My Offenses	L'élément **My Offenses** affiche les cinq violations les plus récentes 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.

Tableau 2-2 Offense items (suite)

Eléments du tableau de bord	Description
Top Sources	L'élément **Top Sources** affiche les principales sources de violation. 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.
Top Local Destinations	L'élément **Top Local Destinations** affiche les destinations locales principales. 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.
Categories	L'élément **Top Categories Types** affiche les cinq principales catégories associées au plus grand nombre de violations.

Eléments de l'activité du journal

Les éléments du tableau de bord Log Activity vous permettent de surveiller et d'étudier les événements en temps réel.

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

Le tableau suivant décrit les éléments Log Activity :

Tableau 2-3 Log activity items

Dashboard item	Description
Event Searches	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'élément est basé. QRadar Network Anomaly Detection comprend des critères de recherche enregistrés par défaut qui sont préconfigurés pour l'affichage des éléments de recherche d'événements sur le menu de votre onglet **Dashboard**. Vous pouvez ajouter d'autres éléments de tableau de bord de recherche d'événements au menu de votre onglet **Dashboard**. Pour plus d'informations, voir **Ajout d'éléments du tableau de bord basés sur la recherche à la liste Add Items**. Sur un élément de tableau de bord **Log Activity**, les résultats de recherche affichent des données de dernière minute sur un graphique. Les types de graphiques pris en charge sont les séries temporelles, les tableaux, les graphiques circulaires et les barres. Le type de graphique par défaut est bar. Ces graphiques sont configurables. Pour plus d'informations sur la configuration de graphique, voir **Configuration des graphiques**. Les tableaux de série temporelle sont interactifs. Vous pouvez agrandir et parcourir un calendrier pour enquêter sur l'activité du journal.
Events By Severity	L'élément du tableau de bord **Events By Severity** affiche le nombre d'événements actifs regroupés par ordre de gravité. Cette élément 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 manière dont la cible a été préparée pour l'attaque. La plage de gravité est de 0 (faible) à 10 (élevé). Les types de graphiques pris en charge sont les tableaux, les graphiques circulaires et les barres.
Top Log Sources	L'élément du tableau de bord **Top Log Sources** affiche les cinq principales sources de journal qui envoient des événements à QRadar Network Anomaly Detection dans les 5 dernières minutes. Le nombre d'événements envoyés à partir de la source de journal spécifiée est indiqué dans le graphique. Cet élément vous permet de visualiser des changements potentiels dans le comportement, par exemple, si une source de journal du pare-feu qui figure généralement pas dans la liste des 10 meilleures contribue actuellement à un grand pourcentage du comptage de message global, vous devriez étudier cet événement. Les types de graphique pris en charge sont les tableaux, les graphiques circulaires et les barres.

Eléments de rapports les plus récents

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 le rapport a été généré et le format du rapport.

Eléments 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 :

- **Current Flows Per Second** - Affiche le débit des flux par seconde.
- **Flows (Past 24 Hours)** - Affiche le nombre total de flux actifs affichés les 24 dernières heures.
- **Current Events Per Second** - Affiche le débit des événements par seconde.
- **New Events (Past 24 Hours)** - Affiche le nombre total d'événements récents reçus pendant les 24 dernières heures.
- **Updated Offenses (Past 24 Hours)** - Affiche le nombre total des violations qui ont été créées ou modifiées avec la nouvelle démonstration pendant les 24 dernières heures.
- **Data Reduction Ratio** - Affiche le rapport de données réduites en fonction de l'intégralité des événements détectés pendant les 24 dernières heures ainsi que le nombre de violations modifiées pendant les 24 dernières heures.

Eléments de notifications 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 manière de configurer les notifications d'événement puis créer les règles d'événement, voir le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

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

- **Flag** - Affiche un symbole 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 de **santé**
  - **Icône** d'information (?)
  - **Icône** d'erreur (X)
  - **Icône** d'avertissement (!)
- **Created** - Affiche le temps écoulé depuis la création de la notification.
- **Description** - Affiche 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 :

- **Host IP** - Affiche l'adresse IP hôte de l'hôte ayant créé la notification.
- **Severity** - Affiche le niveau de gravité de l'incident ayant créé cette notification.
- **Low Level Category** - Affiche la catégorie de bas niveau associée à l'incident ayant généré cette notification. Par exemple : interruption service. Pour plus d'informations sur les catégories, voir le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
- **Payload** - Affiche le contenu de charge utile associée à l'incident ayant généré cette notification.
- **Created** - Affiche le temps écoulé depuis la création de la notification.

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 QRadar Network Anomaly Detection. Ces notifications contextuelles sont affichées sur le coin droit inférieur de l'interface utilisateur, quel que soit l'onglet sélectionné.

Les notifications contextuelles sont uniquement disponibles pour les utilisateurs ayant des autorisations administratives. 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 :

- **Next icon (>)** - 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.
- **Close icon (X)** - Ferme la fenêtre contextuelle de cette notification.
- **(details)** - Affiche les informations supplémentaires sur cette notification du système.

Centre de documentation Menace Internet

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

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

Les recommandations actuelles sont répertoriées dans l'élément de tableau de bord. Pour afficher un récapitulatif de recommandation, cliquez sur l'icône Arrow

située 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 l'intégralité de la recommandation, cliquez sur le lien associé. Le site Web IBM Internet Security Systems s'ouvre dans une autre fenêtre du navigateur et affiche les détails sur l'intégralité de la recommandation.

Tâches de gestion du tableau de bord

Sur l'onglet **Dashboard**, vous pouvez personnaliser vos tableaux de bord pour afficher et organiser les éléments des tableaux de bord correspondant à vos exigences en termes de sécurité des réseaux.

Affichage d'un tableau de bord

QRadar Network Anomaly Detection fournit cinq tableaux de bord par défaut, ce qui vous permet d'accéder à la zone de liste **Show Dashboard**. Lorsque vous avez préalablement affiché un tableau de bord et que vous l'avez renvoyé vers l'onglet **Dashboard**, le dernier tableau de bord vu s'affiche.

Procédure

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

Vous pouvez créer un tableau de bord personnalisé pour vous permettre un groupe d'éléments de bord correspondant à une exigence particulière.

A propos de cette tâche

Une fois que vous créez un tableau personnalisé, le nouveau tableau de bord s'affiche dans l'onglet **Dashboard** et est répertorié dans la zone de liste **Show Dashboard**. Un nouveau tableau de bord personnalisé est vide par défaut ; donc, vous devez ajouter les éléments au tableau de bord. Pour plus d'informations sur les éléments disponibles du tableau de bord, voir **Eléments disponibles du tableau de bord**.

Procédure

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

Etape 2 Cliquez sur l'icône **New Dashboard**.

Etape 3 Dans le champ **Name**, entrez un nom unique pour le tableau de bord.

La longueur maximale est de 65 caractères.

Etape 4 Dans le champ **Description**, entrez une description pour le tableau de bord.

La longueur maximale est de 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**.

Etape 6 Pour chaque élément que vous souhaitez ajouter, sélectionnez un élément dans la zone de liste **Add Item**.

Etude du journal ou de l'activité du réseau à partir d'un élément du tableau de bord

Vous pouvez étudier l'activité du journal ou du réseau à partir d'un élément du tableau de bord. Les éléments du tableau de bord axé sur la recherche fournissent un lien vers les onglets **Log Activity** ou **Network Activity**. Pour plus d'informations sur les éléments du tableau de bord, voir **Eléments disponibles du tableau de bord**.

Procédure

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

Etape 2 Sélectionnez l'une des options suivantes :

- Cliquez sur le lien **View in Log Activity**.
- Cliquez sur le lien **View in Network Activity**.

Result

Lorsque vous ouvrez l'onglet **Log Activity** ou **Network Activity** depuis l'onglet **Dashboard**, les données ainsi que les deux graphiques qui correspondent aux paramètres de votre élément de votre tableau de bord s'affichent. 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 et Network Activity** pour indiquer le type de graphique ainsi que le nombre d'objets de données que vous souhaitez afficher. Vos configurations de graphique personnalisées sont conservées afin qu'elles soient affichées comme étant configurées chaque fois que vous accédez à l'onglet**Dashboard**.

A propos de cette tâche

QRadar Network Anomaly Detection 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.

Procédure

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 Sur l'en-tête de l'élément du tableau de bord que vous souhaitez configurer, cliquez sur l'icône **Settings**.

Etape 4 Configurez les paramètres suivants :

Option	Description
Value to Graph	Dans la zone de liste, sélectionnez le type d'objet que vous voulez représenter sur le graphique. Les options incluent tous les paramètres d'événements personnalisés ou de flux inclus dans vos paramètres de recherche.
Chart Type	Dans la zone de liste, sélectionnez le type de graphique que vous souhaitez afficher. Ces options incluent : • **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 en ligne interactif représentant les enregistrements correspondants par intervalle de temps spécifique.
Display Top	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.
Capture Time Series Data	Cochez cette case pour activer la capture de série temporelle. Lorsque vous activez cette case à cocher, la fonction de graphique commence à accumuler des données pour les graphiques de séries temporelles. Par défaut, cette option est désactivée. ***Remarque :*** *Cette option est uniquement disponible sur les graphiques de série temporelle. Vous devez disposer d'autorisations appropriées pour gérer et afficher des graphiques de série temporelle. Pour plus d'informations sur les autorisations des rôles, voir le IBM Security QRadar Network Anomaly DetectionGuide d'administration.*
Time Range	Dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez afficher. ***Remarque :*** *Cette option est uniquement disponible sur les graphiques de série temporelle. Vous devez disposer d'autorisations appropriées pour gérer et afficher des graphiques de série temporelle. Pour plus d'informations sur les autorisations des rôles, voir le IBM Security QRadar Network Anomaly DetectionGuide d'administration.*

Suppression d'éléments

Vous pouvez supprimer les éléments d'un tableau de bord. Lorsque vous supprimez un élément du tableau de bord, l'élément n'est pas complètement

supprimé de fQRadar Network Anomaly Detection. Vous pouvez rajouter l'élément à tout moment.

Procédure

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.

Détachement d'un élément

Vous pouvez détacher l'élément de votre tableau de bord et afficher l'élément dans une nouvelle fenêtre sur votre ordinateur.

Lorsque vous détachez un élément du tableau de bord, l'élément original du tableau de bord reste sur l'onglet **Dashboard**, pendant qu'une fenêtre détachée avec un élément du tableau de bord dupliqué demeure ouvert et et s'actualise durant les intervalles programmés. Lorsque vous fermez l'application QRadar Network Anomaly Detection, la fenêtre détachée reste ouverte pour le contrôle et poursuit l'actualisation jusqu'à ce que vous fermez manuellement la fenêtre ou que vous arrêtiez votre ordinateur.

Procédure

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 du tableau de bord, cliquez sur l'icône verte pour détacher l'élément du tableau de bord puis ouvrez le dans une autre fenêtre.

Modification de nom d'un tableau de bord

Vous pouvez renommer un tableau de bord et mettre à jour la description.

Procédure

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 de 255 caractères.hol

Etape 6 Cliquez sur **OK**.

Suppression d'un tableau de bord

Vous pouvez utiliser un tableau de bord. Une fois le tableau de bord supprimé, l'onglet **Dashboard** s'actualise et le premier tableau de bord figurant 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**.

Procédure

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**.

Gestion des notifications système

Vous pouvez spécifiez le nombre de notifications que vous souhaitez afficher sur votre élément du tableau de bord **System Notification** puis désactiver les notifications du système après les avoir lues.

Avant de commencer

Assurez-vous que l'élément de tableau de bord **System Notification** est ajouté à votre tableau de bord. Pour plus d'informations, voir **Création d'un tableau de bord personnalisé**.

Procédure

Etape 1 - Dans l'en-tête de l'élément de tableau de bord de la notification du système, cliquez sur l'icône **Settings**.

Etape 2 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 s'affiche en incluant toutes les notifications du système. Pour plus d'informations sur les événements, voir **Etude de l'activité du journal**.

Etape 3 Pour fermer une notification de système, cliquez sur l'icône **Delete**.

Ajout d'éléments du tableau de bord basés sur la recherche à la liste Add Items

Depuis les onglets **Log Activity** et **Network Activity**, vous pouvez ajouter des éléments du tableau de bord basés sur la recherche vers le menu **Add Items**.

A propos de cette tâche

Cette procédure s'applique à tous les éléments du tableau de bord basés sur la recherche.

Avant de commencer

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.

Procédure

Etape 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 du tableau de bord de la recherche d'événement, cliquez sur l'onglet **Log Activity**.

Etape 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**.

Etape 3 Configurer ou modifier vos paramètres de recherche, tel que requis. Pour plus d'informations sur les éléments de recherche, voir **Recherche d'événements ou de flux**.

Etape 1 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**.

Etape 2 Cliquez sur **Filter**.

Les résultats de la recherche sont affichés.

Etape 3 Cliquez sur **Save Criteria**. Voir **Enregistrement des critères de recherche sur l'onglet Offense**.

Etape 4 Cliquez sur **OK**.

Etape 5 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 l'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 GESTION DES VIOLATIONS

QRadar Network Anomaly Detection peut comparer les événements et les flux aux adresses IP cible localisées dans plusieurs réseaux de la même violation. Ceci vous permet d'étudier efficacement chaque violation 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 et les flux uniques à l'origine de la violation.

Présentation des violations

L'onglet **Offenses** vous permet d'étudier les violations, les adresses IP source et cible, les comportements de réseau et les anomalies de votre réseau. Vous pouvez également rechercher des violations en fonction de critères différents.

Pour plus d'informations sur la recherche des violations, voir **Recherches de violations**.

Prise en compte des droits de violation

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

Termes clés

L'onglet Offenses vous permet d'accéder et d'analyser les **éléments** suivants :

- **Offenses** - Une violation comprend plusieurs événements ou flux provenant d'une seule source, comme un hôte ou une source de journal. L'onglet **Offenses** affiche les violations, notamment le trafic et les vulnérabilités qui collaborent et valident l'ampleur d'une violation. L'ampleur d'une violation est déterminée par plusieurs tests effectués sur la violation chaque fois qu'elle est ré-évaluée. La réévaluation se produit lorsque des événements sont ajoutés à la violation 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.

Conservation des violations

Sur l'onglet **Admin,** vous pouvez configurer les paramètres du système de la durée de conservation des violations pour supprimer les violations de la base de données après une période de temps configurée. La valeur par défaut de la durée de conservation de la violation est 3 jours. 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, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection - Configuring System Settings*.

Les violations que vous fermez sont supprimées de la base de données une fois leur durée de conservation écoulée. Si des événements supplémentaires se produisent pour une violation, une nouvelle violation est créée. Si vous effectuez une recherche qui inclut les violations fermées, l'article est affiché dans les résultats de la recherche tant qu'il n'a pas été retiré de la base de données.

Contrôle des violations

En utilisant les différents affichages disponibles sur l'onglet **Offenses**, vous pouvez contrôler les violations pour déterminer celles qui sont en cours sur votre réseau. Les violations sont énumérées en premier en fonction de la plus grande ampleur. Vous pouvez localiser et afficher les détails d'une violation particulière, puis prendre des mesures sur la violation, si nécessaire.

Après avoir démarré la navigation sur différents affichages, le côté supérieur de l'onglet **Offenses** affiche le trajet de navigation sur votre affichage actuel. Si vous souhaitez renvoyer à une page déjà affichée, cliquez sur le nom de la page sur le trajet de navigation.

Dans le menu de navigation, sur l'onglet **Offenses**, vous pouvez accéder aux pages suivantes :

Tableau 3-1 Options de menu de navigation de l'onglet Offense

Options	Description
My Offenses	Affiche toutes les violations qui vous sont affectées.
All Offenses	Affiche toutes les violations globales sur le réseau.
By Category	Affiche toutes les violations regroupées par catégorie de haut et de bas niveau.
By Source IP	Affiche toutes les violations regroupées par les adresses IP source qui sont impliquées dans une violation.
By Destination IP	Affiche toutes les violations regroupées par les adresses IP cible qui sont impliquées dans une violation.

Tableau 3-1 Options de menu de navigation de l'onglet Offense (suite)

Options	Description
By Network	Affiche toutes les violations regroupées par les réseaux impliqués dans une violation.
Rules	Permet d'accéder à la page Rules, à partir de laquelle vous pouvez afficher et créer des règles personnalisées. Cette option s'affiche uniquement si vous disposez des droits d'utilisation View C**ustom Rules. Pour plus d'informations, voir Gestion des règles**.

Contrôle des pages All Offenses ou My Offenses

Vous pouvez contrôler les violations sur les pages All Offenses ou My Offenses. La page All Offenses affiche la liste de toutes les violations sur votre réseau. La page My Offenses fournit la liste des violations qui vous sont affectées.

A propos de cette tâche

La partie supérieure du tableau affiche les détails des paramètres de recherche de violations, le cas échéant, appliqués aux résultats de la recherche. Pour supprimer ces paramètres de recherche, cliquez sur **Clear Filter**. Pour plus d'informations sur la recherche des violations, voir **Recherches de violations**.

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**. Pour plus d'informations sur les options de la barre d'outils, voir **Fonctions de la barre d'outils de l'onglet Offense**.

Procédure

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

Etape 2 Dans le menu de navigation, sélectionnez **All Offenses** ou **My Offenses**.

Etape 3 Vous pouvez affiner la liste des violations à l'aide des options suivantes :

- Dans la zone de liste View Offenses**, sélectionnez une option afin de filtrer la liste des violations pour une période donnée.**
- Si nécessaire, cliquez sur le lien **Clear Filter** à côté de chaque filtre affiché dans le panneau Current Search Parameters.

Etape 4 Cliquez deux fois sur la violation que vous souhaitez afficher.

Etape 5 Dans la page Offense Summary, consultez les détails de la violation. Voir **Paramètres des violations**.

Etape 6 Effectuez toutes les actions nécessaires sur la violation. Voir **Tâche de gestion des violations**.

Contrôle des violations regroupées par catégorie

Vous pouvez contrôler les violations sur la page By Category details, qui vous fournit une liste de violations regroupées sur la catégorie de haut niveau.

A propos de cette tâche

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

Procédure

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

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

Etape 3 Pour afficher les groupes de catégorie de bas niveau pour une catégorie particulière de haut niveau, cliquez sur la flèche à côté du nom de la catégorie de haut niveau.

Etape 4 Pour afficher la liste des violations d'une catégorie de bas niveau, cliquez deux fois sur la catégorie de bas niveau.

Etape 5 Cliquez deux fois sur la violation que vous souhaitez afficher.

Etape 6 Dans la page Offense Summary, consultez les détails de la violation. Voir **Paramètres des violations**.

Etape 7 Effectuez toutes les actions nécessaires sur la violation. Voir **Tâche de gestion des violations**.

Contrôle des violations regroupées par IP source

Dans la page Source, vous pouvez contrôler des violations regroupées par adresse IP source.

A propos de cette tâche

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

Procédure

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

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

Etape 3 Vous pouvez affiner la liste des violations à l'aide des options suivantes :

- Dans la zone de liste View Offenses**, sélectionnez une option afin de filtrer la liste des violations pour une période donnée.**
- Si nécessaire, cliquez sur le lien **Clear Filter** à côté de chaque filtre affiché dans le panneau Current Search Parameters.

Etape 4 Cliquez deux fois sur le groupe que vous souhaitez afficher.

Etape 5 Pour afficher une liste des adresses IP cibles locales pour l'adresse IP source, cliquez sur **Destinations** dans la page de la barre d'outils source.

Etape 6 Pour afficher une liste des violations associées à cette adresse IP source, cliquez sur **Offenses** dans la barre d'outils de la page Source.

Etape 7 Cliquez deux fois sur la violation que vous souhaitez afficher.

Etape 8 Dans la page Offense Summary, consultez les détails de la violation. Voir **Paramètres des violations**.

Etape 9 Effectuez toutes les actions nécessaires sur la violation. Voir **Tâche de gestion des violations**.

Contrôle des violations regroupées par IP de destination

Dans la page Destinations, vous pouvez contrôler des violations regroupées par les adresses IP cible locales.

A propos de cette tâche

Toutes les adresses IP cible sont listées en premier en fonction de la plus grande ampleur.

Procédure

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

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

Etape 3 Vous pouvez affiner la liste des violations à l'aide des options suivantes :

- Dans la zone de liste View Offenses**, sélectionnez une option afin de filtrer la liste des violations pour une période donnée.**
- Si nécessaire, cliquez sur le lien **Clear Filter** à côté de chaque filtre affiché dans le panneau Current Search Parameters.

Etape 4 Cliquez deux fois sur l'adresse IP cible que vous souhaitez afficher.

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

Etape 6 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 Destination.

Etape 7 Cliquez deux fois sur la violation que vous souhaitez afficher.

Etape 8 Dans la page Offense Summary, consultez les détails de la violation. Voir **Paramètres des violations**.

Etape 9 Effectuez toutes les actions nécessaires sur la violation. Voir **Tâche de gestion des violations**.

Contrôle des violations regroupées par réseau

Dans la page networks, vous pouvez contrôler des violations regroupées par réseau.

A propos de cette tâche

Tous les réseaux sont listés en premier en fonction de la plus grande ampleur.

Procédure

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

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

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

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 Network.

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 Network.

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

Etape 7 Cliquez deux fois sur la violation que vous souhaitez afficher.

Etape 8 Dans la page Offense Summary, consultez les détails de la violation. Voir **Paramètres des violations**.

Etape 9 Effectuez toutes les actions nécessaires sur la violation. Voir **Tâche de gestion des violations**.

Tâche de gestion des violations

Lors du contrôle des violations, vous pouvez effectuer des actions sur la violation.

Vous pouvez effectuer les actions suivantes :

- Ajouter des notes
- Supprimer des violations
- Protéger des violations
- Exporter des données de violation vers XML ou CSV
- Affecter des violations à d'autres utilisateurs
- Envoyer des notifications par courrier électronique
- Marquer une violation pour suivi
- Masquer ou fermer une violation de toute liste des violations

Pour effectuer une action sur plusieurs violations, maintenez la touche Control enfoncée pendant que vous sélectionnez chaque violation que vous souhaitez sélectionner. Pour afficher les détails d'une violation sur une nouvelle page, maintenez la touche Control enfoncée pendant que vous cliquez deux fois sur une violation.

Ajout de notes

Vous pouvez ajouter des notes à toute violation sur l'onglet **Offenses**. Les notes peuvent comprendre des informations que vous souhaitez inclure dans la violation, comme le numéro de ticket Customer Support ou les informations de gestion des violations.

A propos de cette tâche

Les notes peuvent inclure jusqu'à 1996 caractères. Le texte de la note n'effectue pas une recherche en boucle automatiquement 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 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.

L'option **Add Note** est disponible aux emplacements suivants dans un récapitulatif de violation :

- La zone de liste **Actions** dans la barre d'outils récapitulative de violation.
- L'icône **Add Note** dans le panneau Last 5 Notes.

Procédure

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

Etape 2 Naviguez jusqu'à la violation à laquelle vous souhaitez ajouter des notes.

Etape 3 Cliquez deux fois sur la violation.

Etape 4 A partir de la zone de liste **Actions**, sélectionnez A**dd Note.**

Etape 5 Entrez la note que vous souhaitez inclure pour cette violation.

Etape 6 Cliquez sur Add Note**.**

Result

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

Masquage des violations

Pour empêcher une violation de s'afficher sur l'onglet **Offenses**, vous pouvez cacher cette violation.

A propos de cette tâche

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

Procédure

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

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Sélectionnez la violation que vous souhaitez masquer.

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

Etape 5 Cliquez sur **OK**.

Affichage des violations masquées

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

A propos de cette tâche

Pour afficher les violations masquées, vous devez effectuer une recherche incluant des violations masquées. Les résultats de la recherche comprennent toutes les violations, notamment celles cachées et non cachées. Les violations sont indiquées comme cachées par l'icône **Hidden** dans la colonne **Flag**.

Procédure

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

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Rechercher des violations cachées :

- **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**.

Etape 4 Localisez et sélectionnez la violation masquée que vous souhaitez afficher.

Etape 5 Dans la zone de liste **Actions**, sélectionnez **Show**.

Fermeture des violations

Pour supprimer une violation complètement de votre système, vous pouvez fermer la violation.

A propos de cette tâche

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

Lorsque vous fermez des violations, vous devez sélectionner la cause de cette fermeture et vous pouvez ajouter une note. La zone **Notes** affiche la note entrée pour la fermeture de la violation précédente. Les notes ne doivent pas dépasser 2000 caractères. La note est affichée dans le panneau Notes de cette violation. Si vous disposez de l'autorisation Manage Offense Closing, vous pouvez ajouter de nouvelles causes personnalisées dans la zone de liste **Reason for Closing**. Pour plus d'informations, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Procédure

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

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Sélectionnez l'une des options suivantes :

- Sélectionnez la violation que vous souhaitez fermer, puis sélectionnez **Close** dans la zone de liste **Actions**.
- 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**.

Etape 5 Facultatif. Dans la zone **Notes**, entrez une note pour fournir des informations supplémentaires sur la fermeture de la note.

Etape 6 Cliquez sur OK**.**

Result

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

Protection des violations

Vous pouvez empêcher les violations spécifiées d'être supprimées de la base de données après que la période de conservation est écoulée.

A propos de cette tâche

Les violations sont conservées pendant une durée de conservation configurable. La valeur par défaut de la durée de conservation est 3 jours; cependant les administrateurs peuvent personnaliser la durée de conservation. Vous pourriez

disposer de violations que vous souhaitez conserver quelle que soit la durée de conservation. Vous pouvez empêcher ces violations spécifiées d'être supprimées de la base de données après que la période de conservation est écoulée. Pour plus d'informations sur la durée de conservation des violations, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

ATTENTION : *Lorsque le modèle de données SIM est réinitialisé en utilisant l'option* ***Hard Clean****, toutes les violations, y compris les violations 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.*

Procédure

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

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Sélectionnez l'une des options suivantes :

- Sélectionnez la violation que vous souhaitez protéger, puis sélectionnez **Protect** dans la zone de liste **Actions**.
- Dans la zone de liste **Actions**, sélectionnez **Protect Listed**.

Etape 4 Cliquez sur **OK**.

Result

La violation protégée est indiquée par une icône Protected dans la colonne **Flag**.

Annulation de la protection des violations

Vous pouvez annuler la protection des violations précédemment protégées de la suppression à la fin de la durée de conservation de la violation.

A propos de cette tâche

Pour répertorier uniquement les violations protégées, vous pouvez effectuer une recherche qui filtre uniquement les violations 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 violations protégées s'affichent.

Procédure

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

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Facultatif. Effectuez une recherche qui affiche uniquement les violations protégées.

Etape 4 Sélectionnez l'une des options suivantes :

- Sélectionnez la violation que vous souhaitez protéger, puis sélectionnez **Unprotect** dans la zone de liste **Actions**
- Dans la zone de liste **Actions**, sélectionnez **Unprotect Listed**.

Etape 5 Cliquez sur **OK**.

Exportation des violations

Vous pouvez exporter des violations au format Extensible Markup Language (XML) ou Comma Separated Values (CSV).

A propos de cette tâche

Si vous souhaitez utiliser à nouveau ou stocker vos données de violation, vous pouvez exporter les violations. Par exemple, vous pouvez exporter des violations pour créer des rapports non basés sur QRadar Network Anomaly Detection. Vous pouvez également exporter des violations comme stratégie secondaire de conservation à long terme. Le service clients peut vous demander d'exporter des violations 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.

Procédure

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

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

Etape 3 Sélectionnez la violation que vous souhaitez exporter.

Etape 4 Sélectionnez l'une des options suivantes :

- Pour exporter les violations au format XML, sélectionnez **Actions > Export to XML** dans la zone de liste **Actions**.
- Pour exporter les violations au format CSV, sélectionnez **Actions > Export to CSV** dans la zone de liste **Actions**

Etape 5 Sélectionnez l'une des options suivantes :

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

Etape 6 Cliquez sur **OK**.

Affectation des violations aux utilisateurs

En utilisant l'onglet **Offenses**, vous pouvez affecter des violations aux utilisateurs QRadar Network Anomaly Detection pour investigation.

A propos de cette tâche

Lorsqu'une violation est affectée à un utilisateur, la violation est affichée sur la page My Offenses appartenant à cet utilisateur. Vous devez disposer de privilèges appropriés pour affecter des violations aux utilisateurs. Pour plus d'informations sur les rôles d'utilisateur, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Vous pouvez attribuer des violations aux utilisateurs soit à partir de l'onglet **Offenses** ou des pages Offense Summary. Cette procédure fournit des instructions sur l'affectation des violations dans l'onglet Offenses.

Procédure

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

Etape 2 Cliquez sur **All Offenses**.

Etape 3 Sélectionnez la violation que vous souhaitez affecter.

Etape 4 Dans 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 violation.

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

Etape 6 Cliquez sur **Save**.

Result

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

Envoi de notification par courrier électronique

Vous pouvez envoyer un e-mail contenant un récapitulatif de violation à n'importe quelle adresse e-mail valide.

A propos de cette tâche

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 la violation ou de la règle d'événement
- Description complète de la violation ou de la règle d'événement
- Division d'identification de la violation
- Les cinq principales catégories

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

Procédure

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

Etape 2 Naviguez jusqu'à la violation pour laquelle vous souhaitez envoyer une notification par e-mail

Etape 3 Cliquez deux fois sur la violation.

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

Etape 5 Configurez les paramètres suivants :

Paramètre	Description
To	Entrez l'adresse e-mail de l'utilisateur que vous souhaitez notifier si un changement se produit dans la violation 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**.

Marquage d'éléments pour suivi

En utilisant l'onglet **Offenses**, vous pouvez marquer une violation, une adresse IP source, une adresse IP cible et un réseau pour suivi. Cela vous permet de contrôler un élément particulier pour une investigation complémentaire.

Procédure

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

Etape 2 Naviguez jusqu'à la violation que vous souhaitez marquer pour suivi.

Etape 3 Cliquez deux fois sur la violation.

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

Result

La violation affiche désormais un indicateur dans la colonne **Flags**, indiquant que la violation est marquée pour suivi. Si vous ne voyez pas votre violation marquée sur la liste de violations, vous pouvez trier la liste pour afficher en premier toutes les violations marquées. Pour trier une liste de violations par violation marquée, cliquez deux fois sur l'en-tête de colonne **Flags**.

Fonctions de la barre d'outils de l'onglet Offense

Chaque page et tableau sur l'onglet **Offenses** dispose d'une barre d'outils permettant de fournir les fonctions nécessaires pour effectuer certaines actions ou pour étudier les facteurs qui ont contribué à une violation. Le tableau suivant fournit des descriptions sur les fonctions de la barre d'outils.

Tableau 3-2 Fonctions de la barre d'outils de l'onglet Offense

Fonction	Description
Add Note	Cliquez sur **Add Note** pour ajouter une nouvelle note à une violation. Cette option n'est disponible que sur le panneau Last 5 Notes de la page Offense Summary.
Actions	Les options disponibles dans la zone de liste **Actions** varient en fonction de la page, du tableau ou de l'élément (comme une violation ou une adresse IP source). La zone de liste **Actions** peut ne pas s'afficher exactement comme indiqué ci-dessous. Dans la zone de liste **Actions**, vous pouvez sélectionner l'une des actions suivantes : • **Follow up** - Sélectionnez cette option pour marquer un élément pour un suivi ultérieur. Voir **Marquage d'éléments pour suivi**. • **Hide** - Sélectionnez cette option pour masquer une violation. Pour plus d'informations sur les violations masquées, voir **Masquage des violations**. • **Show** - Sélectionnez cette option pour afficher toutes les violations masquées. Pour plus d'informations sur l'affichage des violations, voir **Affichage des violations masquées**. • **Protect Offense** - Sélectionnez cette option pour protéger une violation. Pour plus d'informations sur la protection des violations, voir **Protection des violations**. • **Close** - Sélectionnez cette option pour fermer une violation. Pour plus d'informations sur la fermeture des violations, voir **Fermeture des violations**. • **Close Listed** - Sélectionnez cette option pour fermer la violation listée. Pour plus d'informations sur la fermeture des violations listées, voir **Fermeture des violations**. • **Email** - Sélectionnez cette option pour envoyer un récapitulatif de violation à un ou plusieurs destinataires. Voir **Envoi de notification par courrier électronique**. • **Add Note** - Sélectionnez cette option pour ajouter des notes à un élément. Voir **Ajout de notes**. • **Assign** - Sélectionnez cette option pour affecter une vviolation à un utilisateur. Voir **Affectation des violations aux utilisateurs**. • **Print** - Sélectionnez cette option pour imprimer une violation.

Tableau 3-2 Fonctions de la barre d'outils de l'onglet Offense (suite)

Fonction	Description
Annotations	Cliquez sur **Annotations** pour afficher toutes les annotations d'une violation. • **Annotation** - Indique les détails d'une annotation. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux violations comme composant de la réponse de la règle. Pour plus d'information sur les règles, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*. • **Time** - Indique la date et l'heure où l'annotation a été créée. • **Weight** - Indique la pondération de l'annotation.
Anomaly	Cliquez sur **Anomaly** pour afficher les résultats de la recherche sauvegardée à l'origine de la règle de détection d'anomalie qui a généré cette violation. ***Remarque :*** *Ce bouton s'affiche uniquement si la violation a été générée par une règle de détection d'anomalie.*
Categories	Cliquez sur **Categories** pour afficher les informations de catégorie de la violation sélectionnée. 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** ou **Flows**. Alternativement, vous pouvez mettre en évidence la catégorie et cliquez sur l'icône **Events** ou **Flows** dans la barre d'outils Event Categories. Pour plus d'information sur les catégories, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Destinations	Cliquez sur **Destinations** pour afficher toutes les adresses IP cible locales d'une violation, l'adresse IP source ou le réseau. ***Remarque :*** *Si les adresses IP cible sont distantes, une page séparée s'ouvre pour fournir des informations liées aux adresses IP cible distantes.*
Display	La page Offense Summary affiche plusieurs tableaux d'informations relatifs à une violation. Pour localiser un tableau, vous pouvez défiler jusqu'au tableau à afficher ou sélectionner l'option dans la zone de liste **Display**.
Events	Cliquez sur **Events** pour afficher tous les événements d'une violation. Lorsque vous cliquez sur **Events**, les résultats de la recherche d'événement s'affichent. Pour des informations sur les événements recherche, voir **Recherche d'événements ou de flux**.
Flows	Cliquez sur **Flows** pour continuer à étudier les flux associés à une violation. Lorsque vous cliquez sur **Flows**, les résultats de la recherche de flux sont affichés. Voir **Recherche d'événements ou de flux**..

Tableau 3-2 Fonctions de la barre d'outils de l'onglet Offense (suite)

Fonction	Description
Log Sources	Cliquez sur **Log Sources** pour afficher toutes les sources de journal d'une violation.
Networks	Cliquez sur **Networks** pour afficher tous les réseaux de destination d'une violation.
Notes	Cliquez sur **Notes** pour afficher toutes les notes d'une violation, l'adresse IP source, l'adresse IP cible ou le réseau.Pour plus d'information sur les notes, voir **Ajout de notes**.
Offenses	Cliquez sur **Offenses** pour afficher la liste des violations associées à une adresse IP source, cible ou à un réseau.
Print	Cliquez sur **Print** pour imprimer une violation.
Rules	Cliquez sur **Rules** pour afficher toutes les règles ayant contribué à une violation. La règle qui a créé la violation est listée en premier. Si vous disposez d'autorisations appropriées pour modifier une règle, cliquez deux fois sur la règle pour lancer la page Edit Rules. Pour plus d'informations sur les rôles d'utilisateur, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*. 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.
Save Criteria	Après avoir effectué une recherche de violation, cliquez sur **Save Criteria** pour sauvegarder vos critères de recherche pour une utilisation ultérieure.
Save Layout	Par défaut, la page By Category details est triée par le paramètre Offense Count. Si vous changez l'ordre de tri, 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.
Search	Cette option est uniquement disponible sur la barre d'outils du tableau List of Local Destinations. Cliquez sur **Search** pour filtrer les IP cible d'une adresse IP source. Pour filtrer les cibles : **1** Cliquez sur **Search**. **2** Entrez des valeurs pour les paramètres suivants : **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**.

Tableau 3-2 Fonctions de la barre d'outils de l'onglet Offense (suite)

Fonction	Description
Show Inactive Categories	Dans la page By Category details, les comptages pour chaque catégorie sont accumulés à partir des valeurs dans les catégories de bas niveau Les catégories de bas niveau sur les violations 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**.
Sources	Cliquez sur **Sources** pour afficher toutes les adresses IP source de la violation, l'adresses IP cible ou le réseau.
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 détaillée.
Users	Cliquez sur **Users** pour afficher tous les utilisateurs associés à une violation.

Paramètres des violations

Le tableau suivant fournit des descriptions de paramètres proposées sur toutes les pages de l'onglet **Offenses**.

Tableau 3-3 Paramètres des violations

Paramètre	Emplacement	Description
Annotation	Tableau Top 5 Annotations	Indique les détails de l'annotation. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux violations comme composant de la réponse à la règle. Pour plus d'information sur les règles, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Anomaly	Tableau Last 10 Events (Anomaly Events)	Sélectionnez cette option pour afficher les résultats de recherche enregistrés ayant provoqué la règle de détection d'anomalie pour générer l'événement.
Anomaly Text	Tableau Last 10 Events (Anomaly Events)	Indique une description du comportement anormal qui a été détecté par la règle de détection d'anomalie.
Anomaly Value	Tableau Last 10 Events (Anomaly Events)	Indique la valeur qui a provoqué la règle de détection d'anomalie pour générer la violation.
Application	Tableau Last 10 Flows	Indique l'application associée au flux.
Application Name	Tableau Offense Source, si le type de violation est App ID	Indique l'application associée au flux qui a créé la violation.
ASN Index	Tableau Offense Source, si le type de violation est Source ASN ou Destination ASN	Indique la valeur ASN associée au flux qui a créé la violation.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Asset Name	Tableau Offense Source, si le type de violation est Source IP ou Destination IP	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**.
Asset Weight	Tableau Offense Source, si le type de violation est Source IP ou Destination IP	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**.
Assigned to	Tableau Offense	Indique l'utilisateur affecté à la violation. Si aucun utilisateur n'est affecté, cette zone indique Not assigned. Cliquez sur **Not assigned** pour affecter la violation à un utilisateur. Pour plus d'informations, voir **Affectation des violations aux utilisateurs**.
Category	Tableau Last 10 Events	Indique la catégorie de l'événement.
Category Name	Page By Category Details	Indique le nom de catégorie de haut niveau. Pour plus d'informations sur les catégories de haut niveau, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Chained	• Tableau Offense Source, si le type de violation est Destination IP • Tableau Top 5 Destination IPs	Indique si l'adresse IP cible est enchaînée. Une adresse IP cible enchaînée est associée à d'autres violations. Par exemple, une adresse IP cible peut devenir l'adresse IP source d'une autre violation. Si l'adresse IP cible est enchaînée, cliquez sur **Yes** pour afficher les violations enchaînées.
Creation Date	Tableau Last 5 Notes	Indique la date et l'heure de création de la remarque.
Credibility	Tableau Offense	Indique la crédibilité de la violation, telle que déterminée par le classement de crédibilité de dispositifs de source. Par exemple, la crédibilité est augmentée lorsque plusieurs violations signalent le même événement ou flux.
Current Search Parameters	• Page By Source IP Details • Page By Destination IP Details	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**. ***Remarque :*** *Ce paramètre s'affiche uniquement après l'application d'un filtre.*

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Description	• Page All Offenses • Page My Offenses • Tableau Offense • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses • Tableau Offense Source, si le type de violation est Log Source • Tableau Top 5 Log Sources	Indique la description de la violation ou de la source de journal.
Destination IP	• Tableau Last 10 Events • Tableau Last 10 Flows	Indique l'adresse IP cible de l'événement ou du flux.
Destination IP	• Tableau Top 5 Destination IPs • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Network - List of Local Destinations	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, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Destination IP(s)	Tableau Offense	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.
Destination IPs	• Page All Offenses • Page My Offenses	Indique les adresses IP et le nom de l'actif (si disponible) des destinations locales ou distantes. Si plusieurs adresses IP cible sont associées à la violation, cette zone indique Multiple et le nombre d'adresses IP cible.
Destination IPs	• Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique les adresses IP et les noms de l'actif (si disponibles) de la destination associée à la violation. 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 consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Destination IPs	Page By Network Details	Indique le nombre d'adresses IP cible associées au réseau.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Destination Port	Tableau Last 10 Flows	Indique le port de destination du flux.
Destination(s)	• Tableau Top 5 Source IPs • Page By Source IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources	Indique le nombre d'adresses IP cible de l'adresse IP source.
Dst Port	Tableau Last 10 Events	Indique le port de destination de l'événement.
Duration	Tableau Offense	Indique la quantité de temps écoulée depuis la première détection de la violation.
Event Name	• Tableau Offense Source, si le type de violation est Event Name • Tableau Last 10 Events • Tableau Last 10 Events (Anomaly Events)	Indique le nom de l'événement, comme indiqué dans la carte QID, associé à l'événement ou au flux qui a créé la violation. Déplacez votre souris sur le non de l'événement pour afficher le QID.
Event/Flow Count	Page By Category Details	Indique le nombre d'événements actifs ou de flux (événements ou flux qui ne sont pas fermés ou masqués) associés à la violation dans la catégorie. Les violations restent actives uniquement pendant une période de temps si aucun nouvel événement ou flux n'est reçu. Les violations s'affichent toujours dans l'onglet **Offenses**, mais ne sont pas comptées dans cette zone.
Event/Flow Count	Page Destination Page Network	Indique le nombre total d'événements ou de flux générés associés à l'adresse IP cible ou au réseau.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Event/Flow Count	Tableau Offense	Indique le nombre d'événements et de flux qui se sont produits pour la violation et le nombre de catégories. Cliquez sur le lien événements afin d'étudier davantage les événements associés à la violation. Lorsque vous cliquez sur le lien événements, les résultats de la recherche d'événement s'affichent. Cliquez sur le lien flux afin d'étudier davantage les flux associés à la violation. Lorsque vous cliquez sur le lien flux, les résultats de la recherche de flux s'affichent. ***Remarque :*** *Si le comptage de flux affiche N/A, la violation 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 (MR2), par conséquent, les flux ne peuvent pas être comptés. Vous pouvez, toutefois, cliquez sur le lien N/A pour enquêter sur les flux associés aux résultats de la recherche de flux.*
Events	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique le nombre d'événements de la violation.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Events/Flows	• Tableau Offense Source, si le type de violation est Source IP, Destination IP, Hostname, Username Source Port ou Destination, Event Name, Port, Source MAC Address ou Destination MAC Address, Log Source, Source IPv6 ou Destination IPv6, Source ASN ou Destination ASN, Rule, App ID • Tableau Top 5 Source IPs • Page By Source IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Page Source Details • Tableau Top 5 Destination IPs • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Network - List of Local Destinations • Tableau Top 5 Users • Tableau Top 5 Log Sources • Tableau Top 5 Categories • Page By Network Details • Tableau Top 5 Categories	Indique le nombre d'événements ou de flux associés à l'adresse IP source, l'adresse IP cible, le nom de l'événement, le nom d'utilisateur, l'adresse MAC, la source de journal, le nom d'hôte, le port, la source de journal, l'adresse ASN, l'adresse IPv6, la règle, ASN, l'application, le réseau ou la catégorie. Cliquez sur le lien pour afficher plus de détails.
First event/flow seen on	Page Source Details	Indique la date et l'heure où l'adresse IP source a généré le premier événement ou flux.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Flag	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique les mesures prises sur la violation. Les actions sont représentées par les icônes suivantes : • **Flag** - Indique que la violation est marquée pour suivi. Ceci vous permet de contrôler un article particulier pour une investigation complémentaire. Pour plus d'informations sur la façon de marquer une violation pour le suivi, voir **Marquage d'éléments pour suivi**. • **User** - Indique que la violation a été affectée à un utilisateur. Lorsqu'une violation est affectée à un utilisateur, la violation est affichée sur la page My Offenses appartenant à cet utilisateur. Pour plus d'informations sur l'affectation des violations aux utilisateurs, voir **Affectation des violations aux utilisateurs**. • **Notes** - Indique qu'un utilisateur a ajouté des notes à la violation. Les notes peuvent inclure toute information que vous souhaitez capturer pour la violation. Par exemple, vous pourriez ajouter une note qui indique une information qui n'est pas automatiquement incluse dans une violation, comme un numéro de ticket de service clients ou d'information de gestion de violation. Pour plus d'informations sur l'ajout des notes, voir **Ajout de notes**. • **Protected** - Indique que la violation est protégée. La fonction Protect évite que les violations spécifiées soient retirées de la base de données après que la période de conservation se soit écoulée. Pour plus d'informations sur les violations protégées, voir **Protection des violations**. • **Inactive Offense** - Indique qu'il s'agit d'une violation inactive. Une violation devient inactive au bout de cinq jours après qu'elle ait reçu le dernier événement. En outre, toutes les violations deviennent inactives après la mise à niveau de votre logiciel QRadar Network Anomaly Detection. Une violation inactive ne peut pas redevenir active. Si de nouveaux événements sont détectés pour la violation, une nouvelle violation est créée et la violation inactive est conservée jusqu'à ce que la durée de conservation de la violation soit écoulée. Vous pouvez effectuer les actions suivantes sur les violations inactives: protéger, indiquer pour suivi, ajouter des notes, et affecter aux utilisateurs. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Flag	• Page By Source IP Details • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Destination IP - List of Sources • Page By Network Details • Page By Network - List of Sources • Page By Network - List of Local Destinations	Indique l'action menée sur l'adresse IP source, l'adresse IP cible ou sur le réseau. Par exemple si un indicateur s'affiche, la violation est l'adresse IP source pour le suivi. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Flows	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique le nombre de flux de la violation. ***Remarque :*** *Si la colonne Flows affiche N/A, la violation peut avoir une date de début qui précède la date où vous avez effectué une mise à niveau vers QRadar Network Anomaly Detection 7.1.0 (MR2).*
Group	• Tableau Offense Source, si le type de violation est Log Source • Tableau Top 5 Log Sources	Indique à quel groupe la source de journal appartient.
Group(s)	Tableau Offense Source, si le type de violation est Rule	Indique le groupe de règles auquel la règle appartient.
High Level Category	Tableau Offense Source, si le type de violation est Event Name	Indique la catégorie de haut niveau de l'événement. Pour plus d'information sur les catégories de haut niveau, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Host Name	Tableau Offense Source, si le type de violation est Source IP ou Destination IP	Indique le nom d'hôte associé à l'adresse IP source ou cible. Si aucun nom d'hôte n'est identifié, cette zone indique Unknown.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Host Name	Tableau Offense Source, si le type de violation est Hostname	Indique le nom d'hôte associé au flux qui a créé la violation.
ID	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses	Indique le numéro d'identification unique que QRadar Network Anomaly Detection affecte à la violation.
IP	• Tableau Offense Source, si le type de violation est Source IP • Page Source Details	Indique l'adresse IP source associée à l'événement ou au flux qui a créé la violation.
IP/DNS Name	Page Destination	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 *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
IPv6	Tableau Offense Source, si le type de violation est Source IPv6 ou Destination IPv6	Indique l'adresse IPv6 associée à l'événement ou au flux qui a créé la violation.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Last Event/Flow	• Page All Offenses • Page My Offenses • Page By Source IP - List of Local Destinations • Tableau Top 5 Source IPs • Page By Source IP Details • Page By Network - List of Sources • Tableau Top 5 Destination IPs • Page By Destination IP Details • Page By Destination IP - List of Sources • Page By Network - List of Local Destinations • Tableau Top 5 Categories	Indique le temps écoulé depuis que le dernier événement ou flux a été observé pour la violation, la catégorie, l'adresse IP source ou cible.
Last event/flow seen on	Page Source Details	Indique la date et l'heure du dernier événement ou flux générés associés à l'adresse IP source.
Last Event/Flow Time	Tableau Offense Source, si le type de violation est Log Source	Indique la dernière date et heure où le nom de source de journal a été observé sur le système.
Last Known Group	Tableau Offense Source, si le type de violation est Username, Source MAC Address, Destination MAC Address ou Hostname	Indique le groupe actuel auquel appartiennent l'utilisateur, l'adresse MAC ou le nom d'hôte. Si aucun groupe n'est actuellement associé, la valeur de cette zone est Unknown. ***Remarque :*** *Cette zone n'affiche pas les informations historiques.*
Last Known Host	Tableau Offense Source, si le type de violation est Username, Source MAC Address ou Destination MAC Address	Indique l'hôte en cours auquel est associé l'utilisateur ou l'adresse MAC. Si aucun hôte n'est identifié, cette zone indique Unknown. ***Remarque :*** *Cette zone n'affiche pas les informations historiques.*
Last Known IP	Tableau Offense Source, si le type de violation est Username, Source MAC Address, Destination MAC Address ou Hostname	Indique l'adresse IP actuel de l'utilisateur, l'adresse MAC ou le nom d'hôte. Si aucune adresse IP n'est identifiée, cette zone indique Unknown. ***Remarque :*** *Cette zone n'affiche pas les informations historiques.*

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Last Known MAC	Tableau Offense Source, si le type de violation est Username ou Hostname	Indique la dernière adresse MAC connue de l'utilisateur ou du 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 Machine	Tableau Offense Source, si le type de violation est Username, Source MAC Address, Destination MAC Address ou Hostname	Indique le nom de machine actuel associé à l'utilisateur, à l'adresse MAC ou au 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 Username	Tableau Offense Source, si le type de violation est Source MAC Address, Destination MAC Address ou Hostname	Indique l'utilisateur en cours de l'adresse MAC ou du nom d'hôte. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown. ***Remarque :*** *Cette zone n'affiche pas les informations historiques.*
Last Observed	Tableau Offense Source, si le type de violation est Username, Source MAC Address, Destination MAC Address ou Hostname	Indique la dernière date et heure où l'utilisateur, l'adresse MAC ou le nom d'hôte a été observé sur le système.
Last Packet Time	Tableau Last 10 Flows	Indique la date et l'heure d'envoi du dernier paquet pour le flux.
Local Destination Count	Tableau Top 5 Categories Page By Category Details	Indique le nombre d'adresses IP cible locales associées à laatégorie.
Local Destination(s)	Page Source Details	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.
Location	• Tableau Offense Source, si le type de violation est Source IP ou Destination IP • Tableau Top 5 Source IPs • Page By Source IP Details • Page Source Details • Page By Destination IP - List of Sources • Page By Network - List of Sources	Indique l'emplacement réseau de l'adresse IP source ou cible. Si l'emplacement est local, vous pouvez cliquer sur le lien pour afficher les réseaux.
Log Source	Tableau Last 10 Events	Indique la source du journal qui a détecté l'événement.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Log Source Identifier	Tableau Offense Source, si le type de violation est Log Source	Indique le nom d'hôte de la source de journal.
Log Source Name	Tableau Offense Source, si le type de violation est Log Source	Indique le nom de la source de journal, comme indiqué dans le tableau des sources de journal, associé à l'événement qui a créé la violation. ***Remarque :*** *Les informations affichées pour les violations 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, consultez le guide d'utilisation IBM Security QRadar Log Sources*
Log Sources	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique les sources de journal associées à la violation. Si plusieurs sources de journal sont associées à la violation, cette zone indique Multiple et le nombre de sources de journal.
Low Level Category	Tableau Offense Source, si le type de violation est Event Name	Indique la catégorie de bas niveau de l'événement. Pour plus d'information sur les catégories de bas niveau, consultez le gui de d'administration *IBM Security QRadar Network Anomaly Detection*.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
MAC	• Tableau Offense Source, si le type de violation est Source IP ou Destination IP • Tableau Top 5 Source IPs • Tableau Top 5 Destination IPs • Page By Source IP Details • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Page By Network - List of Local Destinations	Indique l'adresse MAC de l'adresse IP source ou cible lorsque la violation a commencé. Si l'adresse MAC est inconnue, cette zone indique Unknown.
MAC Address	Tableau Offense Source, si le type de violation est Source MAC Address ou Destination MAC Address	Indique l'adresse MAC associée à l'événement ou au flux qui a créé la violation. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown.
Magnitude	• Page All Offenses • Page My Offenses • Tableau Offense • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses • Tableau Top 5 Categories • Tableau Last 10 Events • Page By Network Details • Page Network	Indique l'importance relative de la violation, la catégorie, l'événement ou le réseau. La barre d'ampleur fournit une représentation visuelle de toutes les variables corrélées. Les variables comprennent Relevance, Severity et Credibility. Déplacez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'ampleur calculée. Pour plus d'informations sur la pertinence, la gravité et la crédibilité, voir le **Glossaire**.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Magnitude	• Tableau Offense Source, si le type de violation est Source IP ou Destination IP • Tableau Top 5 Source IPs • Tableau Top 5 Destination IPs • Page By Source IP Details • Page Source Details • Page By Source IP - List of Local Destinations • Page Destination • Page By Destination IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Page By Network - List of Local Destinations	Indique l'importance relative de l'adresse IP source ou cible. La barre d'ampleur fournit une représentation visuelle de la valeur du risque CVSS de l'actif associé à l'adresse IP. Déplacez votre souris sur la barre d'ampleur pour afficher l'ampleur calculée. Pour plus d'informations sur CVSS, voir le **Glossaire**.
Name	• Tableau Top 5 Log Sources • Tableau Top 5 Users • Tableau Top 5 Categories • Page Network	Indique le nom du de la source de journal, de l'utilisateur, de la catégorie, de l'adresse IP ou du nom du réseau.
Network	Page By Network Details	Indique le nom du réseau.
Network(s)	Tableau Offense	Indique le réseau de destination de la violation. Si la violation 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 la violation dispose de plusieurs réseaux de destination, le terme Multiple s'affiche. Cliquez sur le lien pour afficher des détails supplémentaires.
Notes	• Tableau Offense Source, si le type de violation est Rule • Tableau Last 5 Notes	Indique les notes de la règle.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Offense Count	Page By Category Details	Indique le nombre de violations actives dans chaque catégorie. Les violations actives sont des violations qui n'ont pas été masquées ou fermées. Si la page By Category Details contient le filtre **Exclude Hidden Offenses**, le nombre de violations qui s'affichent dans le paramètre **Offense Count** peuventne pas être correctes. Pour afficher le compte total dans le panneau By Category, cliquez sur **Clear Filter** à côté du filtre **Exclude Hidden Offenses** sur la page By Category Details.
Offense Source	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique des informations sur la source de la violation. L'information qui s'affiche dans la zone **Offense Source** dépend du type de violation. Par exemple, si le type de violation est Source Port, la zone **Offense Source** affiche le port source de l'événement qui a créé la violation.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Offense Type	• Page All Offenses • Page My Offenses • Tableau Offense • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique le type de violation. Le type de violation est déterminé par la règle qui a créé la violation. Par exemple, si le type de violation est l'événement source du journal, la règle qui a généré la violation est corrélée aux événements en fonction du périphérique qui a détecté l'événement. Les types de violation incluent : • 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 Le type de violation détermine le type d'information qui s'affiche sur le panneau récapitulatif de la source de violation.
Offense(s)	• Page Source Details • Page Destination	Indique les noms des violations associées à l'adresse IP source ou cible. Pour afficher des informations supplémentaires à propos de la violation, cliquez sur le nom ou le terme qui s'affiche. Si plusieurs violations existent, le terme Multiple s'affiche.
Offense(s) Launched	Page Network	Indique les violations lancées à partir du réseau. Si plusieurs violations sont responsables, cette zone indique Multiple et le nombre de violations.
Offense(s) Targeted	Page Network	Indique les violations visées par le réseau. Si plusieurs violations sont responsables, cette zone indique Multiple et le nombre de violations.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Offenses	• Tableau Offense Source, si le type de violation est Source IP, Destination IP, Event Name, Username, Source MAC Address ou Destination MAC Address, Log Source, Hostname, Source Port ou Destination Port, Source IPv6 ou Destination IPv6, Source ASN ou Destination ASN, Rule, App ID • Tableau Top 5 Source IPs • Tableau Top 5 Destination IPs • Tableau Top 5 Log Sources • Tableau Top 5 Users • Page By Source IP Details • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Page By Network - List of Local Destinations	Indique le nombre de violations associées à l'adresse IP source, à l'adresse IP cible, au nom d'événement, au nom d'utilisateur, à l'adresse MAC, à la source de journal, au nom d'hôte, au port, à l'adresse IPv6, à ASN, à la règle ou à l'application. Cliquez sur le lien pour afficher plus de détails.
Offenses Launched	Page By Network Details	Indique le nombre de violations provenant du réseau.
Offenses Targeted	Page By Network Details	Indique le nombre de violations destinées au réseau.
Port	Tableau Offense Source, si le type de violation est Source Port ou Destination Port	Indique l'adresse port associée à l'événement ou au flux qui a créé la violation.
Relevance	Tableau Offense	Indique l'importance relative de la violation.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Response	Tableau Offense Source, si le type de violation est Rule	Indique le type de réponse pour la règle.
Rule Description	Tableau Offense Source, si le type de violation est Rule	Indique le récapitulatif des paramètres de la règle.
Rule Name	Tableau Offense Source, si le type de violation est Rule	Indique le nom de la règle associée à l'événement ou au flux qui a créé la violation. ***Remarque :*** *L'information affichée pour les violations de règles est dérivée de l'onglet Rules. Pour plus d'information sur les règles, consultez le guide d'administration IBM Security QRadar Network Anomaly Detection.*
Rule Type	Tableau Offense Source, si le type de violation est Rule	Indique le type de règle pour la violation.
Severity	• Tableau Offense Source, si le type de violation est Event Name • Tableau Offense	Indique la gravité de l'événement ou de la violation. La gravité précise le niveau de menace que constitue une violation 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 la violation. Par exemple, une attaque Denial of Service (DoS) dispose d'une gravité de 10, ce qui indique une occurrence grave.
Source Count	Page By Category Details	Indique le nombre d'adresses IP source associées aux violations dans la catégorie. Si une adresse IP source est associée à des violations dans cinq différentes catégories de bas niveau, l'adresse IP source n'est comptée qu'une seule fois.
Source IP	• Page By Source IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Tableau Top 5 Source IPs • Tableau Last 10 Flows	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 *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
Source IP(s)	Tableau Offense	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 **Contrôle des violations regroupées par IP source**.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Source IPs	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	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 plusieurs adresses IP source sont associées à la violation, cette zone indique Multiple et le nombre d'adresses IP source. 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, consultez le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Source IPs	Page By Network Details	Indique le nombre d'adresses IP source associées au réseau.
Source Port	Tableau Last 10 Flows	Indique le port source du flux.
Source(s)	• Tableau Top 5 Destination IPs • Page By Source IP - List of Local Destinations • Page By Destination IP Details	Indique le nombre d'adresses IP source de l'adresse IP cible.
Source(s)	• Page Destination • Page Network	Indique les adresses IP source de la violation associée à l'adresse IP cible ou au 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 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.
Source(s)	Page By Network - List of Local Destinations	Indique le nombre d'adresses IP source associées à l'adresse cible.
Start	Tableau Offense	Indique la date et l'heure du premier événement ou flux de la violation.
Start Date	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique la date et l'heure du premier événement ou flux associé à la violation.
Status	Tableau Offense Source, si le type de violation est Log Source	Indique le statut de la source de journal.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Status	Tableau Offense	Affiche des icônes pour indiquer l'état d'une violation. Les icônes d'état incluent : • **Inactive Offense** - Indique qu'il s'agit d'une violation inactive. Une violation devient inactive au bout de cinq jours après qu'elle ait reçu le dernier événement. En outre, toutes les violations deviennent inactives après la mise à niveau de votre logiciel QRadar Network Anomaly Detection. Une violation inactive ne peut pas redevenir active. Si de nouveaux événements sont détectés pour la violation, une nouvelle violation est créée et la violation inactive est conservée jusqu'à ce que la durée de conservation de la violation soit écoulée. Vous pouvez effectuer les actions suivantes sur les violations inactives : protect, flag for follow up, add notes et assign to users. • **Hidden Offense** - Indique que la violation est masquée dans la page All Offenses. Les violations masquées sont visibles sur la page All Offenses uniquement si vous effectuez une recherche sur les violations masquées. Pour plus d'informations sur les violations masquées, voir **Masquage des violations**. • **User** - Indique que la violation a été affectée à un utilisateur. Lorsqu'une violation est affectée à un utilisateur, la violation est affichée sur la page My Offenses appartenant à cet utilisateur. Pour plus d'informations sur l'affectation des violations aux utilisateurs, voir **Affectation des violations aux utilisateurs**. • **Protected** - Indique que la violation est protégée. La fonction Protect évite que les violations spécifiées soient retirées de la base de données après que la période de conservation se soit écoulée. Pour plus d'informations sur les violations protégées, voir **Protection des violations**. • **Closed Offense** - Indique que la violation a été fermée. Pour plus d'informations sur la fermeture des violations, voir **Fermeture des violations**. Déplacez votre souris sur l'icône pour afficher des informations supplémentaires.
Time	• Tableau Last 10 Events • Tableau Last 10 Events (Anomaly Events)	Indique la date et l'heure de la détection du premier événement dans l'événement normalisé. Cette date et heure est spécifiée par le périphérique qui a détecté l'événement.
Time	Tableau Top 5 Annotations	Indique la date et l'heure de création de l'annotation.
Total Bytes	Tableau Last 10 Flows	Indique le nombre total d'octets du flux.
Total Events/Flows	• Tableau Top 5 Log Sources • Tableau Top 5 Users	Indique le nombre total d'événements de la source de journal ou de l'utilisateur.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
User	• Tableau Offense Source, si le type de violation est Source IP ou Destination IP • Tableau Top 5 Source IPs • Tableau Top 5 Destination IPs • Page By Source IP Details • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Page By Network - List of Local Destinations	Indique l'utilisateur associé à une adresse IP source ou cible. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
Username	Tableau Offense Source, si le type de violation est Username	Indique le nom d'utilisateur associé à l'événement ou au flux qui a créé la violation. ***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* ***Assets*** *au lieu du nom d'utilisateur associé à l'événement ou au flux ayant créé la violation.*
Username	Tableau Last 5 Notes	Indique l'utilisateur qui a créé la note.
Users	• Page All Offenses • Page My Offenses • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses	Indique les noms d'utilisateur associés à la violation. Si plusieurs noms d'utilisateur sont associés à la violation, cette zone indique Multiple et le nombre de noms d'utilisateur. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
View Offenses	• Page By Source IP Details • Page By Destination IP Details	Sélectionnez une option dans cette zone de liste pour filtrer les violations que vous souhaitez afficher sur cette page. Vous pouvez consulter toutes les violations ou filtrer les violations en fonction d'un intervalle. A partir de la zone de liste, vous pouvez sélectionner l'intervalle que vous souhaitez filtrer.

Tableau 3-3 Paramètres des violations (suite)

Paramètre	Emplacement	Description
Vulnerabilities	Tableau Offense Source, si le type de violation est Source IP ou Destination IP	Indique le nombre de vulnérabilités identifiées associées à l'adresse IP source ou cible. Cette valeur inclut également le nombre de vulnérabilités actives et passives.
Vulnerabilities	Page By Destination IP - List of Sources	Indique si l'adresse IP source dispose de vulnérabilités.
Vulnerability	• Tableau Top 5 Source IPs • Page By Source IP Details • Page By Network - List of Sources • Tableau Top 5 Destination IPs • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Network - List of Local Destinations	Indique si l'adresse IP source ou cible dispose de vulnérabilités.
Weight	• Tableau Top 5 Source IPs • Tableau Top 5 Destination IPs • Page By Source IP - List of Local Destinations • Page By Source IP Details • Page By Destination IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Page By Network - List of Local Destinations • Tableau Top 5 Annotations	Indique la pondération de l'adresse IP source, de l'adresse IP cible ou de l'annotation. La pondération d'une adresse IP est attribuée à l'onglet **Assets**. Pour plus d'informations, voir **Gestion des actifs**.

4 RECHERCHE D'ACTIVITÉ DE JOURNAL

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

Présentation de l'onglet Log Activity

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

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

Barre d'outils de l'onglet Log Activity

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

Tableau 4-1 Log Activity tab toolbar options

Option	Description
Recherche	Cliquez sur **Search** pour effectuer des recherches avancées sur les événements. Les options incluent : • **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 recherche. Pour plus d'informations sur la fonctionnalité de recherche, voir **Recherches de données**.
Recherches rapides	Dans cette zone de liste, vous pouvez exécuter des recherches précédemment enregistrées. Les options sont affichées dans la zone de liste **Quick Searches** uniquement lorsque vous avez enregistré les critères de recherche qui spécifient l'option **Include in my Quick Searches**.
Ajout de filtre	Cliquez sur **Add Filter** pour ajouter un filtre aux résultats de recherche en cours.
Critère de sauvegarde	Cliquez sur **Save Criteria** pour enregistrer les critères de recherche en cours.

Tableau 4-1 Log Activity tab toolbar options (suite)

Option	Description
Résultats de sauvegarde	Cliquez sur **Save Results** pour enregistrer les résultats de recherche en cours. Cette option ne s'affichent qu'une fois la recherche terminée. Cette option est désactivée en mode de diffusion en flux.
Annulation	Cliquez sur **Cancel** pour annuler une recherche en cours. Cette option est désactivée en mode de diffusion en flux.
Faux positif	Cliquez sur **False Positive** pour ouvrir la fenêtre False Positive Tuning, qui vous permet d'ajuster les événements connus pour être des faux positifs à partir de la création de violations. Pour plus d'informations sur les faux positifs, voir le **Glossaire**. Cette option est désactivée en mode de diffusion en flux. Pour plus d'informations sur le réglage de faux positifs, voir **Réglage des faux positifs**.

Tableau 4-1 Log Activity tab toolbar options (suite)

Option	Description
Règles	L'option Règles est visible uniquement si vous avez la permission d'afficher des règles. Cliquez sur **Rules** afin de configurer les règles d'événements personnalisés. Les options incluent : • **Rules** - Sélectionnez cette option pour afficher ou créer une règle. Si vous avez la permission d'afficher des règles, la page de synthèse de l'assistant de Règles s'affiche. Si vous avez la permission de conserver des règles personnalisées, l'assistant de Règles s'affiche et vous pouvez modifier la règle. ***Remarque :*** *Les options de la règle de détection des anomalies ne sont visibles que si vous avez la permission de type* ***Log Activity > Maintain Custom Rules****.* Pour activer les options de la règle de détection des anomalies (Règle de seuil, Règle comportementale, et Règle d'anomalie), vous devez enregistrer les critères de recherche agrégées car les critères de recherche déjà enregistrés indiquent les paraxmètres requis. • **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 en indiquant que plus de 220 clients ne peuvent pas se connecter au serveur entre 08 et 17 heures, les règles génèrent une alerte lorsque le 221ème client tente de se connecter. Lorsque vous sélectionnez l'option **Add Threshold Rule**, l'Assistant de règles s'affiche, prérempli d'options appropriées pour la création d'une règle de seuil. • **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 de pourcentage de la période 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 un changement de plus de 40%, la règle génère une réponse. Lorsque vous sélectionnez l'option **Add Behavioral Rule**, l'Assistant de règles s'affiche, prérempli d'options appropriées pour la création d'une règle comportementale.

Tableau 4-1 Log Activity tab toolbar options (suite)

Option	Description
	• **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 de pourcentage de la période 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. Lorsque vous sélectionnez l'option **Add Anomaly Rule**, l'Assistant de règles s'affiche, prérempli d'options appropriées pour la création d'une règle d'anomalie. Pour plus d'informations sur les règles, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*

Tableau 4-1 Log Activity tab toolbar options (suite)

Option	Description
Actions	Cliquez sur **Actions** pour effectuer les actions suivantes : • **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 d'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 d'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 d'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 d'événements**. • **Delete** - Sélectionnez cette option pour supprimer un résultat de recherche. Voir **Gestion des résultats de recherche d'événements et de flux**. • **Notify** - Sélectionnez cette option pour spécifier que vous souhaitez recevoir une notification par courriel à l'issue des recherches sélectionnées. Cette option est activée uniquement pour les recherches en cours. ***Remarque :*** *Les options **Print**, **Export to XML** et **Export to CSV** sont désactivées en mode de diffusion en flux et lors de l'affichage des résultats de recherche partielle.*
Filtre rapide	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 d'événements. Une recherche de texte est exécutée sur le contenu d'événement pour déterminer lequel correspond à vos critères spécifiés. ***Remarque :*** *Lorsque vous cliquez sur la zone **Quick Filter**, une infobulle s'affiche, fournissant des informations sur la syntaxe à utiliser pour les critères de recherche. Pour plus d'informations sur la syntaxe, voir* **Syntaxe du filtre rapide**.

Syntaxe du filtre rapide

La fonctionnalité Quick Filter vous permet de rechercher des contenus d'événement à l'aide d'une chaîne de recherche de texte. La fonctionnalité Quick Filter est disponible dans les emplacements suivants de 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 d'événements actuellement affichée.
- **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 de filtre et entrer une chaîne de recherche de texte. Cela vous permet d'appliquer votre filtre rapide à la liste d'événements ou des flux actuellement affichée. Pour plus d'informations sur la boîte de dialogue Add Filter, voir **Syntaxe du filtre rapide**.
- **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 les critères de recherche, voir **Recherche d'événements ou de flux.**

Lorsque vous affichez des événements en mode temps réel (diffusion en flux) ou dernier intervalle, vous pouvez entrer uniquement des mots simples ou des phrases dans la zone **Quick Filter**. Lorsque vous affichez des événements à l'aide d'un intervalle de temps, suivez les instructions de syntaxe suivantes pour entrer 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. Par exemple, `"Firewall deny"`
- Les termes de recherche peuvent inclure des caractères génériques uniques ou multiples. Le terme de recherche ne peut pas commencer par un caractère générique. Par exemple, `F?rewall` ou `F??ew*`
- Termes de groupe utilisant des des 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 trouve 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 inversée pour indiquer que le caractère fait partie de votre terme de recherche : + - && || ! () {} [] ^ " ~ * ? : \. Par exemple : `"%PIX\-5\-304001"`

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
Filtrage	Sélectionnez cette option pour filtrer l'événement sélectionné, en fonction du paramètre sélectionné dans l'événement.
Faux positif	Sélectionnez cette option afin d'ouvrir la fenêtre False Positive, qui vous permet d'ajuster les événements connus pour être des faux positifs à partir de la créations des violations. Cette option est désactivée en mode de diffusion en flux. Voir **Réglage des faux positifs**.
Plus d'options :	Sélectionnez cette option pour rechercher une adresse IP ou un nom d'utilisateur. Pour plus d'informations sur la recherche d'une adresse IP, voir **Etude des adresses IP**. Pour plus d'informations sur la recherche d'un nom d'utilisateur, voir **Etude des noms d'utilisateurs**. ***Remarque :*** *Cette option n'est pas affichée en mode de diffusion en flux.*

Barre d'état

Lors de la diffusion en flux des événements, la barre d'état affiche le nombre moyen de résultats reçus par seconde. C'est le nombre de résultats de que la console a reçu avec succès provenant du Processeur d'événement. Si ce nombre est supérieur à 40 résultats par seconde, seulement 40 résultats s'affichent. Le reste s'accumule dans la mémoire tampon de 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 de résultats de recherche actuellement affichés dans l'onglet et le temps requis pour traiter les résultats de recherche.

Moniteur d'activités de journal

Par défaut, l'onglet **Log Activity** affiche les événements en mode diffusion en flux, vous permettant ainsi d'afficher des événements en temps réel. Pour plus d'informations sur le mode de diffusion en flux, voir **Affichage d'événements en mode diffusion en flux**. Vous pouvez spécifier un intervalle de temps différent pour filtrer les événements à l'aide de la zone de liste **View**.

Si vous avez déjà configuré les critères de recherche enregistré, les résultats de cette recherche s'affichent automatiquement lorsque vous accédez à l'onglet **Log Activity**. Pour plus d'informations sur la sauvegarde des critères de recherche, voir **Enregistrement des critères de recherche d'événements et de flux**.

Affichage d'événements en mode diffusion en flux

Le mode de diffusion en flux vous permet d'afficher les données d'événement entrant dans votre système. Ce mode vous fournit un affichage en temps réel de votre activité d'événement en cours en affichant les 50 derniers événements.

A propos de cette tâche

Si vous appliquez des filtres sur l'onglet **Log Activity** ou dans vos critères de recherche avant d'activer le mode de diffusion en flux, les filtres sont maintenus en mode de diffusion en flux. Toutefois, le mode de diffusion en flux ne prend pas en charge les recherches qui incluent des événements groupés. Si vous activez le mode de diffusion en flux sur des événements groupés ou des critères de recherche groupés, l'onglet **Log Activity** affiche les événements normalisés. Voir **Affichage d'événements normalisés**.

Lorsque vous souhaitez sélectionner un événement pour afficher les détails ou effectuer une action, vous devez mettre en pause le mode de diffusion en flux avant de cliquer deux fois sur un événement. Lorsque la diffusion en flux est mise en pause, les 1 000 derniers événements s'affichent.

Procédure

Etape 1 Cliquez surl'onglet **Log Activity**.

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

Pour obtenirdes informations sur les options de la barre d'outils, voir **Tableau 4-1**. Pour plus d'informations sur les paramètres affichés en mode diffusion en flux, voir **Tableau 4-7**.

Etape 3 Facultatif. Mettez en pause ou en lecture la diffusion en flux. Choisissez l'une des options suivantes :

- Pour sélectionner un enregistrement de l'événement, cliquez sur l'icône **Pause** pour mettre en pause le mode diffusion en flux.
- Pour redémarrer le mode diffusion en flux, cliquez sur l'icône **Play**.

Affichage d'événements normalisés

QRadar Network Anomaly Detection collecte des événements en format brut, puis normalise les événements pour un affichage dans l'onglet **Log Activity**.

A propos de cette tâche

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

Remarque : Si vous avez sélectionné un laps de temps à afficher, un graphique de séries temporelles s'affiche. Pour plus d'informations sur l'utilisation des graphiques de séries temporelles, voir **Présentation du graphique de séries temporelles**.

L'onglet **Log Activity** affiche les paramètres suivants lorsque vous affichez des événements normalisés :

Tableau 4-3 Onglet d'activitéde journal - Paramètrespar défaut (Normalisés)

Paramètre	Description
Filtres en cours	La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche. Pour effacer ces valeurs de filtre, cliquez sur **Clear Filter.** ***Remarque :*** *Ce paramètre s'affiche uniquement après avoir appliqué un filtre.*
Affichage	Dans cette zone de liste, vous pouvez sélectionner l'intervalle de temps que vous souhaitez filtrer.
Statistiques en cours	Lorsque le mode Real Time (diffusion en flux) ou Last Minute (actualisation automatique) n'est pas indiqué, les statistiques en cours s'affichent, y compris : ***Remarque :*** *Cliquez sur la flèche près de* ***Current Statistics*** *pour afficher ou masquer les statistiques* • **Total Results** - Indique le nombre total des résultats correspondant à vos critères de recherche. • **Data Files Searched** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total de fichiers de données compressés recherchés dans l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes Lorsque vous contactez le le service client pour identifier et résoudre certains problèmes, vous pouvez être invité à fournir des informations statistiques en cours.*
Graphiques	Affiche des graphiques configurables qui représentent les enregistrements correspondant à l'option d'intervalle de temps et de groupement. Cliquez sur **Hide Charts** si vous souhaitez masquer les graphiques lors de l'affichage. Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du mode Last Interval (actualisation automatique) ou au-dessus et une option de groupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir **Affichagedes violations associées**. ***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 désinstaller le bloqueur de publicités. Pour plus d'informations, voir la documentation de votre navigateur.*

Tableau 4-3 Onglet d'activitéde journal - Paramètrespar défaut (Normalisés) (suite)

Paramètre	Description
Icône de violation	Cliquez sur l'icône **Offenses** pour afficher les détails de la violation associée à cet événement. Pour plus d'informations, voir **Gestion des graphiques**.
Nom de l'événement	Indique le nom normalisé de l'événement.
Source de journal	Indique la source du journal ayant envoyé l'événement à QRadar Network Anomaly Detection. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources de journal.
Comptage d'événement	Indique le nombre total d'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.
Temps	Indique la date et le moment où QRadar Network Anomaly Detection a reçu l'événement.
Catégorie de niveau bas	Indique la catégorie de niveau bas associée à cet événement. Pour plus d'informations sur les catégories d'événement, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Adresse IP source	Indique l'adresse IP source de l'événement.
Port source	Indique le port source de l'événement.
Adresse IP de destination	Indique l'adresse IP de destination de l'événement.
Port de destination	Indique le port de destination de l'événement.
Nom d'utilisateur	Indique le nom d'utilisateur associé à cet événement. Les noms d'utilisateurs sont souvent disponibles dans les événements d'authentification connexes. Pour tous les autres types d'événements où le nom d'utilisateur n'est pas disponible, cette zone spécifie N/A.
Ampleur	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 les valeurs et l'ampleur calculées. Pour plus d'informations sur la crédibilité, la pertinence et la gravité, voir le **Glossaire**.

Procédure

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

Etape 2 A partir de 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.

Etape 4 Cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.

Etape 5 Cliquez deux foissur l'événement que vous souhaitez afficher plus en détails. Voir **Détails d'événement**.

Affichage d'événements bruts

Vous pouvez afficher des données d'événement brutes, qui sont des données d'événement non analysées provenant de a source de journal.

A propos de cette tâche

Lorsque vous affichez des données d'événement brutes, l'onglet **Log Activity** fournit les paramètres suivants pour chaque événement :

Tableau 4-4 Paramètres d'événement brut

Paramètre	Description
Filtres en cours	La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche. Pour effacer ces valeurs de filtre, cliquez sur **Clear Filter.** ***Remarque :*** *Ce paramètre s'affiche uniquement après avoir appliqué un filtre.*
Affichage	A partir de la zone de liste, sélectionnez un intervalle de temps durant lequel vous souhaitez filtrer.
Statistiques en cours	Lorsque le mode Real Time (diffusion en flux) ou Last Minute (actualisation automatique) n'est pas indiqué, les statistiques en cours s'affichent, y compris : ***Remarque :*** *Cliquez sur la flèche à côté de* ***Current Statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total des résultats correspondant à vos critères de recherche. • **Data Files Searched** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total de fichiers de données compressés recherchés dans l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le le service client pour identifier et résoudre certains problèmes, vous pouvez être invité à fournir des informations statistiques en cours.*

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

Paramètre	Description
Graphiques	Affiche des graphiques configurables qui représentent les enregistrements correspondant à l'option d'intervalle de temps et de groupement. Cliquez sur **Hide Charts** si vous souhaitez masquer les graphiques lors de l'affichage. Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du mode Last Interval (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**. ***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 désinstaller le bloqueur de publicités. Pour plus d'informations, voir la documentation de votre navigateur.*
Icône de violation	Cliquez sur cette icône pour afficher les détails de violation associée à cet événement. Pour plus d'informations, voir **Affichage des violations associées**.
Heure de début	Indique l'heure du premier événement telle que rapportée vers QRadar Network Anomaly Detection par la source de journal.
Source de journal	Indique la source de journal étant à l'origine de l'événement. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources de journal.
Contenu	Indique les informations de contenu d'événement d'origine au format UTF-8.

Procédure

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

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.

Etape 4 Cliquez deux foissur l'événement que vous souhaitezs afficher plus en détail. Voir **Détails d'événement**.

Affichage d'événements groupés

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

A propos de cette tâche

La zone de liste **Display** ne s'affiche pas en mode diffusion en flux car ce mode ne prend pas en charge les événements groupés. Si vous entrez le mode de diffusion en flux à l'aide d'un critère de recherche non groupé, cette option s'affiche.

La zone de liste Display fournit les options suivantes :

Tableau 4-5 Options d'événement groupés

Option de groupe	Description
Catégorie de niveau bas	Affiche une liste résumée des événements groupés par la catégorie de niveau bas de l'événement. Pour plus d'informations sur les catégories, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Nom de l'événement	Affiche une liste résumée d'événements groupés par le nom normalisé de l'événement.
Adresse IP de destination	Affiche une liste résumée d'événements groupés par l'adresse IP de destination de l'événement.
Port de destination	Affiche une liste résumée d'événements groupés par l'adresse du port de destination de l'événement.
Adresse IP source	Affiche une liste résumée d'événements groupés par l'adresse IP source de l'événement.
Règle personnalisée	Affiche une liste résumée d'événements groupés par la règle personnalisée associée.
Nom d'utilisateur	Affiche une liste résumée d'événements groupés par le nom d'utilisateur associé à l'événement.
Source de journal	Affiche une liste résumée d'événements groupés par les sources de journal qui envoient l'événement versQRadar Network Anomaly Detection.
Catégorie de niveau supérieur	Affiche une liste résumée d'événements groupés par la catégorie de niveau supérieur de l'événement. pour plus d'informations sur les catégories, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Réseau	Affiche une liste résumée d'événements groupés par le réseau associé à l'événement.
Port source	Affiche une liste résumée d'événements groupés par l'adresse du port source de l'événement.

Après avoir sélectionné une option à partir de la zone de liste **Display**, l'agencement de colonne de données dépend de l'option de groupe choisie. Chaque ligne dans le tableau d'événements représente un groupe d'événements. L'onglet **Log Activity** fournit les informations suivantes pour chaque groupe d'événement :

Tableau 4-6 Paramètres d'événement groupé

Paramètre	Description
Groupement par	Indique le paramètre sur lequel la recherche est groupée.
Filtres en cours	La partie supérieure du tableau affiche les détails du filtre appliqué aux résultats de la recherche. Pour effacer les valeurs de filtre, cliquez sur **Clear Filter**.

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

Paramètre	Description
Affichage	A partir de la zone de liste, sélectionnez un intervalle de temps durant lequel vous souhaitez filtrer.
Statistiques en cours	Lorsque le mode Real Time (diffusion en flux) ou Last Minute (actualisation automatique) n'est pas indiqué, les statistiques en cours s'affichent, y compris : ***Remarque :*** *Cliquez sur la flèche à côté de* ***Current Statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total des résultats correspondant à vos critères de recherche. • **Data Files Searched** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total de fichiers de données compressés recherchés dans l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le le service client pour identifier et résoudre certains problèmes, vous pouvez être invité à fournir des informations statistiques en cours.*

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

Paramètre	Description
Graphiques	Affiche des graphiques configurables qui représentent les enregistrements correspondant à l'option d'intervalle de temps et de groupement. Cliquez sur **Hide Charts** si vous souhaitez supprimer le graphique de votre affichage. Chaque graphique fournit une légende, qui est une référence visuelle pour vous aider à associer les objets de graphique aux paramètres qu'ils représente. En utilisant la fonctionnalité de légende, vous pouvez effectuer les actions suivantes : • Déplacez le pointeur de votre souris sur un élément de légende pour obtenir plus d'informations sur les paramètres qu'il représente. • Cliquez avec le bouton droit de la souris sur un élément de légende afin de mieux étudier ce dernier. pour plus d'informations sur les options du menu contextuel, voir **A propos de la détection des anomalies du réseau QRadar**. • Cliquez sur un élément de légende pour le masquer dans le graphique. Cliquez sur l'élément de légende de nouveau pour afficher l'élément masqué. Vous pouvez également cliquer sur l'élément de graphique correspondant pour masquer et afficher l'élément. • Cliquez sur **Legend** si vous souhaitez retirer la légende de l'affichage de votre graphique. ***Remarque :*** *Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du mode Last Interval (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**. ***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 désinstaller le bloqueur de publicités. Pour plus d'informations, voir la documentation de votre navigateur.*
Adresse IP source (Comptage unique)	Indique l'adresse IP de source associée à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone indique le terme Multiple et le nombre d'adresses IP.
Adresse IP de destination (Comptage unique)	Indique l'adresse IP de destination associée à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone indique le terme Multiple et le nombre d'adresses IP.
Port de destination (Comptage unique)	Indique les ports de destination associés à cet événement. S'il existe plusieurs ports associés à cet événement, cette zone indique le terme Multiple et le nombre de ports.
Nom de l'événement	Indique le nom normalisé de l'événement.

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

Paramètre	Description
Source de journal (Comptage unique)	Indique les sources de journal ayant envoyé l'événement vers QRadar Network Anomaly Detection. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources de journal.
Catégorie de niveau supérieur (Comptage unique)	Indique la catégorie de niveau supérieur de cet événement. S'il existe plusieurs catégories associées à cet événement, cette zone indiqsue le terme Multiple et le nombre de catégories. Pour plus d'informations sur les catégories, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Catégorie de niveau supérieur (Comptage unique)	Indique la catégorie de niveau bas de cet événement. S'il existe plusieurs catégories associées à cet événement, cette zone indique le terme Multiple et le nombre de catégories. Pour plus d'informations sur les catégories, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Protocole (Comptage unique)	Indique l'ID du protocole associé à cet événement. S'il existe plusieurs protocoles associés à cet événement, cette zone indique le terme Multiple et le nombre d'ID du protocole.
Nom d'utilisateur (Comptage unique)	Indique le nom d'utilisateur associé à cet événement, si possible. S'il existe plusieurs noms d'utilisateur associés à cet événement, cette zone indique le terme Multiple et le nombre de noms d'utilisateurs.
Ampleur (Maximum)	Indique l'ampleur maximale calculée pour les événements groupés. Les variables utilisées pour calculer l'ampleur incluent la crédibilité, la pertinence et la gravité. Pour plus d'informations sur la crédibilité, la pertinence et la gravité, voir le **Glossaire**.
Comptage d'événement (Somme)	Indique le nombre total d'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.
Comptage	Indique le nombre total d'événements normalisés dans ce groupe d'événements.

Procédure

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

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

Etape 3 A partir de la zone de liste **Display**, choisissez le paramètre sur lequel vous souhaitez grouper les événements. Voir **Tableau 4-5**.

Les groupes d'événement sont répertoriés. Pour plus d'informations sur les détails de groupe d'événements. Voir **Tableau 4-6**.

Etape 4 Pour afficher la page List of Events pour un groupe, cliquez deux foissur le groupe d'événement que vous souhaitez rechercher.

La page List of Events ne conserve pas les configurations de graphique définis dans l'onglet **Log Activity**. Pour plusd'informations sur les paramètres de la page List of Events, voir **Tableau 4-3**.

Etape 5 Pour afficher les détails d'un événement, cliquezdeux fois sur l'événement que vous souhaitez rechercher. Pourplus d'informations sur les détails d'événement, voir **Tableau 4-7**.

Détails d'événement

Vous pouvez afficher une liste d'événement en plusieurs modes, y compris le mode diffusion en flux ou groupes d'événement. Peu importe le mode choisi pour l'affichage d'événements, vous pouvez localiser et afficher les détails d'un événement unique. La page des détails d'événement fournit les informations suivantes :

Tableau 4-7 Détails relatifs à l'événement

Paramètre	Description
Informations relatives à l'événement	
Nom de l'événement	Indique le nom normalisé de l'événement.
Catégorie de niveau bas	Indique la catégorie de niveau bas de cet événement. Pour plus d'informations sur les catégories, voir le Guide d'administration*IBM Security QRadar Network Anomaly Detection*.
Description d'événement	Indique une description de l'événement, si disponible.
Ampleur	Indique l'ampleur de cet événement. Pour plus d'information sur l'ampleur, voir le **Glossaire**.
Pertinence	Indique la pertinence de cet événement. Pour plus d'informations sur la pertinence, voir le **Glossaire**.
Gravité	Indique la gravité de cet événement. Pour plus d'informations sur la gravité, voir le **Glossaire**.
Crédibilité	Indique la crédibilité de cet événement. Pour plus d'informations sur la crédibilité, voir le **Glossaire**.
Nom d'utilisateur	Indique le nom d'utilisateur associé à cet événement, si disponible.
Heure de début	Indique l'heure à laquelle l'événement a été reçu à partir de la source du journal.
Heure d'archivage	Indique l'heure à laquelle l'événement a été enregistré dans la base de données QRadar Network Anomaly Detection.
Log Source Time	Indique l'heure système telle que rapportée par la source de journal dans le contenu d'événement.
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 Guide d'administration*IBM Security QRadar Network Anomaly Detection*. Cliquez sur l'icône **Anomaly** pour afficher les résultats de la recherche sauvegardés ayant entraîné la génération de cet événement par la règle de détection des anomalies.	
Description de la règle	Indique la règle de détection des anomalies ayant généré cet événement.
Description d'anomalie	Indique une description du comportement anormal qui a été détecté par la règle de détection des anomalies.
Valeur d'alerte d'anomalies	Indique la valeur d'alerte d'anomalie.
Informations sur la source et la destination	

Tableau 4-7 Détails relatifs à l'événement (suite)

Paramètre	Description
Adresse IP source	Indique l'adresse IP source de l'événement.
Adresse IP de destination	Indique l'adresse IP de destination de l'événement.
Nom de l'actif source	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**.
Nom de l'actif de destination	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.**
Port source	Indique le port source de cet événement.
Port de destination	Indique le port de destination de cet événement.
Adresse IP source Pre NAT	Pour un pare-feu ou un autre périphérique capable de traduire des adresses réseau (NAT), ce paramètre indique l'adresse IP source avant l'application des valeurs NAT. NAT traduit une adresse IP dans un réseau vers une adresse IP différente sur un autre réseau.
Adresse IP de destination Pre NAT	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre indique l'adresse IP de destination avant l'application des valeurs NAT.
Port source Pre NAT	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre indique le port source avant l'application des valeurs NAT.
Port de destination Pre NAT	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre indique le port de destination avant l'application des valeurs NAT.
Adresse IP source Post NAT	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre indique l'adresse IP source avant l'application des valeurs NAT.
Adresse IP de destination Post NAT	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP de destination avant l'application des valeurs NAT.
Port source Post NAT	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre indique le port source avant l'application des valeurs NAT.
Port de destination Post NAT	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre indique le port de destination avant l'application des valeurs NAT.
IPv6 Source	Indique l'adresse IPv6 source de l'événement.
Adresse IPv6 de destination	Indique l'adresse IPv6 de destination de l'événement.
Adresse MAC source	Indique l'adresse MAC source de l'événement.
Adresse MAC de destination	Indique l'adresse MAC de destination de l'événement.

Tableau 4-7 Détails relatifs à l'événement (suite)

Paramètre	Description
Informations sur le contenu	
Contenu	Indique le contenu payload de l'événement. Cette zone fournit trois onglets permettant d'afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur **UTF**. • Hexadecimal - Click **HEX**. • Base64 - Cliquez sur **Base64**.
Informations supplémentaires	
Protocole	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 du mappage d'événement**.
Source de journal	Indique la source de journal ayant envoyé l'événement à QRadar Network Anomaly Detection. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources de journal.
Comptage d'événement	Indique le nombre total d'événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs événements du même type pour la même source et adresse IP de destination sont détectés dans un court laps de temps.
Règles personnalisées	Indique les règles personnalisées qui correspondent à cet événement. pour plus d'informations sur les règles, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Règles personnalisées partiellement correspondantes	Indique les règles personnalisées qui correspondent partiellement à cet événement. Pour plus d'informations sur les règles, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection.*
Annotations	Indique l'annotation pour cet événement. Les annotations sont des descriptions texte que les règles peuvent ajouter automatiquement aux événements en tant que faisant partie d'une réponse de règle. Pour plus d'informations sur les règles, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Identity Information - QRadar Network Anomaly Detection collecte des informations sur l'identité, le cas échéant, à partir de messages source de journal. Les informations sur l'identité fournissent des détails supplémentaires au sujet des actifs sur votre réseau. Les sources de journal génèrent des informations sur l'identité uniquement si le message de journal envoyé vers QRadar Network Anomaly Detection contient une adresse IP et au moins un des éléments suivants : user name or MAC address. Toutes les sources de journal ne génèrent pas des informations sur l'identité. Pour plus d'informations sur l'identité et les actifs, voir **Gestion des actifs**.	
Nom d'utilisateur d'identité	Indique le nom d'utilisateur de l'actif associé à cet événement.

Tableau 4-7 Détails relatifs à l'événement (suite)

Paramètre	Description
Adresse IP d'identité	Indique l'adresse IP de l'actif associée à cet événement.
Nom d'identité Net Bios	Indique le nom du système d'entrée/sortie de la base du réseau (Net Bios) de l'actif associé à cet événement.
Zone d'extension d'identité	Indique des informations supplémentaires sur l'actif associé à cet événement. Le contenu de cette zone est un texte défini par l'utilisateur et repose sur les périphériques de votre réseau qui peuvent fournir des informations sur l'identité. On peut citer : l'emplacement physique des périphériques, des politiques pertinentes, des commutateurs de réseau et des noms de port.
Avoir une identité (Indicateur)	Indique True si QRadar Network Anomaly Detection dispose d'informations sur l'identité pour l'actif associé à cet événement. Pour plus d'informations sur les périphériques permettant d'envoyer des informations sur l'identité, voir le Guide de configuration *IBM Security QRadar DSM*.
Nom d'hôte de l'identité	Indique le nom d'hôte de l'actif associé à cet événement.
Adresse MAC d'identité	Indique l'adresse MAC de l'actif associé à cet événement.
Nom de groupe de l'identité	Indique le nom du groupe de l'actif associé à cet événement.

Barre d'outils des détails d'événement

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

Tableau 4-8 Barre d'outilsdes détails d'événement

Fonction	Description
Retour à la liste d'événement	Cliquez sur **Return to Event List** pour retourner à la liste d'événements.
Violation	Cliquez sur **Offense** pour afficher les violations associées à cet événement.
Anomalie	Cliquez sur **Anomaly** pour afficher les résultats de recherche enregistrés ayant provoqué la génération de cet événement par la règle de détection des anomalies. ***Remarque :*** *Cette icône s'affiche uniquement si cet événement a été généré par une règle de détection des anomalies.*
Mappage d'événement	Cliquez sur **Map Event** pour modifier le mappage d'événement. Pour plus d'informations, voir **Modification du mappage d'événement**.
Faux positif	Cliquez sur **False Positive** pour ajuster QRadar Network Anomaly Detection à empêcher les événements du faux positif de générer les violations.

Tableau 4-8 Barre d'outilsdes détails d'événement (suite)

Fonction	Description
Propriété d'extraction	Cliquez sur **Extract Property** pour créer une propriété d'événement personnalisé à partir de l'événement sélectionné. Pour plus d'informations, voir **Propriétés personnalisées d'événements et de flux**.
Précédent	Cliquez sur **Previous** pour afficher l'événement précédent dans la liste d'événement.
Suivant	Cliquez sur **Next** pour afficher l'événement suivant dans la liste d'événement.
Données PCAP	***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**. 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 d'informations PCAP**. • **Download PCAP File** - Sélectionnez cette option pour télécharger le fichier PCAP dans votre système de bureau. Pour plus d'informations, voir **Téléchargement du fichier PCAP sur votre système de bureau**.
Imprimer	Cliquez sur **Print** pour imprimer les détails d'événement.

Affichage des violations associées

A partir de l'onglet **Log Activity**, vous pouvez afficher la violation associée à l'événement.

A propos de cette tâche

Si un événement correspond à une règle, une violation peut être générée dans l'onglet **Offenses**. 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 violations, voir **Gestion des violations**.

Lorsque vous affichez une violation à partir de l'onglet **Log Activity**, il se peut que la violation ne s'affiche pas si le Magistrate n'a pas encore enregistré la violation associée à l'événement sélectionnée sur le disque ou si la violation a été purgé de la base de données. Si cela se produit, le système vous prévient.

Procédure

Etape 1 Cliquez surl'onglet **Log Activity**.

Etape 2 Facultatif. Si vous affichez des événements en mode diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause le mode.

Etape 3 Cliquez sur l'icône **Offense** près de l'événement que vous souhaitez rechercher.

Etape 4 Affichez la violation associée.

Modification du mappage d'événement

Vous pouvez mapper manuellement un événement normalisé ou brut à une catégorie de niveau bas ou supérieur (ou QID). Cette action manuelle permet à QRadar Network Anomaly Detection de mapper des événements de source de journal inconnus à des événements connusQRadar Network Anomaly Detection afin qu'ils puissent être classés et traités de façon adéquate.

A propos de cette tâche

Aux fins de normalisation, QRadar Network Anomaly Detection mappe automatiquement les événements à partir des sources de journal vers des catégories de niveau bas et supérieur. Pour plus d'informations sur les catégories, voir le Guide d'administration *IBM Security QRadar Network Anomaly Detection*.

Lorsque QRadar Network Anomaly Detection reçoit des événements à partir des sources que le système ne parvient pas à catégoriser, QRadar Network Anomaly Detection categorise 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 de journal du vendeur peuvent mettre à jour leur logiciel avec des versions de maintenance pour prendre en charge de nouveaux événements que QRadar Network Anomaly Detection ne prend pas en charge.

Remarque : l'icône **Map Event** est désactivée pour des événements lorsque la catégorie de niveau supérieur est de type SIM Audit ou lorsque le type de source de journal est Simple Object Access Protocol (SOAP).

Procédure

Etape 1 Cliquez surl'onglet **Log Activity**.

Etape 2 Facultatif. Si vous affichez des événements en mode diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause le mode.

Etape 3 Cliquez deux fois sur l'événement que vous souhaitez mapper.

Etape 4 Cliquezsur **Map Event**.

Etape 5 Si vous connaissez le QID que vous souhaitez mapper à cet événement, entrez le QID dans la zone **Enter QID**. Allez à **Etape 7**.

Etape 6 Si vous ne connaissez pas le QID que vous souhaitez mapper à cet événement, vous pouvez rechercher QID particulier :

a Choisissez l'une des options suivantes :

- Pour rechercher un QID par catégorie, sélectionnez la catégorie de niveau supérieur à partir de la zone de liste **High-Level Category**.
- Pour rechercher un QID par catégorie, sélectionnez la catégorie de niveau bas à partir 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 à partir de la zone de liste **Log Source Type**.
- Pour rechercher un QID par nom, entrez un 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 7 Cliquez sur **OK**.

Réglage des faux positifs

Vous pouvez utiliser la fonctionnalité False Positive Tuning pour éviter la création de violations par des événements de faux positifs. Il est possible d'ajuster des événements de faux positifs à partir de la liste d'événement ou de la page de détails d'événement.

A propos de cette tâche

Vous devez avoir des droits appropriés pour créer des règles personnalisées afin de régler les faux positifs. Pour plus d'informations sur les règles, voir le Guide d'administration*IBM Security QRadar Network Anomaly Detection*. Pour plus d'informations sur les faux positifs, voir le **Glossaire**.

Procédure

Etape 1 Cliquez surl'onglet **Log Activity**.

Etape 2 Facultatif. Si vous affichez des événements en mode diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause le mode.

Etape 3 Sélectionnez l'événement que vous souhaitez régler.

Etape 4 Cliquez sur **False Positive**.

Etape 5 Dans le volet de propriété Event/Flow de la fenêtre False Positive, sélectionnezl'une des options suivantes :

- Les valeurs Event/Flow dotées d'un QID spécifique de <Event>
- Toutes les valeurs Event/Flow dotées d'une catégorie de niveau bas du <Event>
- Toutes les valeurs Event/Flow dotées d'une catégorie de niveau supérieur du <Event>

Etape 6 Dans le panneau Traffic Direction, sélectionnez l'une des options suivantes :

- <Adresse IP source> vers <Adresse IP de/// destination>
- <Adresse IP source> vers n'importe quelle destination
- De n'importe quelle source vers <l'adresse IP de destination>
- De n'importe quelle source à n'importe quelle destination

Etape 7 Cliquez sur **Tune**.

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.

Pourplus d'informations sur Juniper JunOS Platform DSM, voir le Guide d'administration *IBM Security QRadar DSM*.

Affichage de la colonne de données PCAP

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.

Avant de commencer

avant d'afficher les données PCAP dans l'onglet **Log Activity**, la source de 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 de journal, voir le Guide utilisateurs *IBM Security QRadar des sources de journal*.

A propos de cette tâche

Lorsque vous effectuez une recherche qui comprend la colonne **PCAP Data**, une icône s'affiche dans la colonne **PCAP Data** des résultats de recherche si les données PCAP sont disponibles pour un événement. En utilisant l'icône **PCAP**, vous pouvez afficher les données PCAP ou télécharger le fichier PCAP sur votre système de bureau.

Procédure

Etape 1 Cliquez surl'onglet **Log Activity.**

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

Etape 3 Facultatif. Pour rechercher des événements dotés de données PCAP, configurez le critère de recherche suivant:

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

b A partir de la seconde zone de liste, sélectionnez **Equals**.

c A partir de la troisième zone de liste, sélectionnez **True**.

d Cliquez sur **Add Filter**.

Etape 4 Configurez vos définitions de colonne pour inclure la colonne **PCAP Data** :

a A partir de 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** vers la liste**Columns**.

c Facultatif. Cliquez sur l'icône **Add Column** dans l'ensemble supérieur des icônes pour déplacer la colonne **PCAP Data** vers la liste **Group By**.

Etape 5 Cliquez sur **Filter**.

Etape 6 Facultatif. Si vous affichez des événements en mode diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause le mode.

Etape 7 Cliquez deux fois sur l'événement que vous souhaitez rechercher.

Etape suivante

Pourplus d'informations sur l'affichage et le téléchargement de données PCAP, voir les sections suivantes :

- **Affichage d'informations PCAP**
- **Téléchargement du fichier PCAP sur votre système de bureau**

Affichage d'informations PCAP

A partir du menu de la barre d'outils **PCAP Data**, vous pouvez afficher des informations PCAP ou télécharger le fichier PCAP sur votre système de bureau. Vous pouvez afficher une version lisible des données dans le fichier PCAP.

Avant de commencer

Avant d'afficher des informations PCAP, vous devez effectuer ou sélectionner une recherche qui affiche la colone **PCAP Data**. Voir **Affichage de la colonne de données PCAP**.

A propos de cette tâche

Avant que les données PCAP s'affichent, QRadar Network Anomaly Detection doit récupérer le fichier PCAP pour l'afficher sur l'interface utilisateur. 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.

Une fois le fichier récupéré, une fenêtre contextuelle fournit une version lisible du fichier PCAP. Vous pouvez lire les informations affichées dans la fenêtre, ou télécharger les informations sur votre système de bureau

Procédure

Etape 1 Pour l'événement que vous souhaitez rechercher, choisissez l'une des options suivantes :

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

Etape 2 Sivous souhaitez 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 à utiliser dans une application externe.
- Cliquez sur **Download PCAP Text** pour télécharger les informations PCAP auformat.TXT.

Etape 3 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 à partir de la zone de liste.
- Si vous souhaitez enregistrer la liste, sélectionnez l'option **Save File.**

Etape 4 Cliquez sur **OK**.

Téléchargement du fichier PCAP sur votre système de bureau

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

Avant de commencer

avant d'afficher une information PCAP, vous devez effectuer ou sélectionner une recherche qui affiche la colonne **PCAP Data**. Voir **Affichage de la colonne de données PCAP**.

Procédure

Etape 1 Pour l'événement que vous souhaitez rechercher, choisissez l'une des options suivantes :

- Sélectionnez l'événement et cliquez sur l'icône the **PCAP**.
- Cliquez avec le bouton droit de la souris sur l'icône **PCAP** de de l'événement et sélectionnez **More Options > Download PCAP File**.
- Cliquez deux fois sur l'événement que vous souhaitez rechercher, puis sélectionnez **PCAP Data > Download PCAP File** à partir de la barre d'outils des détails d'événement.

Etape 2 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 à partir de la zone de liste.
- Si vous souhaitez enregistrer la liste, sélectionnez l'option **Save File.**

Etape 3 Cliquez sur **OK**.

Exportation d'événements

Vous pouvez exporter des événements au format Extensible Markup Language (XML) ou Comma Separated Values (CSV). La durée nécessaire pour exporter vos données dépend du nombre de paramètres spécifiés.

Procédure

Etape 1 Cliquez surl'onglet **Log Activity**.

Etape 2 Facultatif. Si vous affichez des événements en mode diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause le mode.

Etape 3 A partir dela 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 4 Si vous souhaitez résumer vos activités alors que le processus d'exportation se poursuit, cliqu surez **Notify When Done**.

Résultat

Une foisl'exportation terminée, vous recevez une notification vous informant sur l'état d'exportation. Si vous n'avez pas sélectionné l'icône **Notify When Done**, la fenêtre d'état s'affiche.

5 RECHERCHE D'ACTIVITÉ RÉSEAU

A l'aide de l'onglet **Network Activity**, vous pouvez surveiller et rechercher une éventuelle activité réseau (flux) en temps réel ou effectuer des recherches avancées.

Présentation de l'onglet Network Activity

Vous devez avoir la permission d'afficher l'onglet **Network Activity**. Pour plus d'informations sur les permissions et l'assignation des rôles, voir le *Détection des anomalies réseau IBM Security QRadar Guide d'administration*.

L'onglet **Network Activity** vous permet de surveiller visuellement et de rechercher 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 des informations de flux afin de déterminer comment le trafic est communiqué et ce qui est communiqué (si l'option de capture du contenu est activée). Les informations sur le flux peuvent également comprendre cerftains détails tels que les protocoles, les valeurs ASN, ou les valeurs IFIndex.

Barre d'outils de l'onglet Network Activity

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

Tableau 5-1 Onglet d'activité réseau pour les options de la barre d'outils

Option	Description
Recherche	Cliquez sur **Search** pour effectuer des recherches avancées sur les flux. Les options comprennent : • **New Search** - Sélectionnez cette option pour créer une nouvelle recherche de flux. • **Edit Search** - Sélectionnez cette option afin de choisir et modifier une recherche de flux. • **Manage Search Results** - Sélectionnez cette option afin d'afficher et gérer les résultats de recherche. Pour plus d'informations sur la fonction de recherche, voir **Recherches de données.**
Recherches rapides	A partir de cette zone de liste, vous pouvez exécuter des recherches précédemment sauvegardées. Les options sont uniquement affichées dans la zone de liste **Quick Searches** lorsque vous avez enregistré les critères de recherche qui indiquent l'option **Include in my Quick Searches**.

Tableau 5-1 Onglet d'activité réseau pour les options de la barre d'outils (suite)

Option	Description
Ajout de filtre	Cliquez sur **Add Filter** afin d'ajouter un filtre aux résultats de recherche en cours.
Critère de sauvegarde	Cliquez sur **Save Criteria** afin de sauvegarder le critère de recherche suivant.
Résultats de sauvegarde	Cliquez sur **Save Results** afin de sauvegarder les résultats de recherche en cours. Cette option ne s'affichent qu'une fois la recherche terminée. Cette option est désactivée en mode de diffusion en flux.
Annulation	Cliquez sur **Cancel** pour annuler une recherche en progression. Cette option est désactivée en mode de diffusion en flux.
Faux positif	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 de violations. Pour plus d'informations sur les faux positifs, voir le **Glossaire**. Cette option est désactivée en mode de diffusion en flux. Voir **Exportation de flux**.

Tableau 5-1 Onglet d'activité réseau pour les options de la barre d'outils (suite)

Option	Description
Règles	L'option Rules est visible uniquement si vous avez la permission d'afficher les règles personnalisées. Cliquez sur **Rules** afin de configurer les règles de flux personnalisées. Les options comprennent : • **Rules** - Sélectionnez cette option pour afficher ou créer une règle. Si vous avez la permission d'afficher des règles, la page de synthèse de l'assistant de Règles s'affiche. Si vous avez la permission de conserver des règles personnalisées, l'assistant de Règles s'affiche et vous pouvez modifier la règle. ***Remarque :*** *Les options de la règle de détection des anomalies sont visibles uniquement si vous avez la permission* ***Network Activity > Maintain Custom Rules****.* 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 sauvegarder les critères de recherche agrégés parce que les critères de recherche sauvegardés indiquent les paramètres nécessaires • **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 Détection des anomalies réseau QRadar. Par exemple, si vous créez une règle de seuil en indiquant que plus de 220 clients ne peuvent pas se connecter au serveur entre 08 et 17 heures, les règles génèrent une alerte lorsque le 221 ème client tente de se connecter. Lorsque vous sélectionnez l'option **Add Threshold Rule**, l'assistant des règles s'affiche, rempli d'options appropriées pour la création d'une règle de seuil. • **Add Behavioral Rule** - Sélectionnez cette option afin de créer une règle comportementale. Une règle de comportement teste le trafic de flux pour les changements du volume dans le comportement qui se produit dans des modèles saisonniers réguliers. Par exemple, si un serveur de messagerie communique généralement avec 100 hôtes par seconde au milieu de la nuit et qu'ensuite il commence à communiquer avec 1000 hôtes par seconde, la règle comportementale génère une alerte. Lorsque vous sélectionnez l'option **Add Behavioral Rule,** l'assistant des règles s'affiche, rempli d'options appropriées pour la création d'une règle comportementale. • **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 genre de trafic qui s'arrête subitement ou un changement de pourcentage dans le temps imparti à l'activité d'un objet <Par exemple, vous pouvez créer une règle d'anomalie pour comparer le volume moyen du trafic des cinq dernières minutes et le volume moyen du trafic au cours de la dernière heure. Si le changement s'élève à plus de 40%, la règle génère une réponse.

Tableau 5-1 Onglet d'activité réseau pour les options de la barre d'outils (suite)

Option	Description
	Lorsque vous sélectionnez l'option **Add Anomaly Rule**, l'assistant des règles s'affiche, rempli d'options appropriées pour la création d'une règle d'anomalie. Pour plus d'informations sur les règles, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar*.
Actions	Cliquez sur **Actions** pour effectuez les options suivantes : • **Show All** - Sélectionnez cette option afin de supprimer tous les filtres sur le critère de recherche et pour afficher tous les flux non filtrés. • **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 de flux**. • **Export to CSV** - Sélectionnez cette option pour exporter les flux en format CSV. Voir **Exportation de flux**. • **Delete** - Sélectionnez cette option pour supprimer un résultat de recherche. Voir **Recherches de données**. • **Notify** - Sélectionnez cette option pour indiquer que vous souhaitez recevoir une notification par courrier électronique à la fin des recherches sélectionnées. Cette option est activée uniquement pour les recherches en cours. ***Remarque :*** *Les options **Print**, **Export to XML** et **Export to CSV** sont désactivées en mode de diffusion en flux et lors de l'affichage des résultats de recherche partielle.*
Filtre rapide	Entrez vos critères de recherche dans la zone **Quick Filter** et cliquez sur l'icône **Quick Filter** ou appuyez sur la touche "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 la charge utile d'événement afin de déterminer celle qui correspond à votre critère spécifique. ***Remarque :*** *Lorsque vous cliquez sur la zone **Quick Filter**, une 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* **Syntaxe du filtre rapide**.

Syntaxe du filtre rapide

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

- **Network Activity toolbar** - Sur la barre d'outils, une zone **Quick Filter** vous permet d'entrer une chaîne de recherche de texte et de cliquer sur l'icône **Quick Filter** afin d'appliquer votre filtre rapide à la liste actuellement affichée de flux.
- **Boîte de dialogue Add Filter** - 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 chaîne de recherche de texte. Ceci vous permet d'appliquer votre filtre rapide à la liste actuellement affichée de flux. Pour plus d'informations sur la boîte de dialogue **Add Filter**, voir **Recherches de données**.

- **Flow search pages** - A partir des pages de recherche de flux, 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 de critère de recherche, voir **Recherches de données**.

Lorsque vous affichez les flux en mode temps réel (streaming) ou en mode dernier intervalle, vous pouvez uniquement entrer des mots et des phrases simples dans la zone **Quick Filter**. Lorsque vous affichez un flux à l'aide d'un intervalle de temps, utilisez les directives de syntaxe suivantes pour entrer votre critère de recherche :

- Les termes de recherche peuvent contenir n'importe quel texte brut que vous espérez trouver dans le contenu. Par exemple, `Firewall`
- Notamment 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 trouve 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"`

Options du menu contextuel

Sur l'onglet **Network Activity**, vous pouvez effectuer un clic droit sur un flux afin d'accéder à un critère supplémentaire de filtrage de flux.

Les options du menu contextuel sont :

Tableau 5-2 Cliquez avec le bouton droit sur les optionsdumenu

Option	Description
Filtre actif	Sélectionnez cette option pour filtrer les flux sélectionnés, en fonction du paramètre sélectionné dans le flux.

Tableau 5-2 Cliquez avec le bouton droit sur les optionsdumenu (suite)

Option	Description
Faux positif	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. Cette option est désactivée en mode de diffusion en flux. Voir **Exportation de flux**.
Plus d'options :	Sélectionnez cette option pour rechercher une adresse IP. Voir **Etude des adresses**. ***Remarque :*** *Cette option n'est pas désactivée en mode de diffusion en flux*

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 des processeurs 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 Détection des anomalies réseau QRadar ne diffuse pas les flux, la barre d'état affiche le nombre de résultats de recherche actuellement affichés ainsi que le temps nécessaire au traitement des résultats de recherche.

Enregistrement des dépassements

Si vous avez des droits administrateurs, vous pouvez indiquer le nombre maximal de flux que vous souhaitez envoyer à partir de Collecteur QFlow vers les processeurs d'événement. Toutes les données collectées après l'atteinte de la limite de flux configurés 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**.

Surveillance de l'activité réseau

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 diffusion en flux, voir **Affichage de flux en mode diffusion en flux**. Vous pouvez spécifier un intervalle différent pour filtrer les flux à l'aide de la zone de liste **View**.

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 la sauvegarde du critère de recherche, voir **Enregistrement des critères de recherche d'événements et de flux**.

Affichage de flux en mode diffusion en flux

Le mode de diffusion en flux vous permet d'afficher les données de flux entrants dans votre système. Ce mode de diffusion vous apporte un affichage en temps réel de votre activité de flux en cours, tout en affichant les derniers 50 flux.

A propos de cette tâche

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 groupés, l'onglet **Network Activity** affiche les flux normalisés. Voir **Affichage de flux normalisés**.

Lorsque vous souhaitez sélectionner un flux pour voir les détails ou pour effectuer une action, vous devez mettre en pause le mode diffusion en flux avant de faire un

double clic sur un événement. Une fois que le mode diffusion en flux a été mis en pause, les 1000 derniers flux s'affichent.

Procédure

Etape 1 Cliquez surl'onglet **Network Activity**.

Etape 2 A partir dela zone de liste **d'affichage**, sélectionnez **Real Time (streaming)**.

Pourobtenir des informations sur les options de barre d'outils, voir **Tableau 5-1**. Pour plus d'informations sur les paramètres affichés en mode diffusion en flux, voir **Tableau 5-3**.

Etape 3 Facultatif. Mettez en pause ou en lecture la diffusion de flux. Sélectionnez l'une des options suivantes :

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

Affichage de flux normalisés

Détection des anomalies réseau QRadar collecte des données de flux, puis les normalise pour un affichage sur l'onglet **Network Activity**.

A propos de cette tâche

La normalisation implique une préparation des données de flux afin d'afficher des informations lisiblessur l'onglet.

Remarque : Si vous avez sélectionnez un cadre de temps à afficher, un graphique de séries temporelles s'affiche. Pour plus d'informations sur les graphiques de séries temporelles, voir **Présentation du graphique de séries temporelles**.

L'onglet **Network Activity** affiche les paramètres suivants lorsque vous affichez des flux normalisés :

Tableau 5-3 Paramètres d'onglet de l'activité réseau

Paramètre	Description
Filtres en cours	La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche. Pour supprimer ces valeurs de filtres, cliquez sur **Clear Filter**. ***Remarque :*** *Ce paramètre s'affiche uniquement après l'application d'un filtre.*
Affichage	A partir de la zone de liste, vous pouvez sélectionner l'intervalle de temps que vous souhaitez filtrer.

Tableau 5-3 Paramètres d'onglet de l'activité réseau (suite)

Paramètre	Description
Statistiques en cours	Lorsque le mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique) n'est pas précisé, les statistiques en cours s'affichent, y compris : ***Remarque :*** *Cliquez sur la flèche à côté de* ***Current Statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total de résultats correspondant à votre critère de recherche. • **Data Files Searched** - Indique le nombre total de fichiers de données recherchés pendant l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total de fichiers de données compressés dans l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***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 des problèmes liés aux flux, il peut vous être demandé de fournir des informations statistiques récentes.*
Graphiques	Affiche des graphiques configurables représentant les enregistrements correspondants par intervalle de temps et option de groupement. Cliquez sur **Hide Charts** si vous souhaitez retirer les graphiques de votre affichage. Les graphiques s'affichent uniquement après avoir sélectionné le cadre de temps 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 **Configuration des graphiques**. ***Remarque :*** *Si vous utilisez Mozilla Firefox comme navigateur et qu'une extension bloqueur de publicités est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez retirer l'extension bloqueur de publicités. Pour plus d'informations, voir la documentation du navigateur.*
Icône de violation	Cliquez sur l'icône **Offenses** pour afficher les détails de la violation associée au flux.

Tableau 5-3 Paramètres d'onglet de l'activité réseau (suite)

Paramètre	Description
Type de flux	Indique le type de flux. Les types de flux sont mesurés par le taux d'activité entrant et sortant. Les types de flux incluent : • **Standard Flow**- Trafic Bidirectionnel • **Type A** - un-vers-plusieurs (unidirectionnel), par exemple, un hôte unique effectuant une analyse de réseau. • **Type B** - plusieurs-vers-un (unidirectionnel), par exemple, une attaque DoS (DDoS) distribuée. • **Type C** - un-vers-un (unidirectionnel), par exemple, un hôte vers une analyse de port d'hôte.
Premier intervalle de temps	Indique la date et l'heure où Détection des anomalies réseau QRadar reçoit le flux.
Temps d'archivage	Indique le temps durant lequel le flux a été enregistré sur la base de donnés de Détection des anomalies réseau QRadar.
Adresse IP source	Indique l'adresse IP source du flux.
Port source	Indique le port source du flux.
Adresse IP de destination	Indique l'adresse IP de destination du flux.
Port de destination	Indique le port de destination du flux.
Octets source	Indique le nombre d'octets envoyés à partir de l'hôte source.
Octets de destination	Indique le nombre d'octets envoyés à partir de l'hôte de destination.
Octets total	Indique le nombre total d'octets associés au flux.
Paquets source	Indique le nombre total de paquets envoyés à partir de l'hôte source.
Paquets de destination	Indique le nombre total de paquets envoyés à partir de l'ôte de destination.
Paquets total	Indique le nombre total de paquets associés au flux.
Protocole	Indique le protocole associé au flux.
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'application, voir le Guide de configuration d'application*IBM Security QRadar*.
Type/Code ICMP	Indique le type et le code de protocole de messagerie de gestion interréseau (ICMP), le cas échéant. 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 <B>` où `<A>` et `<B>` sont les valeurs numériques du type et du code.
Indicateurs source	Indique les indicateurs de type Transmission Control Protocol(TCP) détectés dans le paquet source, le cas échéant.
Indicateurs de destination	Indique les balises du TCP détectées dans le paquet de destination, le cas échéant.

Tableau 5-3 Paramètres d'onglet de l'activité réseau (suite)

Paramètre	Description
Qualité de service source	Indique le niveau de service de Quality of service (QoS) du flux. QoS permet au serveur de fournir différents niveaux de service pour les flux. QoS fournit les niveaux de service de base suivants : • **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.
QoS de destination	Indique le niveau QoS du service pour le flux de destination.
Source de flux	Indique le système qui a détecté le flux. Pour plus d'informations sur les sources de flux, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar.*
Interface de flux	Indique l'interface qui reçoit le flux.
Index If source	Indique le nombre d'index de l'interface (IFIndex) source.
Index If de destination	Indique le nombre d'Index IF de destination.
ASN source	Indique les valeurs Autonomous System Number (ASN) source.
ASN de la destination	Indique la valeur ASN de destination.

Procédure

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

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

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

Etape 4 Cliquez sur l'icône **Pause** afin de mettre en pause la diffusion en flux.

Etape 5 Cliquez deux foissur le flux que vous souhaitez afficher plus en détails. voir **Détails relatifs aux flux**.

Affichage de 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 sélectionnez le paramètre par lequel vous souhaitez grouper les flux.

A propos de cette tâche

La zone de liste **Display** ne s'affiche pas en mode diffusion en flux car 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.

La zone de liste Display fournit les options suivantes :

Tableau 5-4 Optionsde flux groupé

Option du groupe	Description
Flux unis	Affiche divers flux dans un seul modèle ininterrompu via différents intervalles, dans un enregistrement unique. Par exemple, si un flux dure cinq minutes, le flux uni s'affiche sous forme d'un seul flux de cinq minutes. Sans le flux uni, le flux s'affiche sous forme de cinq flux : un flux par minute. Les flux unis affichent une liste résumée de flux groupés par informations du flux uni.
Adresse IP source ou de destination	Affiche une liste résumée de flux groupés par l'adresse IP associée aux flux.
Adresse IP source	Affiche une liste résumée de flux groupés par l'adresse IP source du flux.
Adresse IP de destination	Affiche une liste résumée de flux groupés par l'adresse IP de destination du flux.
Port source	Affiche une liste résumée de flux groupés par le port source du flux.
Port de destination	Affiche une liste résumée de flux groupés par le port de destination du flux.
Adresse IP source	Affiche une liste résumée de flux groupés par le réseau source du flux.
Réseau de destination	Affiche une liste résumée de flux groupés par le réseau de destination du flux.
Application	Affiche une liste résumée de flux groupés par l'application à l'origine du flux.
Géographique	Affiche une liste résumée de flux groupés par emplacement géographique.
Protocole	Affiche une liste résumée de flux groupés par le protocole associé au flux.
Circulation de flux	Affiche une liste résumée de flux groupés par la direction du flux.
Type ICMP	Affiche une liste résumée de flux groupés par le type ICMP du flux.

Après avoir sélectionné une option à partir de la zone de liste **Display**, l'agencement de colonne de données dépend de l'option de groupe choisie.

Chaque ligne dans la table de flux représente un groupe de flux. L'onglet **Network Activity** fournit les informations suivantes pour chaque groupe de flux :

Tableau 5-5 Paramètres de flux groupés

Paramètre	Description
Groupement par	Indique le paramètre sur lequel la recherche est groupée.
Filtres en cours	La partie supérieure du tableau affiche 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, sélectionnez l'intervalle que vous souhaitez filtrer.
Statistiques en cours	Lorsque le mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique) n'est pas précisé, les statistiques en cours s'affichent, y compris : ***Remarque :*** *Cliquez sur la flèche suivante de* ***Current Statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total de résultats correspondant à votre critère de recherche. • **Data Files Searched** - Indique le nombre total de fichiers de données recherchés pendant l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total des fichiers de données compressés dans l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'indexation recherchés dans l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***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 des problèmes liés aux flux, il peut vous être demandé de fournir des informations statistiques récentes.*
Graphiques	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. Les graphiques s'affichent uniquement après avoir sélectionné le cadre de temps 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 **Configuration des graphiques**. ***Remarque :*** *Si vous utilisez Mozilla Firefox comme navigateur et qu'une extension bloqueur de publicités est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez retirer l'extension bloqueur de publicités. Pour plus d'informations, voir la documentation du navigateur.*

Tableau 5-5 Paramètres de flux groupés (suite)

Paramètre	Description
Adresse IP source (Comptage unique)	Indique l'adresse IP source du flux.
Adresse IP de destination (Comptage unique)	Indique l'adresse IP de destination du flux. S'il existe plusieurs adresses IP de destination associées à ce flux, cette zone indique le terme Multiple et le nombre d'adresses IP.
Port source (Comptage unique)	Affiche le port source du flux.
Port de destination (Comptage unique)	Indique le port de destination du flux. S'il existe plusieurs ports de destination associés à ce flux, cette zone indique le terme Multiple et le nombre de ports.
Réseau source (Comptage unique)	Indique le réseau source du flux. S'il existe plusieurs réseaux source associés au flux, cette zone indique le terme Multiple et le nombre de réseaux.
Réseau de destination (Comptage unique)	Indique le réseau de destination du flux. S'il existe plusieurs réseaux de destination associés au flux, cette zone indique le terme Multiple et le nombre de réseaux.
Application (Comptage unique)	Indique l'application détectée des flux. S'il existe plusieurs applications associées à ce flux, cette zone indique le terme Multiple et le nombre d'applications.
Octets source (Somme)	Indique le nombre d'octets provenant de la source.
Octets de destination (Somme)	Indique le nombre d'octets provenant de la destination.
Octets total (Somme)	Indique le nombre total d'octets associés au flux.
Paquets source (Somme)	Indique le nombre de paquets provenant de la source.
Paquets de destination (Somme)	Indique le nombre de paquets provenant de la destination.
Paquets total (Somme)	Indique le nombre total de paquets associés au flux.
Comptage	Indique le nombre de flux envoyés ou reçus.

Procédure

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

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

Etape 3 Apartir de la zone de liste **Display**, choisissez par quel paramètre vous souhaitez grouper les flux. Voir **Tableau 5-4**.

Les groupes de flux sont répertoriés. Pour plus d'informations sur les détails de groupe de flux. Voir **Tableau 5-6**.

Etape 4 Pour afficher la page liste de flux pour un groupe, cliquez deux foissur le groupe de flux que vous souhaitez rechercher.

La liste de page de flux ne conserve pas les configurations de graphique que vous avez peut-être définies sur l'onglet **Network Activity**. Pour plus d'informations sur les paramètres liste de flux, voir **Tableau 5-3**.

Etape 5 Pour afficher les détails d'un flux, cliquez deux foissur le flux que vous souhaitez rechercher. pourplus d'informations sur la page relative aux détails de flux, voir **Tableau 5-6**.

Détails relatifs aux flux

Vous pouvez afficher une liste de flux dans différents modes, y compris le mode diffusion en flux dou en groupes de flux. Peu importe le mode choisi pour l'affichage des flux, vous pouvez localiser et afficher les détails d'un flux unique. La page relative aux détails de flux fournit les informations suivantes :

Tableau 5-6 Détils de flux

Paramètre	Description
Informations sur les flux	
Protocole	Indique le protocole associé à ce flux. Pour plus d'informations sur les protocoles, voir le Guide de configuration d'application*IBM Security QRadar*.
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'application, voir le Guide de configuration d'application*IBM Security QRadar.*
Ampleur	Indique l'ampleur de ce flux. Pour plus d'informations sur l'ampleur, voir le **Glossaire**.
Pertinence	Indique la pertinence de ce flux. Pour plus d'informations sur la pertinence, voir le **Glossaire**.
Gravité	Indique la gravité de ce flux. Pour plus d'informations sur la gravité, voir le **Glossaire**.
Crédibilité	Indique la crédibilité de ce flux. Pour plus d'informations sur la crédibilité, voir le **Glossaire**.
Premier intervalle de temps	Indique l'heure de début du flux, telle que reportée à Détection des anomalies réseau QRadar par la source du flux. Pour plus d'informations sur les sources de flux, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar*.
Dernier intervalle de temps	Indique l'heure de fin du flux, telle que reportée à Détection des anomalies réseau QRadar par la source du flux. Pour plus d'informations sur les sources de flux, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar*.

Tableau 5-6 Détils de flux (suite)

Paramètre	Description
Temps d'archivage	Indique le temps où le flux a été enregistré sur la base de donnés Détection des anomalies réseau QRadar.
Nom de l'événement	Indique le nom normalisé du flux.
Catégorie de niveau bas	Indique la catégorie de niveau bas de ce flux. pour plus d'informations sur les catégories, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar*.
Description d'événement	Indique une description du flux, si disponible.
Informations sur la source et la destination	
Adresse IP source	Indique l'adresse IP source du flux.
Adresse IP de destination	Indique l'adresse IP de destination du flux.
Nom de l'actif source	Indique l'actif de la source du flux. Pour plus d'informations sur les actifs, voir **Gestion des actifs**.
Nom de d'actif de destination	Indique le nom d'actif de destination du flux. Pour plus d'informations sur les actifs, voir **Gestion des actifs**..
Source IPv6	Indique l'adresse IPv6 source du flux.
Adresse IPv6 de destination	Indique l'adresse IPv6 de destination du flux.
Port source	Indique le port source du flux.
Port de destination	Indique le port de destination du flux.
QoS source	Indique le niveau QoS de service pour le flux source.
QoS de destination	Indique le niveau QoS de service pour le flux de destination.
ASN source	Indique le nombre des valeurs ASN source. ***Remarque :*** *Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres de valeurs ASN source correspondant sont répertoriés.*
ASN de la destination	Indique le nombre de valeurs ASN de destination. ***Remarque :*** *Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres de valeurs ASN de destination correspondant sont répertoriés.*
Index If source	Indique le nombre d'IFIndex source. ***Remarque :*** *Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres d'IFIndex source correspondant sont répertoriés.*

Tableau 5-6 Détils de flux (suite)

Paramètre	Description
Index If de destination	Indique le nombre d'IFIndex de destination. ***Remarque :*** *Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres d'IFIndex source correspondant sont répertoriés.*
Contenu source	Indique le nombre de paquet et d'octets pour le contenu source.
Contenu de destination	Indique le nombre de paquet et d'octets pour le contenu de destination.
Informations sur le contenu	
Contenu source	Indique le contenu source du flux. Cette zone offre trois formats pour afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur **UTF**. • Hexidécimal - Cliquez sur **HEX**. • Base64 - Cliquez **Base64**. ***Remarque :*** *Si votre source de flux correspond à Netflow v9 ou IPFIX, des zones non analysées provenant de ces sources peuvent s'afficher dans la zone* ***Source Payload****. Le format de cette zone non analysée est <name>=<value>. Par exemple,* ***MIN_TTL=x****.*
Contenu de destination	Indique le contenu de destination du flux. La zone offre trois formats pour afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur **UTF**. • Hexidécimal - Cliquez sur **HEX**. • Base64 - Cliquez **Base64**.

Tableau 5-6 Détils de flux (suite)

Paramètre	Description
Informations supplémentaires	
Type de flux	Indique le type de flux. Les types de flux sont mesurés par le taux d'activité entrant et sortant. Les types de flux incluent : • **Standard** - trafic bidirectionnel • **Type A** - Un -vers-plusieurs (unidirectionnel) • **Type B** - Plusieurs-vers-un (unidirectionnel) • **Type C** - un-vers-un (unidirectionnel)
Direction de flux	Indique la direction du flux. Les directions du flux comprennent : • **L2L** - trafic interne d'un 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.
Règles personnalisées	Indique les règles personnalisées qui correspondent à ce flux. Pour plus d'informations sur les règles, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar A.*
Règles personnalisées partiellement correspondantes	Indique les règles personnalisées qui correspondent partiellement à ce flux. Pour plus d'informations sur les règles, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar.*
Source/Interface du flux	Indique le nom de la source du flux du système ayant détecté le flux. ***Remarque :*** *Si ce flux possède des enregistrements en double provenant 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 pouvant être automatiquement ajoutées aux flux comme faisant partie de la réponse à la règle. Pour plus dd'informations sur les règles, voir le Guide d'administration *Détection des anomalies réseau IBM Security QRadar.*

Barre d'outils des détails de flux

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

Tableau 5-7 Barre d'outils des détails de flux

Fonction	Description
Retour aux résultats	Cliquez sur **Return to Results** pour retourner à la liste des flux.
Violation	Cliquez sur **Offense** pour afficher les violations auxquelles le flux est corrélé.

Tableau 5-7 Barre d'outils des détails de flux (suite)

Fonction	Description
Propriété d'extraction	Cliquez sur **Extract Property** pour créer une propriété de flux personnalisé à partir du flux sélectionné. Pour plus d'informations, voir **Propriétés personnalisées d'événements et de flux.**
Faux positif	Cliquez sur **False Positive** 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 de violations. Cette option est désactivée en mode de diffusion en flux. Voir **Exportation de flux**.
Précédent	Cliquez sur **Previous** pour afficher le flux précédent dans la liste d'événements.
Suivant	Cliquez sur **Next** pour afficher le flux suivant dans la liste d'événements.
Imprimer	Cliquez sur **Print** pour imprimer les détails du flux.

Réglage des faux positifs

Vous pouvez utiliser la fonction False Positive Tuning pour éviter une création de violation par les flux de faux positifs. Vous pouvez régler les flux de faux positifs à partir de la page de liste de flux ou détails de flux.

A propos de cette tâche

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 Guide d'administration *Détection des anomalies réseau IBM Security QRadar*. Pour plus d'informations sur les faux positifs, voir le **Glossaire**.

Procédure

Etape 1 Cliquez surl'onglet **Network Activity**.

Etape 2 Facultatif. Si vous affichez les flux en mode de diffusion en flux, cliquez sur l'icône**Pause** pour mettre en pause le mode.

Etape 3 Sélectionnez le flux que vous souhaitez régler.

Etape 4 Cliquez sur **False Positive**.

Etape 5 Dans le volet de propriété d'événement/flux de la fenêtre False Positive, sélectionnez une des options suivantes :

- Evénement/Flux(s) avec un QID spécifique de <Event>
- Chaque Evénement/Flux(s) avec une catégorie de niveau bas de <Event>
- Chaque Evénement/Flux(s) avec une catégorie de niveau bas de <Event>

Etape 6 Dans le panneau de direction du trafic, sélectionnez une des options suivantes :

- <Adresse IP source> vers <Adresse IP de destination>
- <Adresse IP source> vers n'importe quelle distination

- N'importe quelle source vers <Adresse IP de destination>
- N'importe quelle source vers n'importe quelle destination

Etape 7 Cliquez sur **Tune**.

Remarque : Vous pouvez régler les flux des faux positifs à partir de la page récapitulative ou des détails.

Exportation de flux

Vous pouvez exporter des flux en format Extensible Markup Language (XML) ou Comma Separated Values (CSV). Le laps de temps nécessaire pour exporter des données dépend du nombre de paramètres spécifiés.

Procédure

Etape 1 Cliquez surl'onglet **Network Activity**.

Etape 2 Facultatif. Si vous affichez les flux en mode de diffusion en flux, cliquez sur l'icône**Pause** pour mettre en pause le mode.

Etape 3 Apartir de la zone de liste **Actions**, sélectionnez 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 de flux. 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 de flux. Une exportation complète peut prendre un certain temps pour terminer.

Etape 4 Si vous souhaitez reprendre vos activités, cliquez sur **Notify When Done**.

Résultat

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.

6 GESTION GRAPHIQUE

A l'aide de la fonction du graphiques osur les onglets **Log Activity** et **Network Activity**, vous pouvez afficher vos données via les différentes options de configuration du graphique.

Présentation des graphiques

Lorsque vous sélectionnez un cadre temporel ou une option de groupement pour afficher les données sur les onglets **Log Activity** et **Network Activity**, les graphiques s'affichent au dessus de la liste d'événements et de flux.Les graphiques ne s'affichent en mode diffusion en flux.

Vous pouvez configurer un graphique pour sélectionner les données que vous souhaitez schématiser. Vous pouvez configurer les graphiques indépendamment l'un de l'autre pour afficher les résultats de la recherche sous différentes perspectives..

Les types de graphiques sont les suivants:

- **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.
- **Time Series** - Affiche un graphique en ligne interactif représentant les enregistrements correspondant par intervalle de temps spécifique. Pour de plus amples informations sur la configuration des critères de recherche de séries temporelles, voir **Présentation de graphiques de séries temporelles**.

Après que vous avez 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 the Mozilla Firefox comme navigateuret 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, consultez la documentation du navigateur.

Présentation de 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 l'analyse des tendances de données à court et à 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 guide administrateur*IBM Security QRadar Network Anomaly Detection.*

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 prend en charge jusqu'à 100 recherches de séries temporelles. 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.

Vous pouvez agrandir et analyser une ligne temporelle sur un graphique de série temporelle en vue d'étudier l'activité du journal ou du réseau. Le tableau suivant fournit des fonctions vous permettant d'afficher les graphiques de séries temporelles:

Tableau 6-1 Les fonctions de graphiques de séries temporelles

Function	Description
Afficher les données avec plus de détails	À l'aide de la fonction zoom, vous pouvez étudier les plus petites tranches horaires du trafic de l'événement. • 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. Lorsque vous agrandissez un graphique de séries temporelles, le graphique s'actualise pour afficher un segment de temps plus petit.
Afficher un intervalle de temps de données plus large	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 : • 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).
Scan the chart	Lorsque vous avez agrandi le graphique de séries temporelles, vous pouvezcliquer et faire glisser le graphique vers la gauche ou la droite pour analyser la ligne temporelle.

Légendes 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.

UA l'aide de la fonction 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 de menu contextuel, voir **A propos de la détection des anomalies du réseau 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

Vous pouvez utiliser les options de configuration pour changer de type de graphique, de type d'objet que vous souhaitez représenter graphiquement, ainsi que le nombre d'objets représentés sur le graphique. Pour les graphiques de séries temporelles, vous pouvez également sélectionner un intervalle et activer la fonction de capture de données de séries temporelles.

A propos de cette tâche

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**.

Avant de commencer

Les graphiques ne sont pas affichés lorsque vous visualisez les événements ou les flux en temps réel et en mode diffusion en flux.Pour afficher les graphiques, il vous faut accéder à l'onglet **Log Activity** ou **Network Activity**, et choisir l'une des options suivantes:

- Sélectionnez les options dans les zones de liste **View** et **Display**, puis cliquez sur **Save Criteria** sur la barre d'outils. Voir **Enregistrement des critères de recherche d'événements et de flux.**
- Sur la barre d'outils, sélectionnez une recherche enregistrée à partir de la zone de liste **Quick Search**.
- Effectuez une recherche groupée, puis cliquez sur **Save Criteria** sur la barre d'outils. Voir **Recherche d'événements ou de flux** et **Enregistrement des critères de recherche d'événements et de flux.**

Si vous envisagez de configurer un graphique de séries temporelles, assurez-vous que les critères de recherche enregistrée sont groupés et qu'ils définissent un intervalle de temps.

Procédure

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

Etape 2 Dans le panneau Charts, cliquez sur l'icône **Configure**.

Etape 3 Configurez les valeurs des paramètres psuivants:.

Paramètres	Description
Value to Graph	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 ou de flux normalisés et personnalisés inclus dans vos paramètres de recherche..

Paramètres	Description
Display Top	Dans la zone de liste, sélectionnez le nombre d'objets que vous souhaitez voir afficher to dans le graphique. La valeur par défaut est 10. L'orientation de plus de 10 éléments peut entraîner l'illisibilité de vos données cartographiques.
Chart Type	Dans la zone de liste, sélectionnez le type de graphique que vous souhaitez afficher. Si votre barre, graphique circulaire ou graphique comparatif repose sur des critères de recherche enregistrés avec un intervalle de plus d'1 heure, il vous sera nécessaire de cliquer sur**Update Details** pour mettre à jour le graphique et remplir les détails d'événement.
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.. Cette option n'est disponible que sur les graphiques de séries temporelles.
Intervalle de temps	A partir de la zone de liste, sélectionnez l'intervalle que vous souhaitez afficher. Cette option n'est disponible que sur les graphiques de séries temporelles.

Etape 4 Si vous avez sélectionné l'option de graphique **Time Series** et avez activé l'option **Capture Time Series Data**, cliquez sur **Save Criteria** sur la barre d'outils.

Etape 5 Pour afficher la liste des événements ou de flux lorsque l' intervalle de temps que vous avez défini dépasse 1 heure, cliquez sur **Update Details**.

7 RECHERCHE DE DONNÉES

Dans les onglets **Log Activity**, **Network Activity**, et **Offenses**, vous pouvez rechercher des événements, des flux et des violations à l'aide de critères de recherche spécifiques. Vous pouvez créer une nouvelle recherche ou charger un ensemble de critères précédemment enregistrés. Vous pouvez sélectionner, organiser et regrouper les colonnes de données à afficher dans les résultats de la recherche.

Recherches d'événements et de flux.

Vous pouvez effectuer des recherches dans les onglets **Log Activity** et **Network Activity**. Une fois que vous effectuez une recherche, vous pouvez sauvegarder les critères de recherche et les résultats de la recherche.

Rechercher des événements ou des flux

Dans les onglets **Log Activity** et **Network Activity**, vous pouvez rechercher des événements et des flux qui correspondent aux critères de recherche.

A propos de cette tâche

Lorsque vous effectuez une recherche, Détection des anomalies QRadar recherche l'ensemble de la base de données pour les événements ou les flux qui correspondent à vos critères de recherche. Ce processus peut prendre du temps en fonction de la taille de la base de données.

Le paramètre de recherche **Quick Filter** dans le volet Search Parameters vous permet de rechercher des événements et des flux qui correspondent à votre chaîne de texte dans le contenu de l'événement. Pour plus d'informations sur comment utiliser le paramètre **Quick Filter**, voir **Syntaxe de filtrage rapide** (événements) ou **Syntaxe de filtrage rapide** (flux).

Le tableau suivant décrit les options de recherche que vous pouvez utiliser pour rechercher des données d'événement et de flux :

Tableau 7-1 Options de recherche d'événement et de flux

Options	Description
Group	Cette zone de liste vous permet de sélectionner un groupe de recherche d'événement ou de flux pour afficher la liste **Available Saved Searches**.

Tableau 7-1 Options de recherche d'événement et de flux

Options	Description
Type Saved Search or Select from List	Ce champ vous permet d'entrer le nom de la recherche enregistrée ou un mot-clé pour filtrer la liste **Available Saved Searches**.
Available Saved Searches	Cette liste affiche toutes les recherches disponibles sauf si vous appliquez un filtre à la liste en utilisant les options **Group or Type Saved Search** ou **Select from List**. Vous pouvez sélectionner une recherche enregistrée sur la liste à afficher ou modifier.
Search	L'icône **Search** est disponible dans plusieurs volets sur la page de recherche. Vous pouvez cliquer sur **Search** une fois que vous avez terminé la configuration de la recherche et que vous souhaitez afficher les résultats.
Include in my Quick Searches	Cette case vous permet d'inclure cette recherche dans votre menu **Quick Search** qui se trouve sur l'onglet **Log Activity** et les barres d'outils **Network Activity**. Pour plus d'informations sur le menu **Quick Search**, consultez **Etude de l'activité du journal** ou **Etude de l'activité du réseau**.
Include in my Dashboard	Cette case vous permet d'inclure les données dans vos recherches sauvegardées sur l'onglet **Dashboard**. Pour plus d'informations sur l'onglet **Dashboard**, voir **Gestion du tableau de bord**. ***Remarque :*** *Ce paramètre ne s'affiche que si la recherche est regroupée.*
Set as Default	Cette case vous permet de définir cette recherche comme votre recherche par défaut lorsque vous accédez à l'onglet **Log Activity** ou **Network Activity**.
Share with Everyone	Cette case vous permet de partager cette recherche avec tous les autres utilisateurs.
Real Time (streaming)	Cette option vous permet d'afficher des résultats d'événement ou de flux en mode de diffusion. Pour plus d'informations sur le mode de diffusion, voir **Affichage des événements en flux**. ***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 volet Column Definition, un message d'erreur s'ouvre.*
Last Interval (auto refresh)	Cette option vous permet de rechercher des résultats en mode d'actualisation automatique. En mode actualisation automatique, les onglets **Log Activity** et **Network Activity** s'actualisent dans un intervalle d'une minute pour afficher les informations les plus récentes.
Recent	Cette option vous permet de sélectionner un intervalle prédéfini pour votre recherche. Une fois que vous choisissez cette option, vous devez sélectionner une option d'intervalle dans la zone de liste.

Tableau 7-1 Options de recherche d'événement et de flux

Options	Description
Specific Interval	Cette option vous permet de sélectionner un intervalle personnalisé pour votre recherche. Une fois que vous choisissez cette option, vous devez sélectionner l'intervalle date et heure dans les agendas **Start Time** et **End Time**.
Data Accumulation	Ce volet s'affiche uniquement lorsque vous chargez une recherche enregistrée. L'activation de comptages uniques sur des données accumulées qui sont partagées avec beaucoup d'autres recherches et rapports sauvegardés peut diminuer la performance du système. Lorsque vous chargez une recherche enregistrée, ce volet affiche les options suivantes : • Si aucune donnée ne s'accumule pour cette recherche, les informations suivantes s'affichent : `Data is not being accumulated for this search`. • Si les données s'accumulent pour cette recherche enregistrée, les options suivantes s'affichent : **columns** - Lorsque vous cliquez ou pointez votre souris sur ce lien, une liste de colonnes de données qui s'accumulent s'ouvre. **Enable Unique Counts/Disable Unique Counts** - Ce lien vous permet d'activer ou de désactiver les résultats de la recherche pour afficher des comptages d'événement et de flux au lieu de comptages moyens dans le temps. Une fois que vous cliquez sur le lien **Enable Unique Counts**, une boîte de dialogue s'ouvre et indique les recherches et les rapports sauvegardés qui partagent les données accumulées.
Current Filters	Cette liste affiche les filtres appliqués à cette recherche. Les options permettant d'ajouter un filtre se trouvent sur la liste **Current Filters**.
Save results when the search is complete	Cette case vous permet de sauvegarder et de nommer les résultats de la recherche.
Display	Cette liste vous permet de sélectionner un ensemble de colonnes prédéfinies dans les résultats de la recherche.
Saisissez Column ou Sélectionner dans la liste	Vous pouvez utiliser ce champ pour filtrer les colonnes qui sont répertoriées dans la liste **Available Columns**. Vous pouvez entrer le nom de la colonne que vous souhaiter localiser ou entrer un mot-clé pour afficher une liste de noms de colonne qui incluent ce mot-clé. Par exemple, saisissez **Device** pour afficher la liste des colonnes qui incluent Device dans le nom de la colonne.
Available Columns	Cette liste affiche des colonnes disponibles. Les colonnes qui sont actuellement en usage pour cette recherche enregistrée sont soulignées et affichées dans la liste **Columns**.

Tableau 7-1 Options de recherche d'événement et de flux

Options	Description
Add and remove column icons (top set)	Les premiers ensembles d'icônes vous permettent de personnaliser la liste **Group By**. • **Add Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Available Columns** et cliquez sur l'icône **Add Column**. • **Remove Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Group By** et cliquez sur l'icône **Remove Column**.
Add and remove column icons (bottom set)	Les derniers ensembles d'icône vous permettent de personnaliser la liste **Columns**. • **Add Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Available Columns** et cliquez sur l'icône **Add Column**. • **Remove Column** - Sélectionnez une ou plusieurs colonnes dans la liste **Columns** et cliquez sur l'icône **Remove Column**.
Group By	Cette liste indique les colonnes sur lesquelles la recherche enregistrée regroupe les résultats. Vous pouvez personnaliser davantage la liste **Group By** en utilisant les options suivantes : • **Move Up** - Sélectionnez une colonne et déplacez-la vers la liste prioritaire en utilisant l'icône **Move Up**. • **Move Down** - Sélectionnez une colonne et déplacez-la vers le bas liste prioritaire en utilisant l'icône **Move Down**. 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 la colonne suivante.
Columns	Indique les colonnes choisies pour la recherche. Vous pouvez sélectionner plus de colonnes dans la liste **Available Columns**. Vous pouvez personnaliser d'avantage la liste **Columns** en utilisant les options suivantes : • **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**. 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. Si le type de colonne est un groupe, la colonne contient une zone de liste qui vous permet de définir le nombre de niveaux que vous souhaitez inclure dans le groupe.

Tableau 7-1 Options de recherche d'événement et de flux

Options	Description
Order By	A partir de la première zone de liste, sélectionnez la colonne dans laquelle vous voulez trier les résultats de la recherche. Puis, dans la deuxième zone de liste, sélectionnez la commande que vous souhaitez afficher pour les résultats de la recherche. Les options incluent **Descending** et **Ascending**.

Procédure

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 enregistrée, allez à **Etape 4**.
- Pour créer une nouvelle recherche, consultez **Etape 5**.

Etape 4 Sélectionnez une recherche précédemment sauvegardé :

a Sélectionnez l'une des options suivantes :

- Dans la liste **Available Saved Searches**, sélectionnez la recherche sauvegardée que vous souhaitez 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**.

c Dans le volet Edit Search, sélectionnez les options que vous voulez pour cette recherche. Voir **Tableau 7-1**.

Etape 5 Dans le volet Time Range, sélectionnez les options pour l'intervalle que vous voulez capturer pour cette recherche. Voir **Tableau 7-1**.

Etape 6 Facultatif. Dans le volet Data Accumulation, activez les comptages uniques :

a Cliquez sur **Enable Unique Counts**.

b Dans la fenêtre Warning, lisez le message d'avertissement puis cliquez sur **Continue**. Pour plus d'informations sur l'activation de comptages uniques, voir **Tableau 7-1**.

Etape 7 Dans le volet Search Parameters, définissez les critères de recherche :

a Dans la zone de liste, sélectionnez un paramètre que vous souhaitez rechercher. Par exemple : Device, Source Port, ou Event Name.

b Dans la deuxième zone de liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche.

c Dans le champ de saisie, saisissez des informations spécifiques liées au paramètre de recherche.

d Cliquez sur **Add Filter**.

e Répétez les étapes **a** à **d** pour chaque filtre que vous souhaitez ajouter aux critères de recherche.

Etape 8 Facultatif. Pour enregistrer automatiquement les résultats de la recherche lorsque la recherche est terminée, cochez la case **Save results when search is complete** puis entrez un nom pour la recherche sauvegardée.

Etape 9 Dans le volet Column Definition, définissez les colonnes et l'agencement de colonne que vous souhaitez utiliser pour afficher les résultats :

a Dans zone de liste **Display**, sélectionnez un ensemble de colonnes préconfigurées pour l'associer à cette recherche.

b Cliquez sur la flèche à côté de **Advanced View Definition** afin d'afficher les paramètres de recherche avancée.

c Personnalisez les colonnes à afficher dans les résultats de la recherche. Voir **Tableau 7-1**.

Etape 10 Cliquez sur **Filter**.

Résultat

Lorsque vous générez une recherche qui s'affiche sur l'onglet **Log Activity** ou **Network Activity** avant que la recherche ne collecte tous les résultats, la page de résultats partielle s'affiche. 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 partiels de la recherche, 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, le statut **Completed** s'affiche dans le coin supérieur droit.

Enregistrement des critères de recherche d'événements et de flux

Dans les onglets **Log Activity** et **Network Activity**, vous pouvez enregistrer les critères de recherche de sorte que vous pussiez réutiliser les critères et utiliser les critères de recherche enregistrées dans les autres composants Détection des anomalies QRadar, tels que les rapports. Les critères de recherche enregistrée n'expirent pas.

A propos de cette tâche

Si vous indiquer un intervalle pour la recherche, Détection des anomalies QRadar ajoute le nom de la recherche à l'intervalle spécifié. Par exemple, une recherche enregistrée nommé Exploits by Source avec un intervalle de 5 dernières minutes devient un Exploits by Source - 5 dernières minutes.

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.

Procédure

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 **Rechercher des événements ou des flux**.

Les résultats de la recherche sont affichés.

Etape 3 Cliquez sur **Save Criteria**.

Etape 4 Entrez la valeur de ces paramètres :

Parameter	Description
Search Name	Saisissez le nom unique que vous souhaitez attribuer à ces critères de recherche.
Assign Search to Group(s)	Cochez cette case pour le groupe auquel 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 groupes de recherche**.
Manage Groups	Cliquez sur **Manage Groups** pour gérer des groupes de recherche. Pour plus d'informations, voir **Gestion de groupes de recherche**.
Timespan options:	Sélectionnez l'une des options suivantes : • **Real Time (streaming)** - Sélectionnez cette option pour filtrer vos résultats de la recherche en mode de diffusion. Pour plus d'informations sur le mode de diffusion, voir **Affichage des événements en continu** ou **Affichage des flux en continu**. • **Last Interval (auto refresh)** - Sélectionnez cette option pour filtrer vos résultats de la recherche en mode d'actualisation automatique. Les onglets **Log Activity** et **Network Activity** s'actualisent par intervalles d'une minute pour afficher les informations les plus récentes. • **Recent** - Sélectionnez cette option et, dans cette zone de liste, sélectionnez l'intervalle que souhaiter filtrer. • **Specific Interval** - Sélectionnez cette option et, à partir de l'agenda, sélectionnez la date et l'intervalle que vous souhaitez filtrer.
Include in my Quick Searches	Cochez cette case pour inclure cette recherche dans votre zone de liste **Quick Search**, qui se trouve sur les barres d'outils **Log Activity** et **Network Activity**.
Include in my Dashboard	Cochez cette case pour inclure les données dans vos recherches sauvegardées sur l'onglet **Dashboard**. Pour plus d'informations sur l'onglet **Dashboard**, voir **Gestion du tableau de bord**. ***Remarque :*** *Ce paramètre ne s'affiche que si la recherche est regroupée.*
Set as Default	Cochez cette case pour définir cette recherche comme votre recherche par défaut lorsque vous accédez à l'onglet **Log Activity** ou **Network Activity**.

Parameter	Description
Share with Everyone	Cochez cette case pour partager ces critères de recherche avec tous les autres utilisateursDétection des anomalies QRadar.

Etape 5 Cliquez sur **OK**.

Recherches de violations

You pouvez rechercher des violations en utilisant des critères spécifiques pour afficher des violations correspondant à des critères de recherche dans une liste de résultats. Vous pouvez créer ou charger un ensemble de critères de recherche précédemment enregistrées.

Recherche de violations sur les pages My Offenses and All Offenses

Dans les pages **My Offenses** et **All Offenses** de l'onglet **Offense**, vous pouvez rechercher des violations qui correspondent à vos critères.

A propos de cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser pour rechercher des données de violation dans les pages My Offenses et All Offenses :

Tableau 7-2 Options de recherche de pages My Offenses et All Offenses

Options	Description
Group	Cette zone de liste vous permet de sélectionner un groupe de recherche de violations à afficher dans la liste **Available Saved Searches**.
Entrez Saved Search ou Select from List	Ce champ vous permet d'entrer le nom de la recherche enregistrée ou un mot-clé pour filtrer la liste **Available Saved Searches**.
Available Saved Searches	Cette liste affiche toutes les recherches disponibles sauf si vous appliquez un filtre à la liste en utilisant les options **Group or Type Saved Search** ou **Select from List**. Vous pouvez sélectionner une recherche enregistrée sur la liste à afficher ou à modifier.
All Offenses	Cette option vous permet de rechercher toutes les violations sans tenir compte de la plage horaire.
Recent	Cette option vous permet de sélectionner un intervalle prédéfini pendant lequel vous souhaitez appliquer le filtre. Une fois que vous choisissez cette option, vous devez sélectionner un intervalle dans la zone de liste.

Tableau 7-2 Options de recherche de pages My Offenses et All Offenses

Options	Description
Specific Interval	Cette option vous permet de configurer un intervalle personnalisé pour votre recherche. Une fois que vous choisissez cette option, vous devez sélectionner l'une des options suivantes. • **Start Date between** - Cochez cette case pour rechercher des violations qui ont commencé durant une période bien définie. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. • **Last Event/Flow between** - Cochez cette case pour rechercher des violations pour lesquelles le dernier événement détecté s'est déroulé dans une période bien définie. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Recherche	L'icône **Search** est disponible dans plusieurs volets sur la page de recherche. Vous pouvez cliquer sur **Search** une fois que vous avez terminé la configuration la de recherche et que vous souhaitez afficher les résultats.
ID de violation	Dans ce champ, vous pouvez entrer l'ID de violation que vous souhaitez rechercher.
Description	Dans ce champ, vous pouvez entrer la description que vous souhaitez rechercher.
Assigned to user	Dans cette zone de liste, vous pouvez sélectionner le nom d'utilisateur que vous souhaitez rechercher.
Direction	Dans cette zone de liste, vous pouvez sélectionner la direction de la violation que vous souhaitez rechercher. Ces options incluent : • Local to Local • Local to Remote • Remote to Local • Remote to Remote • Local to Remote ou Local • Remote to Remote ou Local
IP source	Dans ce champ, vous pouvez entrer l'adresse IP source ou la plage CIDR que vous souhaitez rechercher.
Destination IP	Dans ce champ, vous pouvez entrer l'adresse IP de destination ou la plage CIDR que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez spécifier une amplitude et puis sélectionner de n'afficher que les violations avec une amplitude qui es égale à, inférieure à ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.
Severity	Dans la zone de liste, vous pouvez indiquer une gravité puis choisir de n'afficher que les violations dont la gravité est égale à, inférieure à ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.

Tableau 7-2 Options de recherche de pages My Offenses et All Offenses

Options	Description
Credibility	Dans cette zone de liste, vous pouvez indiquer une crédibilité et choisir de n'afficher que les violations dont la crédibilité est égale à, inférieure à ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.
Relevance	Dans la zone de liste, vous pouvez indiquer une importance et choisir de n'afficher que les violations qui sont égales à, inférieures à ou supérieures à la valeur configurée. L'intervalle se situe entre 0 et 10.
Contains Username	Dans ce champ, vous pouvez entrer une expression régulière (regex) pour rechercher les violations contenant un nom d'utilisateur spécifique. Lorsque vous définissez des modèles d'expressions régulières personnalisés, conformez vous aux règles d'expressions régulières tel que définies par le langage de programmation de Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.
Source IP	Dans la zone de liste, vous pouvez sélectionner le réseau source que vous souhaitez rechercher.
Destination Network	Dans cette zone de liste, vous pouvez sélectionner le réseau de destination que vous souhaitez rechercher.
High Level Category	Dans cette zone de liste, vous pouvez sélectionner la catégorie de haut niveau que vous souhaitez rechercher. Pour plus d'informations sur catégories, voir *IBM Security QRadar Network Anomaly Detection - Guide d'administration.*
Low Level Category	Dans la zone de liste, vous pouvez sélectionner la catégorie de niveau faible que vous souhaitez rechercher. Pour plus d'informations sur les catégories, voir *IBM Security QRadar Network Anomaly Detection - Guide d'administration.*
Exclude	Cette option qui se trouve dans ce volet vous permet d'exclure des violations des résultats de la recherche. Les options incluent : • Active Offenses • Hidden Offenses • Closed Offenses • 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 Exclude. Dans cette zone de liste, vous pouvez cocher le nom d'utilisateur dont vous souhaitez rechercher les violations fermées ou cocher **Any** pour afficher toutes les violations fermées.

Tableau 7-2 Options de recherche de pages My Offenses et All Offenses

Options	Description
Reason For Closing	Ce paramètre ne s'affiche que lorsque la case **Closed Offenses** n'est pas cochée dans le panneau Exclude. Dans cette zone de liste, vous pouvez sélectionner une raison pour laquelle vous souhaitez rechercher des violations fermées ou cocher **Any** pour afficher toutes les violations.
Events	Dans cette zone de liste, vous pouvez indiquer un comptage d'événement et choisir de n'afficher que les violations dont le comptage d'événement est égal à, inférieur à ou supérieur à la valeur configurée.
Flows	Dans cette zone liste, vous pouvez indiquer un comptage de flux et puis sélectionner que les violations dont le comptage de flux est égal à, inférieur à ou supérieur à la valeur configurée.
Total Events/Flows	Dans cette zone de liste, vous pouvez indiquer un comptage total d'événement et de flux et puis choisir de n'afficher que les violations dont le comptage total d'événement et de flux est égal à, inférieur à ou supérieur à la valeur configurée.
Destinations	Dans cette zone liste, vous pouvez indiquer un comptage d'adresse IP de destination et puis sélectionner que les violations dont le comptage d'adresse IP de destination est égal à, inférieur à ou supérieur à la valeur configurée.
Log Source Group	Dans cette zone de liste, vous pouvez sélectionner un groupe de sources de journal qui contient la source de journal que vous souhaitez rechercher. La zone de liste **Log Source** affiche toutes les sources de journal affectées au groupe de source de journal.
Log Source	Dans cette zone de liste, vous pouvez sélectionner la source de journal que vous souhaitez rechercher.
Rule Group	Dans cette zone de liste, vous pouvez sélectionner un groupe de règle contenant la règle de contribution que vous souhaitez rechercher. La zone de liste **Rule** affiche toutes les règles affectées au groupe de règle sélectionné.
Rule	Dans cette zone de liste, vous pouvez sélectionner la règle de contribution que vous souhaitez rechercher.
Offense Type	Dans cette zone de liste, vous pouvez sélectionner un type de violation que vous souhaitez rechercher. Pour plus d'informations sur les options dans la zone de liste **Offense Type**, voir **Tableau 7-3**.

Le tableau suivant décrit les options disponibles dans la zone de liste Offense Type :

Tableau 7-3 Options Offense type

Types de violation	Description
Any	Cette option recherche toutes les sources de violation.

Tableau 7-3 Options Offense type (suite)

Types de violation	Description
IP source	Pour rechercher des violations avec une adresse IP source spécifique, vous pouvez sélectionner cette option, puis entrer l'adresse IP source que souhaitez rechercher.
Destination IP	Pour rechercher des violations avec une adresse IP de destination spécifique, vous pouvez sélectionner cette option et puis entrer la destination de l'adresse IP que souhaitez rechercher.
Event Name	Pour rechercher des violations avec un nom d'événement spécifique, vous pouvez cliquer sur l'icône **Browse** pour ouvrir le navigateur d'événement et sélectionner l'e nom de l'événement (QID) que vous souhaitez rechercher. Vous pouvez rechercher un QID particulier à l'aide des options suivantes : • 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**.
Username	Pour rechercher des violations avec un nom d'utilisateur spécifique, vous pouvez sélectionner cette option et puis entrer la user de l'adresse name que souhaitez rechercher.
Source MAC Address	Pour rechercher des violations avec une adresse MAC source, vous pouvez sélectionner et puis entrez l'adresse MAC source que vous souhaitez rechercher.
Destination MAC Address	Pour rechercher des violations avec une adresse MAC de destination spécifique, vous pouvez sélectionner cette option et entrez l'adresse MAC de destination que vous souhaitez rechercher.
Log Source	Dans la zone de liste **Log Source Group**, vous pouvez sélectionner le groupe de source de journal contenant la source de journal que vous souhaitez rechercher. La zone de liste **Log Source** affiche toutes les sources de journal affectées au groupe de source de journal sélectionné. Dans la zone de liste **Log Source**, sélectionnez la source de journal que vous souhaitez rechercher.
Host Name	Pour rechercher toutes les violations avec un nom d'hôte spécifique, vous pouvez sélectionner cette option et puis entrer le nom d'hôte que vous souhaitez rechercher.
Source Port	Pour rechercher les violations avec un port source spécifique, vous pouvez sélectionner cette option puis entrez le port source que vous souhaitez rechercher.

Tableau 7-3 Options Offense type (suite)

Types de violation	Description
Destination Port	Pour rechercher des violations avec un port de destination spécifique, vous pouvez entrer le port de destination que vous souhaiter rechercher.
Source IPv6	Pour rechercher des violations avec une adresse IPv6 source, vous pouvez sélectionner cette option et puis entrer l'adresse IPv6 source que vous souhaitez rechercher.
Destination IPv6	Pour rechercher des violations avec une adresse IPv6 de destination, vous pouvez sélectionner cette option et puis entrer l'adresse IPv6 de destination que vous souhaitez rechercher.
Source ASN	Pour rechercher des violations avec un avis préalable d'expédition source spécifique, vous pouvez sélectionner l'avis préalable d'expédition source dans la zone de liste **Source ASN**.
Destination ASN	Pour rechercher des violations avec une destination ASN spécifique, vous pouvez sélectionner la destination dans la zone de liste **Destination ASN**.
Rule	Pour rechercher des violations associées à une règle spécifique, vous pouvez sélectionner le groupe de règle contenant la règle que vous souhaitez rechercher dans la zone de liste **Rule Group.** La zone de liste **Rule Group** affiche toutes les règles affectées au groupe de règle sélectionné. Dans la zone de liste **Rule**, vous pouvez sélectionner la règle que vous souhaitez rechercher.
App ID	Pour rechercher des violations avec un ID d'application, vous pouvez sélectionner l'ID d'application dans la zone de liste **App ID.**

Procédure

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, consultez **Etape 4**.
- Pour créer une nouvelle recherche, consultez **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 Facultatif. Sélectionnez la case **Set as Default** pour définir cette recherche comme votre recherche par défaut.

Si vous définissez cette recherche comme la recherche par défaut, la recherche s'effectue automatiquement et affiche des résultats à chaque fois que vous accédez à l'onglet **Offenses**.

Etape 7 Dans le volet Time Range, sélectionnez une option pour l'intervalle que vous voulez capturer pour cette recherche. Voir **Tableau 7-2**.

Etape 8 Dans le volet Search Parameters, définissez les critères de recherche spécifique. Voir **Tableau 7-2**.

Etape 9 Dans le volet 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 vos paramètres de recherche. Voir **Tableau 7-3**.

Etape 10 Dans le volet 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 Dans la deuxième zone de liste, sélectionnez la commande que vous souhaitez afficher pour les résultats de la recherche. Les options incluent **Descending** et **Ascending**.

Etape 11 Cliquez sur **Search**.

Etape suivante

Enregistrement des critères de recherche dans l'onglet Offense

Recherche de violations sur la page By Source IP

Cette rubrique fournit la procédure pour rechercher des violations sur la page **By Source IP** de l'onglet **Offense**.

A propos de cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser sur la page By Source IP :

Tableau 7-4 Options de recherche de page By Source IP All Offenses

Options	Description
All Offenses	Vous pouvez sélectionner cette option pour rechercher toutes les adresses IP source sans tenir compte de l'intervalle.
Recent	Vous pouvez sélectionner cette option et, dans la zone de liste, sélectionnez la plage horaire que vous souhaiter rechercher.

Tableau 7-4 Options de recherche de page By Source IP All Offenses

Options	Description
Specific Interval	Pour indiquer un intervalle à rechercher, vous pouvez sélectionner l'option Specific Interval et puis sélectionner l'une des options suivantes : • **Start Date between** - Cochez cette case pour rechercher des adresses IP source associées à des violations qui ont commencé au cours d'un certain intervalle de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. • **Last Event/Flow between** - Cochez cette case pour rechercher des adresses IP source associées aux violations pour lesquelles le dernier événement détecté s'est déroulé dans une période bien définie. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Search	L'icône **Search** est disponible dans plusieurs volets sur la page de recherche. Vous pouvez cliquer sur **Search** une fois que vous avez terminé la configuration la de recherche et que vous souhaitez afficher les résultats.
Source IP	Dans ce champ, vous pouvez entrer l'adresse IP ou la plage CIDR que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez pouvez indiquer une amplitude et choisir de n'afficher que les violations avec une amplitude qui est égale à, inférieure à ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.
Risque VA	Dans cette zone de liste, vous pouvez indiquer un risque VA et choisir de n'afficher que les violations avec un risque VA qui est égal à, inférieur à ou supérieur à la valeur configurée. L'intervalle est compris entre 0 et 10.
Events/Flows	Dans cette zone de liste, vous pouvez indiquer un comptage d'événement ou de flux et choisir de n'afficher que les violations avec une amplitude qui est égale à, inférieure à ou supérieure à la valeur configurée.
Exclude	Vous pouvez cocher les cases pour les violations que vous souhaitez exclure des résultats de la recherche. Les options sont les suivantes : • Active Offenses • Hidden Offenses • Closed Offenses • Inactive offenses • Protected Offense

Procédure

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 volet Time Range, sélectionnez une option pour l'intervalle que vous souhaitez capturer pour cette recherche. Voir **Tableau 7-4**.

Etape 5 Dans le volet Search Parameters, définissez les critères de recherche spécifique. Voir **Tableau 7-4**.

Etape 6 Dans le volet 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** Dans la deuxième zone de liste, sélectionnez la commande que vous souhaitez afficher pour les résultats de la recherche. Les options incluent **Descending** et **Ascending**.

Etape 7 Cliquez sur **Search**.

Etape suivante

Enregistrement des critères de recherche dans l'onglet Offense

Recherche de violations sur la page By Destination IP

Sur la page **By Destination IP** de l'onglet **Offense**, vous pouvez rechercher des violations regroupées par adresse IP de destination.

A propos de cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser pour rechercher des violations sur la page By Destination IP :

Tableau 7-5 Options de recherche de page By Destination IP All Offenses

Options	Description
All Offenses	Vous pouvez sélectionner cette option pour rechercher toutes les adresses IP de destination sans tenir compte de l'intervalle.
Recent	Vous pouvez sélectionner cette option et, dans cette zone de liste, sélectionnez l'intervalle que vous souhaiter rechercher.
Specific Interval	Pour indiquer un intervalle à rechercher, vous pouvez sélectionner l'option Specific Interval et sélectionner l'une des options suivantes : • **Start Date between** - Cochez la case pour rechercher les adresses IP de destination associées à des violations qui ont commencé au cours d'un certain intervalle de temps. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. • **Last Event/Flow between** - Cochez cette case pour rechercher des adresses IP de destination associée aux violations pour lesquelles le dernier événement détecté s'est déroulé dans une période bien définie. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Search	L'icône **Search** est disponible dans plusieurs volets sur la page de recherche. Vous pouvez cliquer sur **Search** une fois que vous avez terminé la configuration de la recherche et que vous souhaitez afficher les résultats.
Destination IP	Vous pouvez entrer l'adresse IP de destination ou la plage CIDR que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez spécifier une amplitude et puis choisir de n'afficher que les violations avec une amplitude qui es égale à, inférieure à ou supérieure à la valeur configurée.
VA Risk	Dans cette zone de liste, vous pouvez indiquer un risque VA et choisir de n'afficher que les violations avec un risque VA qui est égal à, inférieur à ou supérieur à la valeur configurée. L'intervalle est compris entre 0 et 10.
Events/Flows	Dans cette zone de liste, vous pouvez indiquer une amplitude de comptage d'événement ou de flux et puis choisir de n'afficher que les violations dont le comptage d'événement est égal à, inférieur à ou supérieur à la valeur configurée.

Procédure

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 volet Time Range, sélectionnez une option pour l'intervalle que vous souhaitez capturer pour cette recherche. Voir **Tableau 7-5**.

Etape 5 Dans le volet Search Parameters, définissez les critères de recherche caractéristique. Voir **Tableau 7-5**.

Etape 6 Dans le volet 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 Dans la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de la recherche.Les options comprennent **Descending** et **Ascending**.

Etape 7 Cliquez sur **Search**.

Etape suivante

Enregistrement des critères de recherche dans l'onglet Offense

Recherche de violations sur la page By Networks

Dans la page **By Network** de l'onglet **Offense**, vous pouvez rechercher des violations regroupées par les réseaux associés.

A propos de cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser sur la page By Network IP :

Tableau 7-6 By Options de recherche de page Network

Options	Description
Network	Dans cette zone de liste, vous pouvez sélectionner le réseau que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez indiquer une amplitude et choisir de n'afficher que les violations avec une amplitude qui est égale à, inférieure à ou supérieure à la valeur configurée.
VA Risk	Dans cette zone de liste, vous pouvez indiquer un risque VA et choisir de n'afficher que les violations avec un risque VA qui est égal à, inférieur à ou supérieur à la valeur configurée.
Event/Flows	Dans cette zone de liste, vous pouvez indiquer un comptage d'événement ou de flux et puis choisir de n'afficher que les violations dont le comptage d'événement est égal à, inférieur à ou supérieur à la valeur configurée.

Procédure

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 volet Search Parameters, définissez les critères de recherche spécifique. Voir **Tableau 7-6**.

Etape 5 Dans le volet 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 Dans la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de la recherche.Les options comprennent **Descending** et**Ascending**.

Etape 6 Cliquez sur **Search**.

Etape suivante

Enregistrement des critères de recherche dans l'onglet Offense

Enregistrement des critères de recherche dans l'onglet Offense

Dans l'onglet **Offenses**, vous pouvez enregistrer des critères de recherche pour pouvoir réutiliser les critères pour des recherches ultérieures. Les critères de recherche enregistrée n'expirent pas.

Procédure

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

Etape 2 Effectuez une recherche. Voir **Recherches de violations**.

Les résultats de la recherche sont affichés.

Etape 3 Cliquez sur **Save Criteria**.

Etape 4 Entrez les valeurs pour les paramètres suivants :

Paramètre	Description
Search Name	Entrez un nom que vous souhaitez attribuer à ces critères de recherche.
Assign Search to Group(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.
Manage Groups	Cliquez sur **Manage Groups** pour gérer des groupes de recherche. Voir **Gestion de groupes de recherche**.

Paramètre	Description
Timespan options:	Sélectionnez l'une des options suivantes : • **All Offenses** - Sélectionnez cette option pour rechercher toutes les violations quel que soit l'intervalle de temps. • **Recent** - Sélectionnez cette option puis, dans cette zone de liste, sélectionnez l'intervalle que vous souhaitez rechercher. • **Specific Interval** - Pour spécifier un intervalle à rechercher, sélectionnez l'option **Specific Interval**, et puis sélectionnez les options suivantes : **Start Date between** - Cochez cette case pour rechercher les violations qui ont commencé durant une période bien définie. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher. **Last Event/Flow between** - Cochez cette case pour rechercher des violations pour lesquelles le dernier événement détecté s'est déroulé dans une période bien définie. Une fois que vous cochez cette case, utilisez les zones de liste pour sélectionner la date que vous souhaitez rechercher.
Set as Default	Cochez cette case pour définir cette recherche comme votre recherche par défaut.

Etape 5 Cliquez sur **OK**.

Suppression de critères de recherche

Si les critères de recherche enregistrée ne sont plus requis, vous pouvez supprimer les critères de recherche.

A propos de cette tâche

Lorsque vous supprimez une recherche enregistrée, les objets Détection des anomalies QRadar associés à la rechercher enregistrée peut ne plus fonctionner. Les rapports et les règles de détection d'anomalies sont des objetsDétection des anomalies QRadar qui utilisent des critères de recherche sauvegardés. Une fois que vous supprimez une recherche enregistrée, modifiez les objets associés pour s'assurer qu'il continuent de fonctionner.

Procédure

Etape 1 Choisissez 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 objetsDétection 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. Notez les objets associés. Voir **Etape 6**.

Etape 5 Cliquez sur **OK**.

Etape 6 C - Sélectionnez une des options suivantes :

- Cliquez sur **OK** pour continuer. La recherche enregistrée est maintenant supprimée.
- Cliquez sur **Cancel** pour fermer la fenêtre Delete Saved Search.

Etape suivante

Si les critères de recherche ont été associés à d'autres objetsDétection des anomalies QRadar, accédez aux objets que vous avez notés et modifiez-les pour supprimer ou remplacer l'association avec la recherche enregistrée qui a été supprimée.

Effectuer une sous-recherche

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.

A propos de cette tâche

Cette fonction n'est pas disponible pour les recherches regroupées, les recherches en cours, ou en mode de diffusion.

Avant de commencer

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.

Procédure

Etape 1 Choisissez l'une des options suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Effectuez une recherche. Voir **Rechercher des événements ou des flux**.

Etape 3 Lorsque vous terminez votre recherche, ajoutez un autre filtre :

a Cliquez sur **Add Filter**.

b Dans la première zone de liste, sélectionnez un paramètre que vous souhaitez rechercher.

c Dans 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 le champ de saisie, saisissez des informations spécifiques liées à votre recherche.

e Cliquez sur **Add Filter**.

Résultat

Le volet Original Filter indique les filtres d'origine appliqués à la recherche de base. Le volet Current Filter indique les filtres appliqués à la sous-recherche. Vous pouvez effacer les filtres de sous- recherche 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.

Si vous supprimez les critères de recherche de base des critères de sous-recherche 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

Etape suivante

Enregistrement des critères de recherche d'événements et de flux

Gestion des résultats de recherche d'événements et de flux

Vous pouvez initier plusieurs recherches d'événement et de flux puis naviguer vers d'autres onglets pour effectuer d'autres tâches pendant que votre recherche se termine dans l'arrière-plan. Vous pouvez configurer une recherche pour qu'elle vous envoie une notification par courrier électronique lorsque la recherche se termine. A tout moment pendant qu'une recherche est en cours, vous pouvez retourner vers les onglets **Log Activity** ou **Network Activity** pour afficher des résultats partiels ou complets.

Enregistrement des résultats de recherche

Une fois que vous effectuez une recherche d'événement ou de flux, vous pouvez enregistrer les résultats de la recherche.

A propos de cette tâche

Si vous effectuez une recherche et que vous n'enregistrez pas de façon explicite les résultats de la recherche. Ces derniers sont disponibles sur les fenêtres Manage Search pendant 24 heures et sont automatiquement supprimés.

Procédure

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 **Rechercher des événements ou des flux**.

Etape 3 Cliquez sur **Save Results**.

Etape 4 Sur la fenêtre Save Search Result, entrez un seul nom pour les résultats de la recherche.

Etape 5 Cliquez sur **OK**.

Affichage des résultats de recherche gérés

En utilisant la page Manage Search Results, vous pouvez afficher des résultats de recherche complets ou partiels.

A propos de cette tâche

La fonction Saved Search Results conserve les configurations graphiques dans les critères de recherche associés, cependant, si le résultat de la recherche est basé sur les critères qui ont été supprimés, les graphiques (barre et graphique circulaire) par défaut s'affichent.

La page Manage Search Results fournit les paramètres suivants :

Tableau 7-7 Paramètres de la page Manage Search Results

Paramètre	Description
Flags	Indique qu'une notification par courrier électronique est en attente pour la fin de la recherche.
User	Indique le nom de l'utilisateur ayant lancé la recherche.
Name	Spécifie le nom de la recherche, si la recherche a été enregistrée. Pour plus d'informations sur la sauvegarde d'une recherche, voir **Enregistrement des résultats de recherche**.
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.

Tableau 7-7 Paramètres de la page Manage Search Results (suite)

Paramètre	Description
Expires On	Indique la date et l'heure d'expiration d'un résultat de recherche non enregistrée. 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, voir *IBM Security QRadar Network Anomaly Detection - Guide d'administration*.
Status	Indique le statut de la recherche. Les statuts sont : • **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 **Surveillance de l'activité du journal** ou **Surveillance de l'activité du réseau**.
Taille	Indique la taille du fichier de l'ensemble des résultats de la recherche.

La barre d'outils de la fenêtre The Manage Search Results fournit les fonctions suivantes :

Tableau 7-8 Barre d'outils Manage Search Results

Fonction	Description
New Search	Cliquez sur **New Search** afin de créer une recherche. Lorsque vous cliquez sur cette icône, la page de recherche s'affiche. Voir **Rechercher des événements ou des flux**.
Save Results	Cliquez sur **Save Results** pour sauvegarder les résultats de la recherche sélectionnée. Voir **Enregistrement des résultats de recherche**.
Cancel	Cliquez sur **Cancel** pour annuler les résultats de recherche sélectionnés qui sont en cours ou en attente de lancement. Voir **Annulation d'une recherche**.
Delete	Cliquez sur **Delete** pour supprimer le résultat de recherche sélectionné. Voir **Suppression d'un résultat de recherche**.
Notify	Cliquez sur **Notify** pour activer la notification par courrier électronique lorsque la recherche sélectionnée est terminée s.

Tableau 7-8 Barre d'outils Manage Search Results (suite)

Fonction	Description
View	Dans cette zone de liste, vous pouvez sélectionner les résultats de la recherche que vous souhaitez répertorier sur la page Search Results. Les options incluent : • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

Procédure

Etape 1 Sélectionnez l'une des options suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Dans le menu Search, sélectionnez **Manage Search Results**.

Etape 3 Affichez la liste des résultats de la recherche. Voir **Tableau 7-7**.

Etape suivante

Annulation d'une recherche

Suppression d'un résultat de recherche

Annulation d'une recherche

Pendant qu'une recherche est en attente ou en cours, vous pouvez annuler la recherche dans la page Manage Search Results.

A propos de cette tâche

Si la recherche était en cours au moment où vous l'annulez, les résultats qui étaient accumulés sont maintenus.

Procédure

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**.

Etape 3 Sélectionnez le résultat de recherche en attente ou en cours que vous souhaitez annuler.

Etape 4 Cliquez sur **Cancel**.

Etape 5 Cliquez sur **Yes**.

Suppression d'un résultat de recherche

Si un résultat de la recherche n'est pas requis, vous pouvez supprimer le résultat de la recherche de la page Manage Search Results.

Procédure

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**.

Etape 3 Sélectionnez le résultat de la recherche que vous souhaitez supprimer.

Etape 4 Cliquez sur **Delete**.

Etape 5 Cliquez sur **Yes**.

Gestion de groupes de recherche

A l'aide de la fenêtre Search Groups, vous pouvez créer et gérer des groupes de recherche. Ces groupes vous permettent de localiser facilement des critères de recherche sur les onglets **Log Activity**, **Network Activity** et **Offenses** puis dans l'Assistant de Rapport.

Affichage de groupes de recherche

Détection des anomalies QRadar fournit une définition de groupes et de sous-groupes par défaut, que vous pouvez afficher dans les fenêtres Event Search Group, Flow Search Group ou Offense Search Group.

A propos de cette tâche

Toutes les recherches enregistrées qui ne sont pas affectés à un groupe se trouvent dans le groupe **Other.**

Les fenêtres Event Search Group, Flow Search Group et Offense Search Group affichent les paramètres suivants pour chaque groupe :

Tableau 7-9 Paramètres de la fenêtre Search Group

Paramètre	Description
Name	Indique le nom du groupe de recherche.
User	Indique le nom de l'utilisateur qui a créé le groupe de recherche.
Description	Indique la description du groupe de recherche.
Date Modified	Indique la date à laquelle le groupe de recherche a été modifié.

Les barres d'outils des fenêtres Event Search Group, Flow Search Group et Offense Search Group fournissent les fonctions suivantes :

Tableau 7-10 Les fonctions de la barre d'outils Search Group

Fonction	Description
New Group	Pour créer un nouveau groupe de recherche, vous pouvez cliquer sur **New Group**. Voir **Création d'un nouveau groupe de recherche**.
Edit	Pour modifier un groupe de recherche existant, vous pouvez cliquer sur **Edit**. Voir **Modification d'un groupe de recherche**.

Tableau 7-10 Les fonctions de la barre d'outils Search Group (suite)

Fonction	Description
Copy	Pour copier une recherche enregistrée vers un autre groupe de recherche, vous pouvez cliquer sur **Copy**. Voir **Copie d'une recherche enregistrée sous un autre groupe**.
Remove	Pour supprimer un groupe de recherche ou une recherche enregistrée à partir d'un groupe de recherche, sélectionnez l'élément que vous souhaitez retirer et cliquez sur **Remove**. Voir **Suppression d'un groupe ou d'une recherche enregistrée dans un groupe**.

Procédure

Etape 1 Choisissez 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**.

Etape 4 Afficher les groupes de recherche. Voir **Tableau 7-9**.

Etape suivante

Création d'un nouveau groupe de recherche

Modification d'un groupe de recherche

Copie d'une recherche enregistrée sous un autre groupe

Suppression d'un groupe ou d'une recherche enregistrée dans un groupe

Création d'un nouveau groupe de recherche

Dans les fenêtres Event Search Group, Flow Search Group et Offense Group Search, vous pouvez créer un nouveau groupe de recherche.

Procédure

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**.

Etape 4 Sélectionnez le dossier du nouveau groupe dans lequel vous souhaitez créer le nouveau groupe.

Etape 5 Cliquez sur **New Group**.

Etape 6 Dans la zone **Name**, saisissez un nom unique du nouveau groupe.

Etape 7 Facultatif. Dans la zone **Description**, saisissez une description.

Etape 8 Cliquez sur **OK**.

Modification d'un groupe de recherche

Vous pouvez modifier les champs **Name** et **Description** d'un groupe de recherche.

Procédure

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**.

Etape 4 Sélectionnez le groupe que vous souhaitez modifier.

Etape 5 Cliquez sur **Edit**.

Etape 6 Modifiez les paramètres :

- Entrez un nouveau nom dans le champ **Name**.
- Entrez une nouvelle description dans le champ **Description** field.

Etape 7 Cliquez sur **OK**.

Copie d'une recherche enregistrée sous un autre groupe

Vous pouvez copier une recherche enregistrée vers un autre groupe. Vous pouvez copier la recherche enregistrée vers plusieurs groupes.

Procédure

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**.

Etape 4 Sélectionnez la recherche enregistrée que vous souhaitez copier.

Etape 5 Cliquez sur **Copy**.

Etape 6 Dans la fenêtre Item Groups, cochez la case du groupe vers lequel vous souhaitez copier la recherche enregistrée.

Etape 7 Cliquez sur **Assign Groups**.

Suppression d'un groupe ou d'une recherche enregistrée dans un groupe

Vous pouvez utiliser l'icône Remove pour supprimer une recherche d'un groupe ou d'un groupe de recherche.

A propos de cette tâche

Lorsque vous supprimez une recherche enregistrée d'un groupe, la recherche enregistrée ne sera pas supprimée de votre système. La recherche enregistrée est supprimée du groupe et déplacée automatiquement vers le groupe **Other**.

Il est impossible de supprimer les groupes suivants de votre système :

- Event Search Groups
- Flow Search Groups
- Offense Search Groups
- Other

Procédure

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**.

Etape 4 Sélectionnez l'une des options suivantes :

- Sélectionnez la recherche sauvegardée que vous voulez supprimer du groupe.
- Sélectionnez le groupe que vous souhaitez supprimer.

Etape 5 Cliquez sur **Remove**.

Etape 6 Cliquez sur **OK**.

8 PROPRIÉTÉS D'ÉVÉNEMENTS ET DE FLUX PERSONNALISÉS

Les propriétés d'événements et de flux vous permettent de rechercher, d'afficher et de produire un rapport sur les informations figurant dans les journaux n'étant généralement ni normalisées ni affichées par QRadar Network Anomaly Detection.

Présentation des propriétés personnalisées

Vous pouvez créer des propriétés d'événement et de flux personnalisés à partir de plusieurs emplacements via les onglets du journal **d'activité** or **Network Activity**:

- **Détails de l'événement** - Vous pouvez sélectionner un événement à partir de l'onglet **Log Activity** pour créer une propriété d'événement personnalisé tirée de son contenu.
- **Détails du flux** - Vous pouvez sélectionner un flux à partir de l'onglet **Network Activity** pour créer une propriété flow property personnalisé tirée de son contenu.
- **Page de recherche** -Vous pouvez créer et modifier un événement ou propriété personnalisé à partir de la page de recherche. Lorsque vous créez une nouvelle propriété personnalisée à partir de la page de recherche, la propriété d'événement ne provient pas d'un événement ou d'un flux particulier et, par conséquent, la fenêtre de définition de la propriété personnalisée n'est pas préremplie. Vous pouvez copier et coller le contenu des informations à partir d'une autre source.

Autorisations requises

Pour créer des propriétés ppersonnalisées, il est nécessaire que vous ayez l'autorisation **User Defined Event Properties** ou **User Defined Flow Properties**. Si vous disposez d'autorisations de l'administrateur, vous pouvez également créer et modifier les propriétés personnalisées à partir de l'onglet **Admin.** Cliquez sur **Admin > Data Sources > Custom Event Properties** ou **Admin > Data Sources > Custom Flow Properties**. Vérifiez avec votre administrateur pour vous assurer que vous disposez d'autorisations requises. Pour de plus amples informations sur les autorisations, consultez le guide administrateur *IBM Security QRadar Network Anomaly Detection.*

Types de propriétés personnalisées

Lorsque vous créez une propriété personnalisée, vous pouvez choisir de créer une propriété personnalisée de ce type:

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

  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, QRadar Network Anomaly Detection en règle générale ne peut pas afficher le compte utilisateur courant ou l'autorisation qui a été modifiée. Vous pouvez créer une propriété personnalisée pour extraire cette information des journaux, et ensuite utiliser la propriété dans les recherches et les rapports.

  L'utilisation de cette fonctionnalité requiert une connaissance avancée des expressions régulières (regex). L'expression régulière définit le champ que vous souhaitez voir devenir la propriété personnalisée. 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 vous référer aux tutoriels d'expression régulière disponibles sur le web.

  Une propriété personnalisée peut être associée à plusieurs expressions régulières. Lorsqu'un événement ou un flux est analysé, chaque modèle d'expression régulière est testé sur l'événement ou le flux jusqu'à ce qu'il corresponde au contenu. Le premier modèle d'expression régulière correspondant au contenu d'événement ou de flux 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 ou de flux 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.

Gestion des propriétés personnalisées

vous pouvez créer, modifier, copier et supprimer les propriétés personnalisées.

Création d'une propriété personnalisée basée sur l'expression régulière

Vous pouvez créer can create une propriété clientbasée sur l'expression régulière p pour faire correspondre les contenusd'événements ou de flux avec l'expression régulière.

A propos de cette tâche

Lorsque vous configurez une propriété personnalisée basée sur l'expression régulière, les fenêtres de propriété d'événement personnalisé ou de propriété de flux personnalisé fournissent les paramètres suivants:

Tableau 8-1 Custom property definition window parameters (regex)

Paramètre	Description
Champ de test	Indiquez le contenu qui a été extrait de des événements non normalisés ou des de flux.
Définition des Depropriétés	
Propriété existante	Pour sélectionner une propriété existante, sélectionnez cette option, ensuite sélectionnez un nom de propriété déjà sauvegardé à partir de la zone de liste.
Nouvelle propriété	Pour créer une nouvelle propriété, sélectionnez cette option et entrez un nom unique pour cette propriété de p 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*.
Optimisez l'analyse syntaxique des règles, des rapports et des recherches	Pour analyser et stocker la propriété la première fois que QRadar Network Anomaly Detection reçoit l'événement ou le flux, sélectionnez la case à cocher. Lorsque vous sélectionnez la case à cocher, la propriété ne nécessite aucune analyse supplémentaire de test de rapport, de recherche ou de règle. Si vous désélectionnez cette case à cocher, la propriété est analysée à chaque fois que le test de rapport de recherche ou de règle est effectué. Cette option est désactivée par défaut.
	Dans la zone de liste, sélectionnez le type de zone. Le type de zone détermine comment la propriété ppersonnalisée s'affiche dans QRadar Network Anomaly Detection et quelles sont les options disponibles pour l'agrégation. Les options du type de zone sont : • Alpha-Numeric • Numeric • IP • Port L'option par défaut est Alpha-Numeric.
Description	Entrez une description de cette propriété de ppersonnalisé.
Définition de l'expression de propriété	
Type de source de journal	Dans la zone de liste, sélectionnez le type de source de journal auquel s'applique cette propriété d'événement personnalisé. Ce paramètre ne s'affiche que sur la Fenêtre de définition de propriété de l'événement.

Tableau 8-1 Custom property definition window parameters (regex) (suite)

Paramètre	Description
Source de journal	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 définit le terme Multiples et le nombre de sources du journal. Ce paramètre ne s'affiche que sur la Fenêtre de définition de propriété de l'événement.
Nom de l'événement	Pour spécifier un nom d'événement auquel s'applique cette propriété personnalisé, sélectionnez cette option. Cliquez sur **Browse** pour accéder au navigateur Event Browser et sélectionnez l' identificateurQRadar Network Anomaly Detection (QID) pour le nom de l'événement que vous souhaitez appliquer à cette propriété ppersonnalisé. Cette option est activée par défaut
Category	Pour spécifier une catégorie de bas niveau à laquelle s'applique cette propriété ppersonnalisé, sélectionnez cette option. Pour sélectionner une catégorie de bas niveau : **1** Dans la zone de liste **High Level Category**, sélectionnez la catégorie de haut-niveau. La liste **Low Level Category** se met à jour pour inclure uniquement les catégories associées à la catégorie haut niveau sélectionnée. **2** Dans la zone de liste **Low Level Category**, sélectionnez la catégorie de bas niveau à laquelle s'applique cette propriété p personnalisé.

Tableau 8-1 Custom property definition window parameters (regex) (suite)

Paramètre	Description
expression régulière	Entrez l'expression régulière que vous souhaitez utiliser pour extraire les données du contenu. Les expressions régulières sont sensibles à la casse. Exemple d'expressions régulières : • courrier électronique : **`(.+@[^\.].*\.[a-z]{2,}$)`** • URL: **`(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)`** • Nom de domaine **`(http[s]?://(.+?)["/?:])`** • Nombre en virgule flottante : **`([-+]?\d*\.?\d*$)`** • Entier: **`([-+]?\d*$)`** • Addresse IP: **`(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)`** Par exemple : pour faire correspondre un journal qui ressemble à: **`SEVERITY=43`** Construire l'Expression régulière comme suit : **`SEVERITY=([-+]?\d*$)`** ***Remarque :****Les groupes de capture doivent être mis entre parenthèses.*
Groupe de capture	Entrez les groupes de capture que vous souhaitez utiliser si l'expression régulière contient plus d'un seul groupe de capture. Les groupes de capture traitent les divers caractères comme étant une seule unité. Dans un groupe de capture, les caractères sont regroupés entre parenthèses.
Test	Cliquez sur **Test** pour tester l'expression régulière par rapport au contenu.
Activée	Sélectionnez cette case à cocher pour activer cette propriété ppersonnalisé. Lorsque vous désélectionnez cette case à cocher, la propriété de ppersonnalisé ne s'affiche pas dans les filtres de recherche sou listes de colonnes et la propriété p n'est pas analysée à partir des contenus. Ce paramètre est activé par défaut.

Procédure

Etape 1 Choisissez l'une des opérations suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Facultatif. Si vous visualisez des événements ou des flux en mode diffusion en flux, cliquez sur l'icône **Pause** pour faire une pause.

Etape 3 Faites un double-clic sur l'événement ou le flux sur lequel vous souhaitez baser la propriété ppersonnalisé.

Etape 4 Cliquez sur **Extract Property**.

Etape 5 Dans la fenêtre Property Type Selection, sélectionnez l'option**Regex Based**.

Etape 6 Configurez les paramètres pde propriété personnalisée. Voir **Tableau 8-1**.

Etape 7 Cliquez sur **Test** pour tester l'expression régulière par rapport au contenu.

Etape 8 Cliquez sur **Save**.

Résultats

La propriété d'événement personnalisé s'affiche en tant qu'option sur la liste des colonnes disponibles sur la page de recherche. Pour inclure une propriété personnalisé dans la liste ou de flux, sélectionnez la propriété ppersonnalisé à partir de la liste des colonnes disponibles lors de la création de la recherche.

Création d'une propriété personnalisée basée sur le calcul

Vous pouvez créer une propriété client sur la base du calcul pour faire correspondre les contenus d'événement ou de flux à l'expression régulière.

A propos de cette tâche

Lorsque vous configurez une propriété personnalisée basée sur l'expression régulière, les fenêtres de propriété d'événement personnalisé ou de propriété de flux personnalisé fournissent les paramètres suivants:

Tableau 8-2 Custom property definition window parameters (calculation)

Paramètre	Description
Définition de la propriété	
nom de la propriété	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 pour cette propriété de l'événement personnalisé.
Définition du calcul de propriété	
Propriété 1	Dans la zone de liste, sélectionnez la première propriété que vous souhaitez utiliser dans votre calcul. Les options incluent toutes les propriétés de flux numériques personnalisés et normalisés. Vous pouvez également indiquer une valeur numérique spécifique. Dans la zone de liste **Property 1**, sélectionnez l'option **User Defined**. Le paramètre **Numeric Property** s'affiche. Entrez une valeur numérique spécifique.

Tableau 8-2 Custom property definition window parameters (calculation) (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 sont les suivantes : • 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 de flux numériques personnalisés et normalisés. Vous pouvez également indiquer une valeur numérique spécifique. Dans la zone de liste **Property 1**, sélectionnez l'option **User Defined**. Le paramètre **Numeric Property** s'affiche. Entrez une valeur numérique spécifique.
Activée	Sélectionnez cette case à cocher pour activer cette propriété p 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 listes de rubriques et la propriété du flux n'est pas analysée à partir des contenus. Ce paramètre est activé par défaut.

Procédure

Etape 1 Choisissez l'une des opérations suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Facultatif. Si vous visualisez des événements ou des flux en mode diffusion en flux, cliquez sur l'icône **Pause** pour faire une pause.

Etape 3 Faites un double-clic sur l'événement ou le flux sur lequel vous souhaitez baser la propriété ppersonnalisé.

Etape 4 Cliquez sur **Extract Property**.

Etape 5 Dans la fenêtre Property Type Selection, sélectionnez l'option**Calculation Based**.

Etape 6 Configurez les paramètres pde propriété personnalisé. Voir **Tableau 8-2**.

Etape 7 Cliquez sur **Save**.

Résultats

La propriété personnalisée s'affiche en tant qu'option sur la liste des colonnes disponibles sur la page de recherche.Pour inclure une propriété personnalisée dans les d'événement ou sur la liste de flux, sélectionnez la propriété personnalisée à partir de la liste de colonnes disponibles lors de la création d'une recherche.

Modification d'une propriété personnalisée

Via la fenêtre Custom Event Properties ou Custom Flow Properties, vous pouvez modifier une propriété personnalisé.

A propos de cette tâche

Les fenêtres Custom Event Properties et Custom Flow Properties fournissent les informations suivantes:

Tableau 8-3 Fenêtres Custom properties colonnes

Colonne	Description
nom de la propriété	Spécifiez un nom unique pour cette propriété ppersonnalisée.
Type	Spécifiez le type de cette propriété ppersonnalisé. Les options sont les suivantes : • **Regex** - Une propriété ppersonnalisée sur la base de l'expression régulière fait correspondre les contenusd'événements ou de fluxà l'expression régulière. Voir **Création d'une propriété personnalisée basée sur l'expression régulière** • **Calculated** - Une propriété ppersonnalisé basé sur le calcul permet d'effectuer un calcul sur les propriétés ou flux Voir **Création d'une propriété personnalisée basée sur le calcul**.
Description de propriété	Spécifiez une description pour cette propriété ppersonnalisé.
Type de source de journal	Spécifie le nom du type de source de journal auquel s'applique la propriété ppersonnalisé. Cette colonne ne s'affiche que sur la Fenêtre de définition de propriété de l'événement personnalisé.
Source de journal	Indique la source du journal à laquelle s'applique la propriété ppersonnalisée. S'il existe plusieurs sources de journal associées à cet événement ou flux, cette zone définit le terme Multiple et le nombre de sources du journal. Cette colonne ne s'affiche que sur la Fenêtre de définition de propriété de l'événement personnalisé.
Expression	Spécifie l'expression de la propriété ppersonnalisé. L'expression dépend du type de propriété d'événement personnalisé : • 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 ppersonnalisé basé sur le calcul, ce paramètre définit le calcul que vous souhaitez utiliser pour créer une valeur de propriété ppersonnalisé.
Nom d'utilisateur	Indique le nom de l'utilisateur qui a créé cette propriété ppersonnalisé.
Activée	Indique si cette propriété ppersonnalisé est activée. Cette zone indique True ou False.

Tableau 8-3 Fenêtres Custom properties colonnes (suite)

Colonne	Description
Date de création	Indique la date de création de cette propriété ppersonnalisé.
Date de modification	Indique la dernière fois que la propriété ppersonnalisé a été modifiée.

Les barres d'outils Custom Event Property et Custom Flow Property fournissent les fonctions suivantes:

Tableau 8-4 Optionsde la barre d'outils Customproperty

Option	Description
Add	Cliquez sur **Add** pour ajouter une nouvelle propriété ppersonnalisé. Voir **Création d'une propriété personnalisée basée sur l'expression régulière** ou **Création d'une propriété personnalisée basée sur le calcul**.
Edit	Cliquez sur **Edit** pour modifier la propriété ppersonnalisé sélectionnée. Voir **Modificationd'une propriété personnalisée**.
Copy	Cliquez sur **Copy** pour copier les propriétés ppersonnalisé sélectionnées.
Delete	Cliquez sur **Delete** pour supprimer les propriétés ppersonnalisé sélectionnées.
Enable/Disable	Cliquer sur **Enable/Disable** pour activer ou désactiver les propriétés p personnalisé sélectionnées en vue d'une analyse ou d'un affichage dans les filtres de recherche ou sur les listes de colonnes s.

Procédure

Etape 1 Choisissez l'une des opérations suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

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

Etape 3 Cliquez sur **Gestion des propriétés personnalisées**.

Etape 4 ²Sélectionnez la propriété personnalisée p que vous souhaitez modifier et cliquez sur**Edit**.

Etape 5 Modifiez les paramètres requis. Voir **Tableau 8-1**.

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

Etape 7 Cliquez sur **Save**.

Copier une propriété personnalisée

Pour créer une nouvelle propriété personnalisée basée sur une propriété personnalisée existante, vous pouvez copier la propriété personnalisée pexistante puis en modifier les paramètres.

Procédure

Etape 1 Choisissez l'une des opérations suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

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

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

Etape 4 Sélectionnez la propriété p personnalisé 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 Modifiez les paramètres requis. Voir **Tableau 8-1**.

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

Etape 8 Cliquez sur **Save**.

Supprimer une propriété personnalisée

Vous pouvez supprimer toute propriété personnalisée, à condition que la propriété personnalisée ne soit pas associée à une autre.

A propos de cette tâche

Si vous tentez de supprimer une propriété personnalisée associée à une autre propriété personnalisée, un message d'erreur s'affiche pour fournir le le nom de la propriété personnalisée associée.

Procédure

Etape 1 Choisissez l'une des opérations suivantes :

- Cliquez sur l'onglet **Log Activity**.
- Cliquez sur l'onglet **Network Activity**.

Etape 2 Dans lazone de liste **Search**, sélectionnez **Edit Search**.

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

Etape 4 Sélectionnez la propriétépersonnalisé que vous souhaitez supprimer et cliquez sur **Delete**.

Etape 5 Cliquez sur **Oui**.

9 GESTION DE RÈGLE

Sur les onglets **Log Activity**, **Network Activity**, et **Offenses**, vous pouvez afficher et garder les règles. Cette rubrique s'applique aux utilisateurs qui ont des permissions de rôle **View Custom Rules** ou **Maintain Custom Rules.**

Considérations de la permission de règle

Vous pouvez afficher et gérer les règles pour les zones du réseau auxquelles vous pouvez accéder si vous avez les permissions de rôle d'utilisateur :

- View Custom Rules
- Maintain Custom Rules

Pour créer des règles de détection d'anomalies, vous devez disposer de la permission **Maintain Custom Rule** pour l'onglet sur lequel vous voulez créer la règle. Par exemple, pour créer une règle de détection d'anomalie sur l'onglet Log Activity, vous devez disposer de **Log Activity > Maintain Custom Rule**.

Pour plus d'informations sur les permissions du rôle d'utilisateur, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration.*

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, voir le *IBM Security QRadar Network Anomaly DetectionGuide d'administration*.

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.

Catégories de règle

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.

Types de règles

Les règles personnalisées comprennent les types de règles suivants :

- **Event Rule** - Une règle d'événements 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 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 testes 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 règle inclut les types de règle suivants :

- **Anomaly** - Une règle d'anomalie teste le trafic des événements et des flux d'une activité anormale, tel 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 inférieur, égal ou supérieur 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 221ème 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 règles

Chaque règle peut contenir les composants 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/toutes les règles suivantes.** Pour une liste complète des fonctions, voir **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 ces serveurs de messagerie d'une autre règle. Les blocs de construction par défaut sont fournis à titre indicatif, ce qui devrait être revu et modifié en fonction des besoins de votre réseau. Pour obtenir une liste exhaustive des règles par défaut, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
- **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, voir **Tests de règle**.

Réponses de règle

Lorsque les conditions de règle sont respectées, une règle peut générer une ou plusieurs des réponses suivantes :

- Créer un violation.
- Envoyer un e-mail.
- Générer des notifications système en utilisant la fonction Dashboard.
- Ajouter des données aux ensembles de références. Pour plus d'informations sur les ensembles de références, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

- Ajouter des données aux collections de données de référence qui peuvent être utilisées dans les tests de règle.Avant de pouvoir configurer une règle pour envoyer des données à une collection de données de référence, vous devez créer la collection de données de référence en utilisant la commande de la ligne d'interface (CLI). Pour plus d'informations sur la manière de créer et d'utiliser les collections de données de référence, voir *IBM Security QRadar Reference Data Collections* technical note.

  A l'aide de cette option, vous pouvez ajouter des données aux types de collection de données :

  - **Reference Map** - Dans une Reference Map, les données sont stockées dans des enregistrements qui font correspondre une clé à une valeur.Par exemple, l'activité utilisateur sur votre réseau, vous pouvez créer une carte de référence qui utilise le paramètre **Username** en tant que clé et l'ID global d'utilisateur en tant que valeur.
  - **Reference Map of Sets** - Dans un Reference Map of Sets, les données sont stockées dans des enregistrements qui font correspondre une clés à des valeurs multiples. Par exemple, pour tester l'accès autorisé à un brevet, vous pouvez créer un Map of Sets qui utilise une propriété d'événement personnalisé pour Patent ID en tant que clé et le paramètre **Username** en tant que la valeur pour remplir une liste d'utilisateurs autorisés.
  - **Reference Map of Maps** - Dans un Reference Map of Maps, les données sont stockées dans des enregistrements qui font correspondre cette carte à une autre clé, laquelle est ensuite reliée à une valeur unique. Par exemple, pour tester des violations de bande passante, vous pouvez créer un Map of Maps qui utilise le paramètre **Source IP** en tant que première clé, le paramètre **Application** en tant que seconde clé et le paramètre **Total Bytes** en tant que la valeur.
- Générer une réponse vers un système externe, y compris les types de serveur 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** - Une règle peut transférer des données de journal brutes provenant de sources de journal et de données d'événement normalisées vers un ou plusieurs systèmes de fournisseur, tels que les systèmes de billetterie ou d'alerte.
  - **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. A l'aide de l'assistant Rule, vous pouvez configurer les règles pour générer une réponse qui envoie des interruptions SNMP à l'hôte configuré.
  - **Interface For Metadata Access Points (IF-MAP)** - Le réponse de la règle Interface For Metadata Access Points (IF-MAP) permet à la règle de publier

des données d'alerte et de violation dérivées des événements, des flux et des données de violation sur un serveur IF-MAP.

Affichage de règles

Vous pouvez afficher les détails d'une règle, y compris les tests, les blocs de constructions et les réponses.

Avant de commencer

En fonction des permissions de rôle, vous pouvez accéder à la page de règle à partir de l'onglet **Offenses**, **Log Activity** ou **Network Activity**. Pour plus d'informations sur les autorisations de rôle, voir le *IBM Security QRadar Network Anomaly DetectionGuide d'administration*.

A propos de cette tâche

La page Rules affiche une liste de règle avec les paramètres associés. Pour plus d'informations sur les paramètres affichés pour chaque règle listée sur la page Rules, voir **Tableau 9-1**.

Pour localiser la règle que vous souhaiter ouvrir et voir les détails, vous pouvez utiliser la zone de liste **Group** ou le champ **Search Rules** sur la barre d'outils. Pour plus d'informations sur la barre de détails de la page Rules, voir **Tableau 9-2**.

Procédure

Etape 1 Sélectionnez l'une des options suivantes :

- Cliquez sur l'onglet **Offenses,** puis cliquez sur **Rules** sur le menu de navigation.
- Cliquez sur l'onglet **Log Activity**, puis sélectionnez **Rules** à partir de la zone de liste **Rules** sur la barre d'outils.
- Cliquez sur **Network Activity**, puis sélectionnez **Rules** à partir de la zone de liste **Rules** sur la barre d'outils.

Etape 2 Dans la zone de liste **Display**, sélectionnez **Rules**.

Etape 3 Cliquez deux fois sur la règle que vous souhaitez afficher.

Etape 4 Revoir les détails de la règle.

Résultats

Si vous avez la permission **View Custom Rules**, mais que vous n'avez pas la permission **Maintain Custom Rules**, la page Rule Summary s'affiche et la règle ne peut pas être éditée.

Si vous avez la permission **Maintain Custom Rules**, la page Rule Test Stack Editor s'affiche. Vous pouvez passer en revue et éditer les détails de règle. Voir **Edition d'une règle**.

Création d'une règle personnalisée

QRadar Network Anomaly Detection fournit les règles par défaut, cependant, vous pouvez créer de nouvelles règles pour répondre aux besoins de votre déploiement.

A propos de cette tâche

Pour créer une nouvelle règle, vous devez avoir la permission **Offenses > Maintain Custom Rules**.

Procédure

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

Etape 2 Dans le menu de la navigation, cliquez sur **Rules**.

Etape 3 A partir de la zone de liste **Actions**, sélectionnez l'une des options suivantes :

- New Event Rule
- New Flow Rule
- New Common Rule
- New Offense Rule

Etape 4 Lisez le texte d'introduction sur Rule Wizard. Cliquez sur **Next**.

Vous êtes invité à choisir la source à partir de laquelle vous voulez que cette règle s'applique. La source par défaut est le type de règle que vous avez sélectionné

dans **Etape 3**. Vous avez uniquement besoin de choisir une source sur cette page si vous souhaitez changer votre sélection.

Etape 5 Cliquez sur **Next** pour afficher la page Rule Test Stack Editor.

Etape 6 Dans le champ **enter rule name here** dans le volet Rule, tapez un nom unique que vous souhaitez assigner à cette règle.

Etape 7 Dans la zone de liste, sélectionnez si vous voulez tester la règle localement ou globalement :

- **Local** - Cette règle est testée 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 de l'événement central, ce qui peut réduire les performances sur le processeur de l'événement central.

Etape 8 Ajouter un ou plusieurs tests à une règle :

a Facultatif. Pour filtrer les options dans la zone de liste **Test Group**, entrez un texte que vous voulez filtrer dans la zone **Type to filter**.

b Dans la zone de liste **Test Group**, sélectionnez le type de test que vous souhaitez ajouter à cette règle.

c Pour chaque test que vous souhaitez ajouter à la règle, sélectionnez le signe **+** à côté du test.

d Facultatif. Pour identifier un test comme exclu, cliquez sur **et** au début du test dans le panneau Rule. **and** est affiché en tant que **and not**.

e Cliquez sur les paramètres configurables soulignés pour personnaliser les variables de test.

f A partir de la boîte de dialogue, sélectionnez les valeurs de la variable puis cliquez sur **Submit**.

Etape 9 Pour exporter la règle configurée en tant que bloc de configuration pour l'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.

Etape 11 Dans le champ **Notes**, entrez une note que vous souhaitez inclure pour cette règle. Cliquez sur **Next**.

Etape 12 Sur la page Rule Responses, configurez les réponses que vous souhaitez que cette règle génère. Sélectionnez l'une des options suivantes :

- Si vous configurez les réponses pour un Event Rule, Flow Rule, ou Common Rule, voir le **Tableau 9-3**.
- Si vous configurez les réponses pour une Offense Rule, voir le **Tableau 9-4**.

Etape 13 Cliquez sur **Next**.

Etape 14 Vérifiez la page Rule Summary pour garantir que les paramètres sont corrects. Effectuez n'importe quel changement, puis cliquez sur **Finish**.

Création d'une règle de détection d'anomalie

L'assistant Anomaly Detection Rule wizard vous permet de créer des règles qui appliquent des critères d'intervalle de temps en utilisant des tests de données et d'heure.

Avant de commencer

Pour créer une nouvelle règle de détection d'anomalies, vous devez remplir les critères suivants :

- Avoir la permission Maintain Custom Rules.
- Effectuez une recherche groupée.

Les options de détection d'anomalies sont uniquement affichées après que ayez effectué une recherche groupe et enregistré les critères de recherche.

A propos de cette tâche

Vous devez avoir la permission de rôle appropriée afin d'être capable de créer une règle de détection des anomalies :

- Pour créer des règles de détection d'anomalies sur l'onglet **Log Activity**, vous devez avoir la permission de rôle **Log Activity > Maintain Custom Rules**
- Pour créer des règles de détection d'anomalies sur l'onglet **Log Activity**, vous devez avoir la permission de rôle **Network > Maintain Custom Rules**

Les règles de détection d'anomalie utilisent tous les critères de filtrage et de regroupement des critères de recherche qui sont sauvegardés, mais n'utilisent pas n'importe quelle plage d'horaire des critères.de la recherche.

Lorsque vous créez une règle de détection d'anomalies, la règle est remplie avec une pile de test 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.

Par défaut, l'option **Test the [Selected Accumulated Property] value of each [group] separately** est sélectionnée sur la page Rule Test Stack Editor. Cela entraîne une règle de détection d'anomalies à tester la propriété accumulée sélectionnée pour chaque événement ou groupe de flux séparément. Par exemple, si la valeur accumulée sélectionnée est **UniqueCount(sourceIP)**, la règle teste chaque adresse IP source unique pour chaque groupe d'événements/flux.

Cette option **Test the [Selected Accumulated Property] value of each [group] separately** est dynamique. La valeur **[Selected Accumulated Property]** dépend de l'option que vous sélectionnez pour le champ de test **this accumulated property** de la pile de test par défaut. 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.

Procédure

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

Etape 2 Effectuez une recherche.

Etape 3 A partir du menu **Rules**, sélectionnez le type de règle que vous souhaitez créer. Les options incluent :

- Add Anomaly Rule
- Add Threshold Rule
- Add Behavioral Rule

L'assistant Rule s'affiche.

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 source par défaut est le type de règle que vous avez sélectionné dans **Etape 3**. Vous avez uniquement besoin de choisir une source sur cette page si vous souhaitez changer votre sélection.

Etape 5 Cliquez sur **Next** pour afficher la page Rule Test Stack Editor.

Etape 6 Dans la zone **enter rule name here**, entrez un nom unique que vous voulez affecter à cette règle.

Etape 7 Pour ajouter un test à une règle :

a Facultatif. Pour filtrer les options dans la zone de liste **Test Group**, entrez le texte que vous voulez filtrer dans la zone **Type to filter**.

b Dans la zone de liste **Test Group**, sélectionnez le type de test que vous voulez appliquer à cette règle.

c Pour chaque test que vous souhaitez ajouter à la règle, sélectionnez le signe **+** à côté du test.

d Facultatif. Pour identifier un test comme exclus, cliquez sur **and** au début du test dans le panneau Rule. **and** s'affiche comme **and not**.

e Cliquez sur les paramètres configurables soulignés pour personnaliser les variables du test.

f partir de la boîte de dialogue, sélectionnez les valeurs de la variable puis cliquez sur **Submit**.

Etape 8 Facultatif. Pour tester le total des propriétés accumulées sélectionnées pour chaque groupe d'événement /flux, décochez la case **Test the [Selected Accumulated Property] value of each [group] separately**.

Etape 9 Dans le volet Groups, sélectionnez les cases à cocher des groupes auxquels vous souhaitez affecter cette règle. Pour plus d'informations sur le groupement de règles, voir **Gestion de groupe de règles**.

Etape 10 Dans la zone **Notes**, entrez les notes que vous voulez inclure à cette règle. Cliquez sur **Next**.

Etape 11 Sur la page Rule Responses, configurez les réponses que vous souhaitez que cette règle génère. Voir **Tableau 9-5**.

Etape 12 Cliquez sur **Next**.

Etape 13 Vérifiez la règle configurée. Cliquez sur **Finish**.

Tâches de gestion des règles

Vous pouvez gérer les règles personnalisées et les règles d'anomalie. Vous pouvez activer ou désactiver les règles, si nécessaire. Vous pouvez également éditer, copier ou supprimer une règle.

Remarque : La fonction de détection d'anomalies sur les onglets **Log Activity** et **Network Activity** vous permettent 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 la page Rules sur l'onglet **Offenses**.

Activation/ désactivation de règles

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.

A propos de cette tâche

Vous devez disposer de la permission de rôle **Offenses > Maintain Custom Rules** pour pouvoir activer ou désactiver une règle.

Procédure

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** sur la page Rules, sélectionnez **Rules**.

Etape 4 =Sélectionner la règle que vous souhaitez activer ou désactiver.

Etape 5 Dans la zone de liste **Actions**, sélectionnez **Enable/Disable**.

Edition d'une règle

Vous pouvez éditer une règle pour changer le nom de la règle, le type de la règle, les tests ou les réponses.

A propos de cette tâche

Vous devez disposer de la permission de rôle **Offenses > Maintain Custom Rules** pour pouvoir éditer une règle.

Procédure

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** sur la page Rules, sélectionnez **Rules**.

Etape 4 Cliquez deux fois sur la que vous souhaitez éditer.

Etape 5 Dans la zone de liste **Actions**, sélectionnez **Open**.

Etape 6 Facultatif. Si vous voulez changer le type de règle, cliquez sur **Back** et sélectionnez un nouveau type de règle.

Etape 7 Sur la page Rule Test Stack Editor, éditez les paramètres.Voir le **Tableau 9-1**.

Etape 8 Cliquez sur **Next**.

Etape 9 Sur la page Rule Response, éditez les paramètres :

- Voir le **Tableau 9-3** pour les réponses d'événement, de flux ou de règle commune.
- Voir le **Tableau 9-4** pour les réponses de règle de violation.
- Voir le **Tableau 9-5** pour les réponses de règle 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.

A propos de cette tâche

Vous devez disposer de la permission de rôle **Offenses > Maintain Custom Rules** pour pouvoir copier une règle.

Procédure

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**.

Suppression d'une règle

QRadar Network Anomaly Detection vous permet de supprimer une règle de votre système.

A propos de cette tâche

Vous devez disposer de la permission de rôle **Offenses > Maintain Custom Rules** afin de pouvoir supprimer une règle.

Procédure

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**.

Gestion de groupe de règles

Si vous êtes un administrateur, vous êtes en mesure de créer, modifier et supprimer des groupes de règles. La catégorisation de vos règles ou blocs de construction en groupes vous permettent de visualiser efficacement et suivre vos règles. Par exemple, vous pouvez afficher toutes les règles relatives à la conformité.

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 d'anomalie**.

Affichage d'un groupe de règles

Sur la page 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.

Procédure

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.

Result

La liste des éléments affectés à ce groupe s'affiche.

Création d'un groupe

La page Rules fournit des groupes de règles par défaut, cependant, vous pouvez créer un nouveau groupe.

Procédure

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.

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 Facultatif. 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.

Affectation d'un élément à un groupe

Vous pouvez affecter une règle et un bloc de construction sélectionnés à un groupe.

Procédure

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.

Edition d'un groupe

Vous pouvez éditer un groupe pour changer le nom ou la description.

Procédure

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 Facultatif. 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 d'un groupe vers d'autres.

Procédure

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 d'un groupe

Vous pouvez supprimer un élément d'un groupe. Lorsque vous supprimez un élément dans un groupe,, la règle ou le bloc de construction est uniquement supprimée du groupe; elle reste sur la page Rules.

Procédure

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

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

Etape 3 Cliquez sur **Groups**.

Etape 4 n 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

Vous pouvez supprimer un groupe. Lorsque vous supprimer un groupe, les règles ou blocs de construction de ce groupe restent disponibles sur la page Rules.

Procédure

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.

Edition de blocs de construction

QRadar Network Anomaly Detection inclut un ensemble de blocs de construction par défaut que vous pouvez éditer pour répondre à vos besoins de déploiement.

A propos de cette tâche

Un bloc de construction est une pile de test de règle réutilisable que vous vous pouvez inclure en tant que composant d'autres règles.

Par exemple, vous pouvez éditer le bloc de construction BB:HostDefinition: Mail Servers afin d'identifier tous les serveurs de messagerie dans votre déploiement. Ensuite, vous pouvez configurer n'importe quelle règle pour exclure vos serveurs de messagerie des tests de règles.

Pour plus d'informations sur les blocs de construction par défaut, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Procédure

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**.

Paramètres de la page Rules

La liste des règles déployées fournit les informations suivantes pour chaque règle :

Tableau 9-1 Paramètres de la page Rules

Paramètre	Description
Rule Name	Affiche le nom de la règle.
Group	Affiche le groupe auquel cette règle est affectée. Pour plus d'informations à propos des groupes, voir **Gestion de groupe de règles**.
Rule Category	Affiche la catégorie de la règle. Les options incluent : • Custom Rule • Anomaly Detection Rule
Rule Type	Affiche le type de règle. Les types des règles incluent : • 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**.

Tableau 9-1 Paramètres de la page Rules (suite)

Paramètre	Description
Response	Affiche la réponse à la règle, le cas échéant. Les réponses à la règle incluent : • Dispatch New Event • Email • Log • Notification • SNMP • Reference Set • Reference Data • IF-MAP Response Pour plus d'informations sur les réponses de règles, voir **Réponses de règle**.
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).
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.

Barre d'outils de la page Rules

La barre d'outils de la page Rules fournit les fonctions suivantes :

Tableau 9-2 Fonction de la barre d'outils de la page Rules to

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 **Gestion de groupe de règles**.

Tableau 9-2 Fonction de la barre d'outils de la page Rules to (suite)

Fonction	Description
Actions	Cliquez sur **Actions** et sélectionnez l'une des options suivantes : • **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'une règle**. • **Edit** - Sélectionnez cette option pour éditer une règle sélectionnée. Voir **Edition 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**.
Revert Rule	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. ***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.*

Tableau 9-2 Fonction de la barre d'outils de la page Rules to (suite)

Fonction	Description
Search Rules	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. Les paramètres suivants sont recherchés pour une correspondance avec votre critère de recherche : • Rule Name • Rule (description) • Notes • Response 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).

Paramètres de la page Rule Response

Tableau 9-3 fournit les paramètres de la page Rule Response si le type de règle est Event Rule, Flow Rule, ou Common.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response

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 le **Glossaire**.
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 le **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 le **Glossaire**.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Ensure the detected event is part of an offense	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. Lorsque vous cochez cette case, les options suivantes s'affichent : • **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. 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. 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. Pour les règles communes, les options incluent destination IP, destination IP identity, destination port, rule, source IP, source IP identity et source port. • **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	Sélectionnez cette case pour forcer l'envoi d'un événement qui est normalement envoyé au composant Magistrate, à la base de données Ariel pour la génération de rapports ou la recherche. Cet événement ne s'affiche pas sur l'onglet **offenses**.
Rule Response	
Dispatch New Event	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. Les paramètres **Dispatch New Event** s'affichent lorsque vous cochez cette case. Par défaut, la case est vide.
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.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
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 le **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 le **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 le **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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
Annotate this offense	Cochez cette case pour ajouter une annotation à cette violation et entrer l'annotation.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Assurer-vous que l'événement envoyé fait partie d'une violation.	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. Lorsque vous cochez cette case, les options suivantes s'affichent : • **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. 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. 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. Pour les règles communes, les options incluent destination IP, destination IP identity, destination port, rule, source IP, source IP identity et source port. • **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 : **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.
Email	Cochez cette case pour afficher les options de courrier électronique. Par défaut, la case est vide.
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.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Alerte SNMP	Ce paramètre ne s'affiche que lorsque les paramètres SNMP sont configurés dans les paramètres du système. Pour plus d'informations sur les catégories d'événements, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration.* ▶ 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 les données de notification, tels que définis par le IBM MIB. Pour plus d'informations sur IBM MIB, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*. Par exemple, la notification SNMP peut ressembler à : **"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"**
Send to Local SysLog	Cochez cette case si vous voulez consigner l'événement ou le transporter localement. Par défaut, la case est vide. Par exemple, la sortie syslog peut ressembler à : **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**
Send to Forwarding Destinations	Cette case ne s'affiche que pour les Règles d'événements. 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. 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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Notify	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. Pour plus d'informations sur l'onglet Dashboard, voir **Gestion du tableau de bord**. ***Remarque :*** *Si vous activez les notifications, configurez le paramètre* ***Response Limiter****.*
Add to Reference Set	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. Pour ajouter des données à l'ensemble de références : **1** A l'aide de la première zone de liste, sélectionnez les données que vous voulez ajouter. Les options incluent toutes les données normalisées ou personnalisées. **2** A l'aide de la seconde zone de liste, sélectionnez l'ensemble de références auquel vous souhaitez ajouter les données spécifiées. La réponse à la règle **Add to Reference Set** offre les fonctions suivantes : • **Refresh** - Cliquez sur **Refresh** pour actualiser la première zone de liste pour garantir que la liste est actuelle. • **Configure Reference Sets** - Cliquez sur **Configure Reference Sets** pour configurer l'ensemble de références. Cette option n'est disponible que si vous avez les permissions administratives. Pour plus d'informations sur la gestion des ensembles de référence, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Add to Reference Data	Avant de pouvoir utiliser cette réponse à la règle, vous devez créer la collection de données de références en utilisant la commande d'interface de ligne de commande (CLI). Pour plus d'informations sur la manière de créer et d'utiliser les collections de données de référence, voir *IBM Security QRadar Reference Data Collections Technical Note*. Cochez cette case si vous souhaitez que les événements générés en résultat de cette règle soient rajoutés à la collection de données de référence. Après avoir sélectionné la case à cocher, sélectionnez l'une des options suivantes : • **Add to a Reference Map** - Sélectionnez cette option pour envoyer les données à une collection de paires de valeurs clé/multiple. Vous devez sélectionner la clé et la valeur de l'enregistrement de données, puis sélectionnez la carte de référence à laquelle vous souhaitez ajouter l'enregistrement de données. • **Add to a Reference Map of Sets** - Sélectionnez cette option pour envoyer les données à une collection de paires de valeurs clé/unique. Vous devez sélectionner la clé et la valeur de l'enregistrement de données, puis sélectionnez la carte de référence des ensembles auxquelles vous souhaitez ajouter l'enregistrement de données. • **Add to a Reference Map of Maps** - Sélectionnez cette option pour envoyer des données à une collection de paires de clés/unique. Vous devez sélectionner une clé pour la première carte, une clé pour la seconde carte, puis la valeur de l'enregistrement de données. Vous devez sélectionner la carte de référence de cartes à laquelle vous souhaitez ajouter l'enregistrement de données.
Publish on the IF-MAP Server	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, voir *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
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.

Tableau 9-4 fournit les paramètres de la page Rule Response si le type de règle est Offense.

Tableau 9-4 Paramètres de la page Offense Rule Response

Paramètre	Description
Rule Action	

Tableau 9-4 Paramètres de la page Offense Rule Response (suite)

Paramètre	Description
Name/Annotate the detected offense	Cochez cette case pour afficher les noms des options.
New Offense Name	Entrer 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 : • **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.
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 système, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*. ▶ Activez cette règle en cochant cette case pour envoyer une notification SNMP (interruption). Pour une règle de violation, la sortie d'alerte SNMP inclut l'heure du système, l'ID objet de l'interruption et les données de notification tels que définis par IBM MIB. Pour plus d'informations sur IBM MIB, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*. Par exemple, la notification SNMP peut ressembler à : **"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"**

Tableau 9-4 Paramètres de la page Offense Rule Response (suite)

Paramètre	Description
Send to Local SysLog	Cochez cette case si vous voulez consigner l'événement ou le transporter localement. Par défaut, la case est vide. Par exemple, la sortie syslog peut ressembler à : **`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`**
Send to Forwarding Destinations	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. 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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
Publish on the IF-MAP Server	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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
Response Limiter	Sélectionnez cette case et utilisez les zones 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.

Le tableau suivant fournit les paramètres de la page Rule Response si le type de règle est Anomaly.

Tableau 9-5 Paramètres de la page Anomaly Detection Rule Response

Paramètre	Description
Rule Response	
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**.

Tableau 9-5 Paramètres de la page Anomaly Detection Rule Response (suite)

Paramètre	Description
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 : • **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 le **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 le **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. Pour plus d'informations sur la pertinence, voir le **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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
Annotate this offense	Cochez cette case pour ajouter une annotation à cette violation et entrer l'annotation.

Tableau 9-5 Paramètres de la page Anomaly Detection Rule Response (suite)

Paramètre	Description
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 : • **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 système, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*. ▶ 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 les données de notification data, tels que définis par IBM MIB. Pour plus d'informations sur IBM MIB, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*. Par exemple, la notification SNMP peut ressembler à : `"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"`
Notify	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. Pour plus d'informations sur l'onglet Dashboard, voir **Gestion du tableau de bord**. ***Remarque :*** *Si vous activez les notifications, configurez le paramètre* ***Response Limiter****.*

Tableau 9-5 Paramètres de la page Anomaly Detection Rule Response (suite)

Paramètre	Description
Send to Local SysLog	Cochez cette case si vous voulez consigner l'événement ou le transporter localement. Par défaut, la case est vide. Par exemple, la sortie syslog peut ressembler à : **`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`**
Add to Reference Set	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. Pour ajouter des données à l'ensemble de références : **1** A l'aide de la première zone de liste, sélectionnez les données que vous voulez ajouter. Les options incluent toutes les données normalisées ou personnalisées. **2** A l'aide de la seconde zone de liste, sélectionnez l'ensemble de références auquel vous souhaitez ajouter les données spécifiées. La réponse à la règle **Add to Reference Set** offre les fonctions suivantes : • **Refresh** - Cliquez sur **Refresh** pour actualiser la première zone de liste pour garantir que la liste est actuelle. • **Configure Reference Sets** - Cliquez sur **Configure Reference Sets** pour configurer l'ensemble de références. Cette option n'est disponible que si vous avez les permissions administratives. Pour plus d'informations sur la gestion des ensembles de références, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.

Tableau 9-5 Paramètres de la page Anomaly Detection Rule Response (suite)

Paramètre	Description
Add to Reference Data	Avant de pouvoir utiliser cette réponse à la règle, vous devez créer la collection de données de références en utilisant la commande d'interface de ligne de commande (CLI). Pour plus d'informations sur la manière de créer et d'utiliser les collections de données de référence, voir *IBM Security QRadar Reference Data Collections Technical Note*. Cochez cette case si vous souhaitez que les événements générés à la suite de cette règle soient rajoutés à la collection de données de référence. Après avoir sélectionné la case à cocher, sélectionnez l'une des options suivantes : • **Add to a Reference Map** - Sélectionnez cette option pour envoyer les données à une collection de paires de valeurs clé/multiple. Vous devez sélectionner la clé et la valeur de l'enregistrement de données, puis sélectionnez la carte de référence à laquelle vous souhaitez ajouter l'enregistrement de données. • **Add to a Reference Map of Sets** - Sélectionnez cette option pour envoyer les données à une collection de paires de valeurs clé/unique. Vous devez sélectionner la clé et la valeur de l'enregistrement de données, puis sélectionnez la carte de référence des ensembles auxquelles vous souhaitez ajouter l'enregistrement de données. • **Add to a Reference Map of Maps** - Sélectionnez cette option pour envoyer des données à une collection de paires de valeurs clé/unique. Vous devez sélectionner une clé pour la première carte, une clé pour la seconde carte, puis la valeur de l'enregistrement de données. Vous devez également sélectionner la carte de référence de cartes à laquelle vous souhaitez ajouter l'enregistrement de données.
Publish on the IF-MAP Server	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, voir le *IBM Security QRadar Network Anomaly Detection Guide d'administration*.
Response Limiter	Cochez cette case et utilisez les cases à cocher pour configurer la fréquence à laquelle vous voulez que cette règle réponde.
Enable Rule	Cochez cette case pour activer cette règle. Par défaut, la case est cochée.

10 GESTION DES ACTIFS

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. A l'aide de longlet **Assets**, vous pouvez créer des actifs sur votre réseau.

Présentation de l'onglet Assets

Les profils d'actifs fournissent des informations sur chaque actif connu sur le réseau, notamment quels services sont en cours d'exécution 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 vulnérabilités positives.
- Imprimer ou exporter des profils d'actif.

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 l'évaluation de la vulnérabilité, voir *IBM Security QRadarVulnerability Assessment Guide*. Pour plus d'informations sur les sources du flux, voir le Manuel d'administrateur *IBM Security QRadar Network Anomaly Detection*

Détails sur les vulnérabilités

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

(NVDB). 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 d'évaluation des vulnérabilités *IBM Security QRadar Network Anomaly Detection.*

Recherche d'actifs

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.

À l'aide de la fonction de recherche d'actifs, 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 la base de données OSVDB, voir *http://osvdb.org/*. Pour plus d'informations sur la base de données NVDB, voir *http://nvd.nist.gov/*.

Etudier les profils d'actif

Lorsque vous accédez à l'onglet **Assets**, la fenêtre Asset Profile Search s'affiche. Vous devez configurer les paramètres de recherche pour afficher les profils d'actifs que vous souhaitez étudier.

A propos de cette tâche

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**.

Procédure

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

Etape 2 Sur la page Asset Profile Search, définissez les critères pour les actifs qui vous souhaitez lister. Choisissez une des options suivantes :

- Pour répertorier tous les profils d'actif dans votre déploiement, cliquez sur **Show All**.

- Pour lister un ensemble défini d'actifs, définissez vos critères de recherche. Voir **Tableau 10-2**.

Etape 3 Facultatif. Pour afficher de plus amples informations sur un actif, déplacez votre souris sur l'adresse IP de l'actif que vous souhaitez étudier.

Etape 4 Pour afficher la page Asset Profile de l'actif, faites un double-clic sur l'actif. Voir **Tableau 10-4**.

Etape 5 Facultatif. Pour étudier de façon plus approfondie les données associées données, cliquez sur une fonction de la barre d'outils dans le panneau Profil d'actif. Pour avoir les descriptions des fonctions de la barre d'outils, voir **Tableau 10-8**.

Etape 6 Facultatif. Pour modifier un paramètre directement à partir de la page Asset Profile, apportez les modifications nécessaires, puis cliquez sur **Save Changes**.

Etape 7 Pour afficher la fenêtre Research Vulnerability Details de l'actif, choisissez l'une des options suivantes:

- Dans le panneau Ports and Vulnerabilities, faites un double-clic 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.

  Voir **Paramètres de la fenêtre Review Vulnerability Details**.

Tâches de gestion des profils d'actif

A l'aide de l'onglet **Assets**, vous pouvez ajouter, modifier, supprimer, importer et exporter des profils d'actif.

Ajouter un profil d'accès

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. Cependant, il se peut que vous soyez tenu d'ajouter manuellement un profil.

A propos de cette tâche

Lors de l'ajout d' un profil actif, vous devez configurer les paramètres suivants:

Tableau 10-1 Add Asset Profile page parameters

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.

Tableau 10-1 Add Asset Profile page parameters (suite)

Paramètre	Description
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.

Procédure

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 les valeurs des paramètres. Voir **Tableau 10-1**.

Etape 5 Cliquez sur **Save**.

Etape suivante

Après avoir ajouté un profil d'actif, vous pouvez modifier le profil pour configurer les paramètres de profils d'actif supplémentaires, tels que les informations sur le système d'exploitation et sur le propriétaire fonctionnel. Voir **Modifier un actif**.

Modifier un actif

Vous pouvez modifier un profil d'actif automatiquement découvert ou manuellement ajouté.

Procédure

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

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

Etape 3 Sur la page Asset Profile Search, définissez les critères pour les actifs qui vous souhaitez lister. Choisissez une des options suivantes :

- Pour lister tous les profils d'actif dans votre déploiement, cliquez sur **Show All**.
- Pour lister un ensemble défini d'actifs, définissez vos critères de recherche. Voir le **Tableau 10-2**.

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. Voir le **Tableau 10-6**.

Etape 7 Cliquez sur **Save Changes**.

Supprimer des actifs

Vous pouvez supprimer des actifs spécifiques ou l'ensemble des profils d'actifs listés.

Procédure

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

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

Etape 3 Sur la page Asset Profile Search, définissez les critères des actifs que vous souhaiter lister. Choisissez une des options suivantes :

- Pour lister tous les profils d'actifs dans votre déploiement cliquez sur **Show All**.
- Pour lister un ensemble défini d'actifs, définissez vos critères de recherche. Voir **Tableau 10-2**.

Etape 4 Sélectionnez l'une des options suivantes :

- Sélectionnez l'actif que vous souhaitez supprimer, puis sélectionnez**Delete Asset** à partir de la zone de liste **Actions**.
- Dans la zone de liste **Actions**, sélectionnez **Delete Listed**.

Etape 5 Cliquez sur **OK**.

Importer des profils d'actifs

Vous pouvez importer des informations de profil d'actif dans QRadar Network Anomaly Detection.

Avant de commencer

Le fichier importé doit être un fichier CSV respectant le format suivant :

```
ip,nom,pondération,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 stockés dans le système..

Procédure

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

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

Etape 3 Dans la zone de liste **Actions**, sélectionnez **Import Assets**.

Etape 4 Cliquez sur **Browse** pour rechercher et sélectionner le fichier CSV à importer.

Etape 5 Cliquez sur **Import Assets** pour commencer le processus d'importation.

Result

Si une erreur se produit pendant le processus d'importation, aucun actif n'est importé.

Exporter des actifs

Vous pouvez exporter des profils d'actifs listés vers un fichier XML ou CSV.

Procédure

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

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

Etape 3 Sur la page Asset Profile Search, définissez les critères des actifs que vous souhaiter lister. Choisissez une des options suivantes :

- Pour lister tous les profils d'actifs dans votre déploiement cliquez sur **Show All**.
- Pour lister un ensemble défini d'actifs, définissez vos critères de recherche. Voir **Tableau 10-2**.

Etape 4 Dans la zone de liste **Actions**, sélec tionnez l'une des options suivantes:

- Exporter vers un fichier XML
- Exporter vers un fichier CSV

Une fenêtre d'état indique la progression du processus d'exportation.

Etape 5 Facultatif. Si vous souhaitez utiliser d'autres onglet et pages pages dans QRadar Network Anomaly Detection alors que le processus d'exportation est en cours, cliquez sur le lien **Notify When Done**.

Une fois l'exportation terminée, la fenêtre File Download s'affiche.

Etape 6 Sur la fenêtre File Download, choisissez l'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 7 Cliquez sur **OK**.

Paramètres de l'onglet Assets et barres d'outils

Cette rubrique contient des tableaux qui décrivent les paramètres et barres d'outils qui s'affichent sur chaque page de l'onglet **Assets**.

Paramètres de la page Asset Profile Search et fonctions de la barre d'outils

Le tableau suivant décrit les paramètres de la page Asset Profile Search:

Tableau 10-2 Paramètres Asset Profile Search

Paramètre	Description
Propriétés d'actifs	
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 un 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 10-2 Paramètres Asset Profile Search (suite)

Paramètre	Description
Afficher uniquement les hôtes avec des vulnérabilités	Sélectionnez cette case à cocher si vous souhaitez afficher uniquement les actifs avec des vulnérabilités dans les résultats de la recherche.
système d'exploitation	Entrez le système d'exploitation des actifs que vous souhaitez rechercher. Par exemple, Red Hat Linux®.
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.
Extended Asset Properties	
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 les informations de contact du propriétaire technique des actifs que vous souhaitez rechercher. Un responsable ou directeur informatique est un exemple 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.
Vulnerability Attributes	
OSVDB ID	Entrez l'identificateur 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.
DISA IAVA	Entrez le numéro IAVA (Information Assurance Vulnerability Alert) de l'agence DISA (Defense Information System Agency) que vous souhaitez rechercher. Par exemple, 2008-A-<nnnn>, où <nnnn> est un identificateur numérique.

Tableau 10-2 Paramètres Asset Profile Search (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 liens URL Generic Exploit URL links to exploit script/code or a detailed text file that explains how to exploit a specific vulnerability.*
Generic Informational URL	Entrez l'URL d'informations génériques que vous souhaitez rechercher. ***Remarque :*** *L' URL d'information générique se relie aux informations relatives au type ou 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 Mail List Post que vous souhaitez rechercher.
Metasploit ID	Entrez l'ID Metasploit que vous souhaitez rechercher.
Microsoft Knowledge Base Article	Entrez l'ID de Knowledge Base Article de 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 News Article que vous souhaitez rechercher. ***Remarque :*** *L'ID de News Article 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 10-2 Paramètres Asset Profile Search (suite)

Paramètre	Description
Autres Advisory URL	Entrez d'autres Advisory URL que vous souhaitez rechercher.
Autres 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 Secunia Advisory 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 Cyber security alert US-CERT que vous souhaitez rechercher. Par exemple, TA06-333A.
VUPEN Advisory	Entrez l'ID de VUPEN Advisory que vous souhaitez rechercher.
Vender Specific Advisory URL	Entrez l'URL de Vender Specific Advisory que vous souhaitez rechercher.
Vendor Specific News/Changelog Entry	Entrez l'URL de Vendor Specific New/Changelog Entry que vous souhaitez rechercher.
Vendor Specific Solution URL	Entrez l'URL du Vendor Specific Solution que vous souhaitez rechercher.
Vendor URL	Entrez l'URL du fournisseur que vous souhaitez rechercher.

La barre d'outils Asset Profile Search fournit les options suivantes:

Tableau 10-3 Assets tab toolbar

Options	Description
Add Asset	Cliquez sur **Add Asset** pour ajouter un profil d'actif. Voir **Ajouter un profil d'accès**.

Tableau 10-3 Assets tab toolbar (suite)

Options	Description
Actions	Cliquez sur **Actions** pour importer des actifs. Voir **Importer des profils d'actifs**. ***Remarque :*** *Le menu Actions est uniquement disponible si vous disposez des privilèges d'administrateur. Pour plus d'informations, voir le guide de l'administrateur IBM Security QRadar Network Anomaly Detection.*

Paramètres de la page Asset Profiles et fonctions de la barre d'outils

La page Asset Profiles fournit les informations suivantes sur chaque actif:

Tableau 10-4 Paramètres de la pageAsset Profile

Paramètre	Description
Adresse IP	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 de l'actif.
Vulnerabilities	Indique le nombre de vulnérabilités identifiées associées 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 page Asset Profiles fournit les fonctions suivantes

Tableau 10-5 Barre d'outils de la pa ge toprofils d'actifs functions

Fonction	Description
Modify Search	Cliquez sur **Modify Search** pour revenir à la page Assets Search et modifier vos critères de recherche. Voir **Etudier les profils d'actif**.
Add Asset	Cliquez sur **Add Asset** pour ajouter un profil d'actif. Voir **Ajouter un profil d'accèse**.
Edit Asset	Click **Edit Asset** pour modifier un profil d'actif a. Cette option est uniquement activée si vous avez sélectionné un profil d'actif dans la liste des résultats. Voir **Modifier un actif**.

Tableau 10-5 Barre d'outils de la pa ge toprofils d'actifs functions (suite)

Fonction	Description
Actions	Cliquez sur **Actions** pour effectuer les actions suivantes : • **Delete Asset** - Sélectionnez cette option pour supprimer les profils d'actif sélectionnés. Voir **Supprimer des actifs**. • **Delete Listed** - Sélectionnez cette option pour supprimer tous les profils d'actif énumérés dans la liste des résultats. Voir **Supprimer des actifs**. • **Import Assets** - Sélectionnez cette option pour importer des actifs. Voir **Importer des profils d'actifs**. • **Export to XML** - Sélectionnez cette option pour exporter des profils d'actif au format XML. Voir **Exporter des actifs**. • **Export to CSV** - Sélectionnez cette option pour exporter des profils d'actif au format CSV. Voir **Exporter des actifs**. ***Remarque :*** *Le menu **Actions** n'est disponible que si vous disposez des privilèges d'administrateur. Pour plus d'informations, voir le guide de l'administrateur IBM Security QRadar Network Anomaly Detection.*
Print	Cliquez sur **Print** pour imprimer les profils d'actif affichés sur la page.

Paramètres de la page Asset Profile et fonctions de la barre d'outils

La page Asset Profile fournit les informations suivantes :

Tableau 10-6 Paramètres de la page Asset Profile

Paramètre	Description
Name	Indique le nom des actifs.
Description	Indique une description pour cet actif.
Adresse IP	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.
système d'exploitation	Indique le système d'exploitation exécuté sur l'actif. ***Remarque :*** *Vous pouvez directement modifier 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.*

Tableau 10-6 Paramètres de la page Asset Profile (suite)

Paramètre	Description
Vendor	Indique le nom du fournisseur du système d'exploitation de l'actif, tel que détecté par le scanner VA ou entré manuellement. ***Remarque :*** *Vous pouvez directement modifier 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.*
Version	Indique la version du système d'exploitation. ***Remarque :*** *Vous pouvez modifier 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.*
Override	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 : • **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.

Tableau 10-6 Paramètres de la page Asset Profile (suite)

Paramètre	Description
Technical Owner	Indique le propriétaire technique de l'actif. Un responsable ou un directeur informatique 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 de la page Asset Profile fournit les fonctions suivantes :

Tableau 10-7 Page Profild'actifsbarre des tâches

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 **Etudier les profils d'actif**.
Print	Cliquez sur **Print** pour imprimer les profils d'actif affichés sur la page.

Le panneau Asset Profile de la page Asset Profile fournit les fonctions suivantes:

Tableau 10-8 Barre d'outils de la pa ge toprofils d'actifs functions

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 **Surveillance des violations groupées par réseau.**
View Source Summary	Si cet actif est la source d'une violation, 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 **Surveillance des violations groupées par IP source**.
View Destination Summary	Si cet actif est la destination d'une violation, 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 **Surveillance des violations groupées par IP cible**.

Tableau 10-8 Barre d'outils de la pa ge toprofils d'actifs functions (suite)

Options	Description
History	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 : • **Plage de temps** - Récent (dernières 24 heures) • **Search Parameters** - Indique les filtres suivants à appliquer aux résultats de la recherche : - Identity is true - Identity IP est l'adresse IP de l'actif • **Column Definition** - Indique les colonnes suivantes à afficher dans les résultats de la recherche : - Event name - Log Source - Start Time - Identity User Name - Identity MAC - Identity Host Name - Identity Net Bios Name - Identity Group Name Vous pouvez personnaliser les paramètres de recherche, si nécessaire. Cliquez sur **Search** pour afficher les informations historiques d'événement. Pour plus d'informations sur les événements de recherche, voir **Recherches de données**.
Applications	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 : • **Plage de temps** - Récent (dernières 24 heures) • **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. 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 **Recherches de données**.

Le panneau Ports and Vulnerabilities de la page Asset Profile affiche les informations suivantes :

Tableau 10-9 Paramètres de la fenêtre Ports and Vulnerabilities

Paramètre	Description
Vuln ID	Indique l'ID de la vulnérabilité. Le paramètre Vuln ID est un identificateur unique généré par Vulnerability Information System (VIS).
Port	Indique le numéro de port pour les services reconnus osur l'actif.
Service	Indique les services reconnus osur l'actif.
Name	Indique le nom de la vulnérabilité. ▶ Cliquez sur le lien pour afficher la fenêtre Research Vulnerability Details. Pour plus d'informations sur la fenêtre Research Vulnerability Details, voir **Paramètres de la fenêtre Review Vulnerability Details**
Description	Indique une description de la vulnérabilité détectée. Cette valeur n'est disponible que lorsque votre système intègre 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 sur l'actif soit de façon passive ou active.
First Seen	Indique la date et l'heure auxquelles le service a été détecté pour la première fois sur l'actif soit de façon passive ou active.
False Positive Tuning	Cliquez sur **False Positive Tuning** pour supprimer les vulnérabilités sélectionnées de la liste. ***Remarque :*** *Cette option est uniquement disponible si vous disposez de l'une des autorisations utilisateur suivantes : Admin ou Remove Vulnerabilities. Pour plus d'informations, voir IBM Security QRadar Network Anomaly Detection Guide d'administration.*

Paramètres de la fenêtre Review Vulnerability Details

La fenêtre Research Vulnerability Details fournit les détails suivants :

Tableau 10-10 Détails de la fenêtre Research Vulnerabilities Details

Paramètre	Description
Vuln ID	Indique l'ID de la vulnérabilité. Le paramètre Vuln ID est un identificateur 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 10-10 Détails de la fenêtre Research Vulnerabilities Details

Paramètre	Description
CVE	Indique l'identificateur CVE de la vulnérabilité. Les identificateurs CVE sont fournis par la base de données NVDB. ▶ Cliquez sur le lien pour obtenir plus d'informations. Le site Web NVDB s'affiche dans une nouvelle fenêtre de navigateur.
OSVDB	Indique l'identificateur OSVDB de la vulnérabilité. ▶ Cliquez sur le lien pour obtenir plus d'informations. Le site Web OSVDB s'affiche dans une nouvelle fenêtre de navigateur.
CVSS Score	Indique le score Common Vulnerability Scoring System (CVSS) de la vulnérabilité. Un score CVSS est une valeur permettant d'évaluer la gravité de la 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/*.
Description	Indique une description de la vulnérabilité détectée. Cette valeur n'est disponible que lorsque votre système intègre les outils V.
Concern	Indique les effets que la vulnérabilité peut avoir sur votre réseau.
Solution	Suivez les instructions fournies pour résoudre la vulnérabilité.
IPS/IDS Mitigation	Affiche des informations sur le périphérique Intrusion Prevention System/Intrusion Detection System (IPS/IDS) associé à cette vulnérabilité. Le tableau IPS/IDS Mitigation affiche les informations suivantes : • **QID** - Indique le QID associé à cette vulnérabilité. Un QID assigne une catégorie de niveau supérieur et de niveau inférieur d'identificateur 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.
Reference	Affiche la liste des références externes, y compris : • **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. ▶ 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.

Tableau 10-10 Détails de la fenêtre Research Vulnerabilities Details

Paramètre	Description
Products	Affiche la liste des produits qui sont associés à cette vulnérabilité. • **Vendor** - Indique le fournisseur du produit. • **Product** - Indique le nom du produit. • **Version** - Indique le numéro de version du produit.

11 GESTION DES RAPPORTS

Vous pouvez utiliser l'option **Reports** pour créer, modifier, distribuer, et gérer les rapports.

L'onglet **Reports** vous fournit :

- des options de rapports détaillées nécessaires pour respecter les diverses normes de réglementation, telles que la conformité PCI.
- la flexibilité dans la présentation et le contenu.

Présentation de l'onglet Reports

Vous pouvez créer vos propres rapports personnalisés dans Détection des anomalies QRadar ou utiliser des rapports par défaut. Vous pouvez personnaliser et renommer des rapports par défaut et les distribuer à d'autres utilisateurs Détection des anomalies QRadar.

L'onglet **Reports** peut nécessiter une période de temps plus longue pour s'actualiser si votre système comporte un nombre important de rapport.

Remarque : 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 le Support technique Microsoft.

Considérations du fuseau horaire

Pours'assurer que la fonction de production de rapports utilise la bonne date et heure pour le rapport de données, votre session Détection des anomalies QRadar doit correspondre à 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 correspond à votre fuseau horaire.

Autorisation de l'onglet Reports

Les administrateurs peuvent afficher tous les rapports créés par d'autres utilisateursDétection des anomalies QRadar. Les utilisateurs non administrateurs peuvent afficher uniquement les rapports qu'ils ont créés ou les rapports qui sont partagés par d'autres utilisateurs.

Paramètres de l'onglet Reports

L'onglet **Reports** affiche une liste de rapports personnalisés par défaut. Dans l'onglet **Reports**, vous pouvez afficher des informations statistiques sur le modèle de rapports, effectuer des actions sur des modèles de rapport, afficher des rapports générés, et supprimer le contenu généré.

L'onglet **Reports** fournit les inforfmations suivantes :

Tableau 11-1 Paramètres d'onglet des rapports

Paramètres	Description
Colonne Indicateur	Si une erreur se produit, provoquant l'échec de la génération du rapport, l'icône **Error** s'affiche dans cette colonne.
Nom de rapport	Indique le nom du rapport.
Groupe	Indique le groupe auquel appartient ce rapport.
Planification	Indique la fréquence à laquelle le rapport est généré. Les rapports qui indiquent une planification par intervalle, une fois activés, 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 **Génération manuelle d'un rapport**.
Prochaine phase d'exécution	Indique la durée, en heures et en minutes, jusqu'à la génération du prochain rapport.
Dernière modification	Indique la date de la dernière modification de ce rapport.
Propriétaire	Indique l'utilisateur Détection des anomalies QRadar qui possède le rapport.
Auteur	Indique l'utilisateur Détection des anomalies QRadar qui a créé le rapport.
Rapports générés	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 de rapports générés**. Si aucun rapport n'est généré, la valeur **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 : • **PDF** - Portable Document Format • **HTML** - Format Hyper Text Markup Language • **RTF** - Rich Text Format • **XML** - Extensible Markup Language (disponible uniquement pour les tableaux) • **XLS** - Microsoft® Excel format (disponible uniquement pour les tableaux)

Vous pouvez pointer votre souris sur n'importe quel rapport pour prévisualiser un résumé de rapport dans une infobulle. Le résumé indique la configuration du rapport et le type de contenu généré par le rapport.

Ordre de tri de l'onglet Reports

Par défaut, les rapports sont triés par la colonne **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 dossier (fréquence) de groupe.

Barre d'outils de l'onglet Reports

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 11-2 Options de la barre d'outils de l'onglet Reports

Option	Description
Groupe	A partir la zone de liste, sélectionnez le groupe que vous souhaitez afficher. le groupe s'affiche avec les rapports affectés. Pour plus d'informations, voir **Groupes de rapports**.
Gestion des groupes	Cliquez sur **Manage Groups** afin de gérer les groupes de rapports. En utilisant la fonction Manage Groups, vous pouvez organiser vos rapports en groupes fonctionnels. Pour plus d'informations, voir **Groupes de rapports**.

Tableau 11-2 Options de la barre d'outils de l'onglet Reports (suite)

Option	Description
Actions	Cliquez sur **Actions** pour effectuez les actions suivantes : • **Create** - Sélectionnez cette option afin de créer un nouveau rapport. Pour plus d'informations, voir **Modification d'un rapport**. • **Edit** - Sélectionnez cette option afin de modifier le rapport sélectionné. Vous pouvez également cliquer deux fois sur un rapport afin de modifier le contenu. • **Duplicate** - Sélectionnez cette option afin de dupliquer ou renommer le rapport sélectionné. Pour plus d'informations, voir **Duplication d'un rapport**. • **Assign Groups** - Sélectionnez cette option afin d'affecter le rapport sélectionné à un groupe de rapport. Pour plus d'informations, voir **Groupes de 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 **Génération manuelle d'un rapport**. Pour générer plusieurs rapports, maintenez la touche de contrôle enfoncée et cliquez sur le rapport que vous souhaitez générer. • **Run Report on Raw Data** - Sélectionnez cette options afin de générer le rapport sélectionné à l'aide de données brutes. Cette option est utile lorsque vous souhaitez générer un rapport avant que les données accumulées nécessaires ne soient disponibles. Par exemple, si vous souhaitez exécuter un rapport hebdomadaire avant qu'une semaine entière ne s'écoule depuis la création du rapport, vous pouvez générer le rapport à l'aide de cette option. • **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.
Masquage des rapports inactifs	Sélectionnez cette case afin de masquer les modèles de rapports inactifs. L'onglet **Reports** s'actualise automatiquement et affiche uniquement les rapports actifs. Décochez la case afin d'afficher les rapports inactifs masqués.

Tableau 11-2 Options de la barre d'outils de l'onglet Reports (suite)

Option	Description
Rapports de recherche	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 : • Titre de rapport • Description du rapport • Groupes de rapports • Nom d'utilisateur de l'auteur du rapport

Barre d'état

The La barre d'état affiche le nombre de résultats de recherche (**Affichage d'1 élément sur 10**) actuellement affichés et la durée de temps requise (**Temps écoulé :**) pour traiter les résultats de recherche.

Agencement du rapport

Un rapport peut être constitué de plusieurs éléments de données et peut représenter données réseau et de sécurité dans une variété de styles, tels que des tableaux, des graphiques linéaires, des graphiques circulaires et des graphiques à courbes.

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 la façon dont chaque graphique affiche un ensemble de données, voir **Types de graphique**.

Types de graphique

Lorsque vous créez un rapport, vous devez choisir un type de graphique pour chaque graphique que vous souhaitez inclure dans votre rapport. Le type de graphique détermine la façon dont le rapport généré présente des objets de données et de réseau. Vous pouvez créer des graphiques de données avec plusieurs caractéristiques et créer des graphiques dans un seul rapport généré.

Détection des anomalies QRadar inclut les types de graphique suivants :

- **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.
- **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 Guide de gestion sur l'évaluation dess vulnérabilités***IBM Security QRadar.*

- **Events/Logs** - Vous pouvez utiliser le graphique Event/Logs pour afficher des informations d'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 **Recherches de données**.

- **Flows** - Vous pouvez utiliser le graphique des flux pour afficher des informations de flux. 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 **Recherches de données**.

- **Top Destination IPs** - Le graphique Top Destination IPs affiche les adresses IP de destination dans les emplacements réseau que vous sélectionnez.
- **Top Offenses** - Le graphique Top Offenses affiche des violations TopN qui se produisent au moment présent pour les emplacements réseau que vous sélectionnez.
- **Top Source IPs** -Le graphique Top Source IPs affiche et tri des sources de violation (adresses IP) qui attaquent votre réseau et actifs métiers.

Pour plus d'informations sur ces types de graphique, voir **Paramètres du conteneur graphique**.

Types de graphe

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 utilisées par les graphiques 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 11-3 Types de graphiques

Type de graphique	Disponibilité
Graphique linéaire	Disponible avec les types de graphiques suivants : • Evénements/Journaux • Flux

Tableau 11-3 Types de graphiques (suite)

Type de graphique	Disponibilité
Graphique linéaire empilé	Disponible avec les types de graphiques suivants : • Evénements/Journaux • Flux
Graphique à barres	Disponible avec les types de graphiques suivants : • Evénements/Journaux • Flux • Vulnérabilités de l'actif
Graphique à barre horizontale	Disponible avec les types de graphiques suivants : • Adresses IP source • Violations • Adresses IP de destination
Graphique à barre empilée	Disponible avec les types de graphiques suivants : • Evénements/Journaux • Flux
Graphique circulaire	Disponible avec les types de graphiques suivants : • Evénements/Journaux • Flux • Vulnérabilités de l'actif
Graphique de tableau	Disponible avec les types de graphiques suivants : • Evénements/Journaux • Flux • Adresses IP source • Violations • Adresses IP de destination Pour afficher le contenu d'un tableau, vous devez concevoir le rapport avec un conteneur en pleine largeur.de page.
Tableau d'agrégation (synthétique)	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.

Création de rapports personnalisés

Dans l'onglet **Reports** vous pouvez accéder à l'instant de rapport pour créer un nouveau rapport.

A propos de cette tâche

L'assistant de rapport donne un guide d'instructions sur la manière de concevoir, planifier, et générer des rapports. L'assistant utilise les éléments clés suivants pour vous aider à créer un rapport :

- **Layout** - Position et taille de chaque conteneur
- **Container** - Marque de réservation pour le contenu présenté
- **Content** - Définition du graphique placé dans le conteneur

Après avoir créé un rapport qui se 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 la période planifiée pour obtenir des résultats. Par exemple, une recherche hebdomadaire nécessite 7 jours pour créer des données. Cette recherche ne renvoie de résultats avant 7 jours.

Lorsque vous indiquez le format de sortie d'un rapport, considérez que la taille du fichier des rapports générés peut atteindre un ou deux mégaoctet, en fonction du format de sortie sélectionné. Le format PDF est la plus petite taille et n'occupe pas un espace important dans le disque de stockage.

Procédure

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

Etape 2 Dans la zone de liste **Actions**, sélectionnez **Create**.

Etape 3 Sur la page d'accueil, cliquez sur **Next** pour passer à la page suivante de l'assistant de rapport.

Etape 4 Sélectionnez l'une des options de planification suivantes:

Option	Description
Manuellement	Génère un rapport une seule fois. Il s'agit du réglage par défaut, mais vous pouvez générer ce rapport aussi souvent que nécessaire.
Horaire	Planifie le rapport pour une génération à la fin de chaque heure en utilisant les données des heures précédentes. Si vous choisissez une option de type Hourly, une autre configuration est obligatoire. Dans les zones de liste, sélectionnez un laps de temps pour démarrer et terminer le cycle de génération. Un rapport est généré pour chaque heure dans ce laps de temps. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00 pour les deux zones **From** et **To**.

Option	Description
Quotidien	Planifie le rapport pour une génération quotidienne en utilisant les données de la journée précédente. Pour chaque graphique du rapport, vous pouvez sélectionner les 24 dernières heures de la journée, ou sélectionner un laps de temps spécifique de la journée précédente. Si vous sélectionnez l'option **Daily**, une configuration supplémentaire est nécessaire. Cochez la case correspondant à chaque jour selon lequel 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.
Hebdomadaire	Planifie le rapport pour une génération hebdomadaire en utilisant les données de la semaine précédente. Si vous sélectionnez l'option **Weekly**, une configuration supplémentaire est requise. 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.
Mensuelle	Planifie le rapport pour une génération mensuelle en utilisant les données du mois précédent. Sic vous sélectionnez l'option **Monthly**, une configuration supplémentaire est requise. A partir de la zone de liste, sélectionnez la date à laquelle 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 début pour le cycle de génération de rapports. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.

Etape 5 Pour permettre à ce rapport de générer un panneau manuel, sélectionnez l'une des options suivantes puis cliquez sur **Next**:

- **Yes** - Active la génération manuelle de ce rapport.
- **No** - Désactive la génération manuelle de ce rapport.

Etape 6 Configurel'agencement 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 l'assistant de rapport.

c Cliquez sur **Next** afin de passer à la page suivante de l'assistant de rapport.

Etape 7 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. Pour plus d'informations sur l'image de marque de votre rapport, voir **Rapports de marque**.

Etape 8 Configurez chaque conteneur dans le rapport :

a Dans la zone de liste **Chart Type** sélectionnez un type de graphique. Voir **Types de graphique**.

b Dans la fenêtre Container Details - <chart_type>, configurez les paramètres graphiques. Pour des informations détaillées sur la configuration de votre graphique, voir **Paramètre du conteneur graphique**.

c Cliquez sur **Save Container Details**.

L'assistant revient à la page Specify Report Contents, vous permettant ainsi de configurer d'autres conteneurs dans votre rapport.

d Si nécessaire, répétez les étapes **a** à **c** pour tous les conteneurs.

e Cliquez sur **Next** pour passer à la page suivante de l'assistant de rapport.

Etape 9 Repartez à la page Layout Preview, puis cliquez sur **Next** pour passer à l'étape suivante de l'assistant de rapport.

Etape 10 Sélectionnez les cases pour les formats de rapport que vous souhaiter générer, puis cliquez sur **Next**.

Les options incluent les formats de rapport suivants :

- **PDF** - Portable Document Format
- **HTML** - Format Hyper Text Markup Language
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (disponible uniquement pour les tableaux)
- **XLS** - Format Microsoft® Excel

Etape 11 Sélectionnez les canaux de distribution pourvotre rapport, puis cliquez sur **Next**. Les options incluent les canaux de distribution suivants :

Option	Description
Console de rapport	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 peuvent être en mesure de d'afficher le rapport généré.	Cette option s'affiche uniquement une fois que vous avez coché la case **Report Console**. Dans la liste des utilisateurs, sélectionnez les utilisateurs Détection des anomalies QRadar auxquels vous souhaitez accorder le droit d'afficher les rapports générés. ***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 la section IBM Security QRadar Network Anomaly DetectionAdministration Guide.*
Sélectionnez tous les utilisateurs	Cette option s'affiche uniquement une fois que vous avez coché la case **Report Console**. Cochez cette case si vous voulez accorder le droit à tous les utilisateurs Détection des anomalies QRadar d'afficher les rapports générés. ***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 la section IBM Security QRadar Network Anomaly DetectionAdministration Guide.*
Courrier électronique	Cochez cette case si vous voulez distribuer le rapport généré par courrier électronique.
Entrez le(s) adresse(s) e-mail de distribution de rapport	Cette option s'affiche uniquement une fois que vous avez coché la case **Email**. Entrez l'adresse e-mail de chaque destinataire de rapport généré; séparez la liste des adresses e-mail avec des virgules. Le nombre maximal de caractères pour ce paramètre est 255. ***Remarque :*** *Les destinataires reçoivent cet e-mail de no_reply_reports@qradar.*
Incluez le rapport comme pièce jointe (non-HTML uniquement)	Cette option s'affiche uniquement une fois que vous avez coché la case **Email**. Cochez cette case pour envoyer le rapport généré en tant que pièce jointe.

Option	Description
Incluez un lien à la console de rapport	Cette option s'affiche uniquement une fois que vous avez coché la case **Email**. Cochez cette case pour inclure un lien à la console de rapport dans l'e-mail.

Etape 12 Sur la page Finishing Up, entrez les valeurs pour les paramètres suivants :

Paramètre	Description
Description du rapport	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.
Groupes	Sélectionnez les groupes auxquels vous voulez assigner ce rapport. Pour plus d'informations à propos des groupes, voir **Groupes de rapport**.
Voulez-vous exécutez le rapport maintenant ?	Cochez cette case si vous souhaitez générer le rapport lorsque l'assistant est terminé. Par défaut, la case est cochée.

Etape 13 Cliquez sur **Next** afin d'afficher le rapport récapitulatif.

Etape 14 Sur la page Report Summary, sélectionnez les onglets disponibles sur le rapport récapitulatif pour prévisualiser votre configuration de rapport.

Etape 15 Cliquez sur **Finish**.

Résultat

Le rapport se génère immédiatement. Si vous avez décoché la case **Would you like to run the report now?** sur la dernière page de l'assistant, le rapport est enregistré et génère au temps prévu.

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 le rapport d'origine reste le même.

Tâches de gestion des rapports

A l'aide de l'onglet Reports et de l'assistant de rapports, vous pouvez gérer vos rapports. Vous pouvez modifier, dupliquer, partager, et marquer vos rapports. Vous pouvez également supprimer les rapports générés.

Modification d'un rapport

A l'aide de l'assistant de rapports, vous pouvez modifier tous les rapports par défaut ou personnalisés.

A propos de cette tâche

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.

Procédure

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

Etape 2 Cliquez deux fois sur le rapport que vous souhaitez personnaliser.

Etape 3 Sur l'assistant de rapport, modifiezles paramètres afin de personnaliser le rapport et générer le contenu dont vous avez besoin. Pour plus d'informations sur la façon d'utiliser l'assistant de rapport, voir **Création de rapports personnalisés**.

Etape 4 Cliquez sur **Finish**.

Résultat

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 le rapport d'origine reste le même.

Affichage de rapports générés

Dans l'onglet **Reports**, une icône s'affiche dans la colonne **Formats** au cas où un rapport génère le contenu. Vous pouvez cliquer sur l'icône pour afficher le rapport.

A propos de cette tâche

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 dispose pas de contenu généré, la valeur **None** s'affiche dans la colonne **Generated Reports**.

Les icônes qui représentent le format de rapport pour le format généré s'affichent dans la colonne **Formats**. Les rapports peuvent être générés selon les formats suivants :

- **PDF** - Portable Document Format
- **HTML** - Format Hyper Text Markup Language
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (disponible uniquement pour les tableaux)
- **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).

Vous pouvez uniquement afficher les rapports auxquels vous avez eu accès de l'administrateurDétection des anomalies QRadar. Les administrateurs peuvent accéder à tous les rapports.

Si vous utilisez Mozilla Firefox comme navigateur et si vous sélectionnez le format de rapport RTF, le navigateur Mozilla Firefox lance une nouvelle fenêtre de navigateur. Ce lancement de la nouvelle fenêtre est le résultat de la configuration du navigateur Mozilla Firefox et n'affecte pas Détection des anomalies QRadar. Vous pouvez fermer la fenêtre et continuer votre session Détection des anomalies QRadar.

Procédure

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

Etape 2 Dans la zone de liste de la colonne **Generated Reports,** sélectionnez l'horodatage de rapport que vous souhaitez afficher.

Etape 3 Cliquez sur l'icône du format que vous souhaitez afficher.

Résultat

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.

Procédure

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

Etape 2 Sélectionnez les rapports pour lesquels vous souhaitez supprimer le contenu généré

Etape 3 Dans la zone de liste **Actions**, cliquez sur **Delete Generated Content**.

Résultat

Tout le contenu généré pour le rapport sélectionné est supprimé.

Génération manuelle d'un rapport

Un rapport peut être configuré de sorte à se générer automatiquement, toutefois, vous pouvez générer un rapport manuellement à tout moment.

A propos de cette tâche

Lorsqu'un rapport se 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 sur 3.
- **(*x* hour(s) *x* min(s) *y* sec(s))** - Le rapport est planifié pour s'exécuter. Le message est un compte cà rebours qui indique à quel moment le rapport suivant doit s'exécuter.

Vous pouvez sélectionner l'icône **Refresh** pour actualiser l'affichage, y compris les informations dans la colonne **Next Run Time**.

Procédure

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

Etape 2 Sélectionnez le rapport que vous souhaitez générer.

Etape 3 Cliquez sur **Run Report**.

Etape suivante

Après la génération d'un rapport, vous pouvez afficher le rapport généré dans la colonne **Generated Reports**. Voir **Affichage de rapports générés**.

Duplication d'un rapport

Pour créer un rapport qui ressemble étroitement à un rapport existant, vous pouvez dupliquer le rapport que vous souhaitez modéliser, ensuite personnalisez-le.

Procédure

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.

Etape 5 Cliquez sur **OK**.

Le nouveau rapport s'affiche dans la liste des rapports.

Etape suivante

Vous pouvez personnaliser le rapport dupliqué. Voir **Modification d'un 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.

A propos de cette tâche

Toutes les mises à jour effectuées par l'utilisateur sur un rapport partagé n'affecte pas la version originale du rapport.

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.

Procédure

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**.

Rapports de marque

Pour marquer les rapports, vous pouvez importer des logos et des images spécifiques. Pour des rapports de marque avec des logos personnalisés, vous devez télécharger et configurer les logos avant de commencer à utiliser l'assistant de rapport.

Avant de commencer

Assurez-vous que le graphique que vous souhaitez utiliser est de type 144 x 50 pixels avec un fond blanc.

Pour vous assurer que votre navigateur affiche le nouveau logo, désactivez votre cache du navigateur.

A propos de cette tâche

Le rapport de marque est bénéfique pour votre entreprise si vous prenez en charge plus d'un seul logo. Lorsque vous téléchargez une image sur Détection des anomalies QRadar, elle est automatiquement enregistrée en tant que Portable Network Graphic (PNG).

Lorsque vous téléchargez une nouvelle image et que vous la définissez comme votre image par défaut, elle 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.

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.

Procédure

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**.

Etape 6 Cliquez sur **Upload Image** afin de télécharger l'image surDétection des anomalies QRadar.

Etape 7 Sélectionnez le logo que vous souhaitez utiliser par défaut et cliquez sur **Set Default Image**.

Groupes de rapports

Dans l'onglet **Reports**, vous pouvez trier la liste des rapports en groupes fonctionnels. Si vous classez les rapports en groupes, vous pouvez organiser et trouver les rapports de manière plus efficace. Par exemple, vous pouvez afficher tous les rapports relatifs à la conformité Payment Card Industry Data Security Standard (PCIDSS).

Pardéfaut, l'onglet **Reports** affiche la liste de tous les rapports, toutefois, vous pouvez classer les rapports en groupes tels que :

- Conformité
- Exécutifs
- Sources de journal
- Gestion de réseau
- Sécurité
- Protocole voix sur IP VoIP
- Autres

Lorsque vous créez un nouveau rapport, vous pouvez affecter le rapport à un groupe existant ou créer un nouveau groupe. Vousdevez disposer d'un accès administrateur pour créer, modifier, ou supprimer des groupes. Pour plus d'infordmations sur les rôles utilisateur, voir la section *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Création d'un groupe

Détection des anomalies QRadar inclut des groupes de rapport par défaut, toutefois, vous pouvez aussi ajouter des groupes.

Procedure

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.

Etape 4 Cliquezsur **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

Vous pouvez modifier un groupe de rapport pour changer le nom ou la description.

Procédure

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 modifier.

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.

Procédure

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

Etape 2 Sélectionnez le rapport que vous souhaitez affecter à un groupe.

Etape 3 Dans 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.

Procédure

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 de rapport d'un groupe

En utilisant l'icône **Remove**, vous pouvez supprimer un rapport d'un groupe.

A propos de cette tâche

Lorsque vous supprimez un rapport d'un groupe, il existe toujours dans l'onglet **Reports**. Le rapport n'est pas supprimé de votre système.

Procédure

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.

Paramètres du conteneur graphique

Le type de graphique détermine la façon dont le rapport généré présente des données et des objets de réseau. Vous pouvez créer des graphiques de données avec plusieurs caractéristiques et créer des graphiques dans un seul rapport généré.

Paramètre du conteneur graphique pour l'évaluation des vulnérabilités des actifs

Le tableau suivant décrit les paramètres du conteneur graphique pour l'évaluation des vulnérabilités des actifs :

Tableau 11-4 Paramètres de conteneurs graphique pour la vulnérabilité des actifs

Paramètre	Description
Détails du conteneur - Actifs	

Tableau 11-4 Paramètres de conteneurs graphique pour la vulnérabilité des actifs (suite)

Paramètre	Description
Titre de graphique	Entrez un titre de graphique ne dépassant pas 100 caractères.
Sous titre de graphique	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas 100 caractères.
Actifs limités	Dans la zone de liste, sélectionnez le nombre d'actifs que vous souhaitez inclure dans ce rapport.
Type de graphique	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **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 du sous-rapport. 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 **Types de graphique**.
Commande des actifs par	Sélectionnez le type de données en fonction desquelles vous souhaitez que le graphique soit trié. Les options incluent : • **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.
Détails de sous-rapport	
Sous-rapport	Indique le type d'informations affichées dans le sous-rapport.

Tableau 11-4 Paramètres de conteneurs graphique pour la vulnérabilité des actifs (suite)

Paramètre	Description
Triage de sous-rapport par	Sélectionnez le paramètre en fonction duquel vous souhaitez organiser le sous-rapport. Les options incluent : • Risqsue (Score de base) • OSVDB ID • Titre OSVDB • Dernière date modifiée • Date de divulgation • Date de détection Pour plus d'information sur la base de données Open Source Vulnerability (OSVDB), voir *http://osvdb.org/*.
Limitation de sous-rapport	Dans la zone de liste, sélectionnez le nombre de vulnérabilités que vous souhaitez inclure dans ce sous-rapport.
Contenu du graphique	
Vulnérabilités	Pour indiquer les vulnérabilités que vous souhaitez signaler : **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 vuilnérabiloté, voir **Gestion des actifs**. **3** Dans la liste **Search Results**, sélectionnez les vulnérabilités que vous souhaitez signaler. Cliquez sur **Add**. **4** Cliquez sur **Submit**.
Adresse IP	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.
Réseaux	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels vous pouvez recueillir des données graphiques.

Paramètres du conteneur graphique Event/Logs

Le tableau suivant décrit les paramètres du conteneur graphique Events/Logs :

Tableau 11-5 Paramètres de conteneur graphique Event/Logs

Paramètre	Description
Détails du conteneur - Events/Logs	
Titre de graphique	Entrez un titre de graphique ne dépassant pas 100 caractères.

Tableau 11-5 Paramètres de conteneur graphique Event/Logs (suite)

Paramètre	Description
Sous titre de graphique	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas 100 caractères.
Limitation Events/Logs	Dans la zone de liste, sélectionnez le nombre d'événements/journaux à afficher dans le rapport généré.
Type de graphique	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **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. Pour afficher des exemples de chaque type de données des graphiques, voir **Types de graphique**.

Tableau 11-5 Paramètres de conteneur graphique Event/Logs (suite)

Paramètre	Description
Planification manuelle	Le panneau Manual Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Manually** dans l'assistant de Report. En utilisant les options Manual Scheduling, vous pouvez créer une planification manuelle qui peut exécuter un rapport sur une période de temps personnalisée, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez. Par exemple, vous pouvez planifier un rapport pour qu'il s'exécute du 1er au 31 octobre, incluant uniquement les données générées pendant vos heures de travail, telles que de lundi à vendredi, entre 8 heures et 21 heures. Pour créer une planification manuelle : **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. ***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.*

Tableau 11-5 Paramètres de conteneur graphique Event/Logs (suite)

Paramètre	Description
	Afin d'affiner d'avantage votre planification : **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 planifier votre rapport.
Planification horaire	Le panneau Hourly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Hourly** dans l'assistant de Report. ▶ Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.* La planification horaire place automatiquement dans des graphiques toutes les données de l'heure précédente.

Tableau 11-5 Paramètres de conteneur graphique Event/Logs (suite)

Paramètre	Description
Planification quotidienne	Le panneau Daily Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Daily** dans l'assistant de rapport. **1** Sélectionnez une des options suivantes : • **Toutes les données du jour précédent (24 heures)** • **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. **2** Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.*

Tableau 11-5 Paramètres de conteneur graphique Event/Logs (suite)

Paramètre	Description
Programmation hebdomadaire	Le panneau Weekly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Weekly** dans l'assistant de rapport. **1** Sélectionnez une des options suivantes : • **Toutes les données de la semaine précédente** • **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. **2** Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.* Afin d'affiner d'avantage votre planification : **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.

Tableau 11-5 Paramètres de conteneur graphique Event/Logs (suite)

Paramètre	Description
Planification mensuelle	Le panneau Monthly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Monthly** dans l'assistant de rapport. **1** Sélectionnez une des options suivantes : • **Toutes le données du mois précédent** • **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. **2** Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.* Afin d'affiner d'avantage votre planification : **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 planifier votre rapport.
Contenu du graphique	
Groupe	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**.

Tableau 11-5 Paramètres de conteneur graphique Event/Logs (suite)

Paramètre	Description
Entrez une recherche enregistrée ou sélectionnez une à partir de a liste	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 une liste de 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.
Recherches enregistrées disponibles	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 ou Select from List**.
Création d'une nouvelle recherche d'événement	Cliquez sur **Create New Event Search** pour créer une nouvelle recherche. Pour plus d'informations sur la création d'une recherche d'événements, voir **Etude de l'activité du journal**.

Paramètres du conteneur graphique des flux

Le tableau suivant décrit les paramètres du conteneur graphique des flux :

Tableau 11-6 Détails de conteneur du graphique des flux

Paramètre	Description
Détails de conteneur - Flux	
Titre de graphique	Entrez un titre de graphique ne dépassant pas 100 caractères.
Sous titre de graphique	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas 100 caractères.
Limitation des flux	Dans la zone de liste, sélectionnez le nombre de flux qui doivent être affichés dans le rapport généré.

Tableau 11-6 Détails de conteneur du graphique des flux (suite)

Paramètre	Description
Type de graphique	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **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. Pour afficher des exemples de chaque type de données des graphiques, voir **Types de graphique**.

Tableau 11-6 Détails de conteneur du graphique des flux (suite)

Paramètre	Description
Planification manuelle	Le panneau Manual Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Manually** dans l'assistant de rapport. En utilisant les options Manual Scheduling, vous pouvez créer une planification manuelle qui peut exécuter un rapport sur une période de temps personnalisée, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez. Par exemple, vous pouvez planifier un rapport pour qu'il s'exécute du 1er au 31 octobre, incluant uniquement les données générées pendant vos heures de travail, telles que de lundi à vendredi, entre 8 heures et 21 heures. Pour créer une planification manuelle : **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. ***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.*

Tableau 11-6 Détails de conteneur du graphique des flux (suite)

Paramètre	Description
	Afin d'affiner d'avantage votre planification : **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. Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.
Planification horaire	Le panneau Hourly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Hourly** dans l'assistant de rapport. ▶ Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.* La planification horaire place automatiquement dans des graphiques toutes les données de l'heure précédente.

Tableau 11-6 Détails de conteneur du graphique des flux (suite)

Paramètre	Description
Planification quotidienne	Le panneau Daily Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Daily** dans l'assistant de rapport. **1** Sélectionnez une des options suivantes : • **Toutes les données du jour précédent (24 heures)** • **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. **2** Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.*

Tableau 11-6 Détails de conteneur du graphique des flux (suite)

Paramètre	Description
Programmation hebdomadaire	Le panneau Weekly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Weekly** dans l'assistant de rapport. **1** Sélectionnez une des options suivantes : • Toute les données de la semaine précédente • **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. **2** Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.* Afin d'affiner d'avantage votre planification : **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.

Tableau 11-6 Détails de conteneur du graphique des flux (suite)

Paramètre	Description
Planification mensuelle	Le panneau Monthly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Monthly** dans l'assistant de rapport. **1** Sélectionnez une des options suivantes : • **Toutes le données du mois précédent** • **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. **2** Dans la zone de liste **Timezone**, sélectionnez le fuseau horaire que vous souhaitez utiliser pour votre rapport. ***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.* Afin d'affiner d'avantage votre planification : **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 planifier votre rapport.
Contenu du graphique	
Groupe	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**.

Tableau 11-6 Détails de conteneur du graphique des flux (suite)

Paramètre	Description
Entrez une recherche enregistrée ou sélectionnez une à partir de la liste	Pour affiner la liste **Available Saved Searches**, entrez le nom de la recherche que vous souhaitez localiser dans la zone **Type Saved Search ou 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.
Recherches enregistrées disponibles	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 ou Select from List**.
Création d'une nouvelle recherche de flux	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 **Etude de l'activité du réseau**.

Paramètres du conteneur graphique Top Source IPs

Le tableau suivant décrit les paramètres du conteneur graphique Top Source IPs :

Tableau 11-7 Paramètres de conteneurs graphique des adresses IP source

Paramètre	Description
Détails de conteneurs - Adresses IP source	
Titre de graphique	Entrez un titre de graphique ne dépassant pas 100 caractères.
Sous titre de graphique	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas 100 caractères.
Limitation des adresses IP source	Dans la zone de liste, sélectionnez le nombre d'adresses IP source devant être affichées dans le rapport généré.
Type de graphique	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **Table** - Affiche les données sous la forme d'un tableau (uniquement avec conteneur de largeur pleine page). • **Horizontal Bar** - Affiche les données dans un graphique à barres.
Triage de résultats par	Dans la zone de liste, sélectionnez la façon dont les données sont triées sur le graphique. Les options incluent : • Poids des actifs • Risque • Ampleur
Contenu du graphique	

Tableau 11-7 Paramètres de conteneurs graphique des adresses IP source (suite)

Paramètre	Description
Réseaux	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels vous pouvez recueillir des données graphiques.

Paramètres du conteneur graphique Top Offenses

Le tableau suivant décrit les paramètres du conteneur graphique Top Offenses :

Tableau 11-8 Paramètres de conteneur graphique des violations

Paramètre	Description
Détails de conteneurs - Violations	
Titre de graphique	Entrez un titre de graphique ne dépassant pas 100 caractères.
Sous titre de graphique	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas 100 caractères.
Limitation des violations	Dans la zone de liste, sélectionnez le nombre de violations à inclure dans les graphiques. La valeur configurée par défaut est 10.
Type de graphique	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **Table** - Affiche les données sous la forme d'un tableau (uniquement avec conteneur de largeur pleine page). • **Horizontal Bar** - Affiche les données dans un graphique à barres.
Triage de résultats par :	Dans la zone de liste, sélectionnez le tri des données sur le graphique. Les options incluent : • Gravité • Ampleur • Pertinence • Crédibilité
Contenu du graphique - Paramètre de base	
Paramètre de base	Sélectionnez cette option si vous souhaitez inclure un graphique de violations basé sur un paramètre dans votre rapport. Une fois cette option sélectionnée, la catégorie **Include**, **Offenses,** et les paramètres **Networks** s'affichent.

Tableau 11-8 Paramètres de conteneur graphique des violations (suite)

Paramètre	Description
Inclure	Cette option s'affiche uniquement si l'option **Parameter Based** est sélectionnée. Cochez la case à côté de l'option que vous souhaitez inclure dans le rapport généré. Les options sont : • Violations actives • Violations inactives • Violations masquées • Violations fermées Les options **Active Offenses** et **Inactive Offenses** sont sélectionnées par défaut. Si vous décochez toutes les cases, aucune restriction n'est appliquée au rapport généré; par conséquent, le rapport généré inclut toutes les violations.
Catégorie de violations	Cette option s'affiche uniquement si l'option **Parameter Based** est sélectionnée. Dans la zone de liste **High Level Category**, sélectionnez la catégorie de niveau supérieur que vous souhaitez inclure dans le rapport généré. Dans la zone de liste **Low Level Category**, sélectionnez la catégorie de niveau bas que vous souhaitez inclure dans le rapport généré. Pour plus d'informations sur les catégories de niveau bas et supérieur, voir la section *IBM Security QRadar Network Anomaly Detection Administration Guide*.
Réseaux	Cette option s'affiche uniquement si l'option **Parameter Based** est sélectionnée. Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels vous pouvez recueillir des données graphiques.
Contenu du graphique - Recherches de base enregistrées	
Recherche de base enregistrées	Sélectionnez cette option si vous souhaitez inclure un graphique de violations basé sur une recherche enregistrée dans votre rapport. Une fois cette option sélectionnée, les paramètres **Type Saved Search ou Select from List, et Available Saved Searches** s'affichent.
Groupe	Dans la zone de liste, sélectionnez un groupe de recherche enregistrée pour afficher les recherches enregistrées appartenant à ce groupe dans la zone de liste **Available Saved Searches**.

Tableau 11-8 Paramètres de conteneur graphique des violations (suite)

Paramètre	Description
Type Saved Search ou 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 ou 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.
Recherches enregistrées disponibles	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 ou Select from List**.

Paramètres du conteneur graphique Top Destination IPs

Le tableau suivant décrit les paramètres du conteneur graphique Top Destination IPs :

Tableau 11-9 Paramètres du conteneur graphique des adresses IP de destination

Paramètre	Description
Détails du codnteneur - Adresses IP de destination	
Titre de graphique	Entrez un titre de graphique ne dépassant pas 100 caractères.
Sous titre de graphique	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas 100 caractères.
Limitation des adresses IP de destination	Dans la zone de liste, sélectionnez le nombre d'adresses IP destination devant être affichées dans le rapport généré.
Type de graphique	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **Table** - Affiche les données sous la forme d'un tableau (uniquement avec conteneur de largeur pleine page). • **Horizontal Bar** - Affiche les données dans un graphique à barres.
Triage de résultats par	Dans la zone de liste, sélectionnez l'affichage des données dans le graphique. Les options incluent : • Poids des actifs • Niveau de risque • Ampleur
Contenu graphique	
Réseaux	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels vous pouvez recueillir des données graphiques.

A TESTS DE RÈGLE

Vous pouvez exécuter des tests sur la propriété d'un événement, d'un flux ou d'une violation telle qu'une adresse IP source, la gravité d'un événement ou l'analyse de taux.

Tests de règle d'événement

Cette section fournit des informations sur les tests de règle d'événement que vous pouvez appliquer à la règle notamment :

- **Test de profile d'hôte**
- **Tests d'adresse IP/Port**
- **Test de propriété d'événement**
- **Tests de propriété communs**
- **Tests de source du journal**
- **Fonction - tests de séquence**
- **Fonction - tests du compteur**
- **Fonction - tests simples**
- **Tests de la date/heure**
- **Tests de propriété du réseau**
- **Fonction - tests négatifs**

Test de profile 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	Valide 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 : • **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**	Configurez les paramètres suivants : • **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 prenne en considération l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est **actively or passively seen**.
Host Existence	Valide lorsque l'hôte source ou de destination est connu pour sa présence via l'analyse active ou passive. Vous pouvez également spécifier si le statut du host est détecté en utilisant l'une des méthodes suivantes : • **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**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test s'applique 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 prenne en considération 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	Valide 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 : • **source | destination** - Indiquez si vous souhaitez que ce test s'applique l'hôte source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test prenne en considération les valeurs supérieures ou inférieures à l'âge d'hôte de du profil. • **this number of** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **time intervals** - Indiquez si ce test doit prendre en considération les minutes ou les heures.
Host Port Age	Valide lorsque l'âge du profil du port source ou de destination est supérieure ou inférieur 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 : • **source | destination** - indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne 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	Valide 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 : • **source | destination** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération.
Host Vulnerable to Event	Valide 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 : • **destination | source | local host | remote host** - Indiquez si vous souhaitez que ce test prenne en considération 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 prenne en considération 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 prenne en considération n'importe quel port en cours. La valeur par défaut est **any IP**.

Tableau A-1 Règle d'événement : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
OSVDB IDs	Valide lorsqu'une adresse IP (source ou destination) est vulnérable aux ID de Open Source Vulnerability Database (OSVDB) condigurés.	lorsque l'IP source (**source IP**) est vulnérable à l'un des ID OSVDB (**OSVDB ID) suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. Pour plus d'informations concernant les ID de OSVDB, consultez *http://osvdb.org/*.

Tests d'adresse IP/Port Les tests d'adresse IP/Port comprennent :

Tableau A-2 Event Rule: IP / Port Test Group

Test	Description	Default Test Name	Parameters
Source Port	Valide lorsque le port 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 vous souhaitez que ce test prenne en considération.
Destination Port	Valide 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 vous souhaitez que ce test prenne en considération.
Local Port	Valide 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 vous souhaitez que ce test prenne en considération.
Remote Port	Valide lorsque le port distant de l'événement fait partie des ports distants configurés.	lorsque le port distant est l'un des ports suivants	**ports** - Indiquez les ports que vous souhaitez que ce test prenne en considération.
Source IP Address	Valide 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 vous souhaitez que ce test prenne en considération.
Destination IP Address	Valide lorsque l'adresse IP de destination de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP de destination fait partie des adresses IP suivantes	**IP addresses** - Indiquez les adresses IP que vous souhaitez que ce test prenne en considération.

Tableau A-2 Event Rule: IP / Port Test Group (suite)

Test	Description	Default Test Name	Parameters
Local IP Address	Valide 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 vous souhaitez que ce test prenne en considération.
Remote IP Address	Valide 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 vous souhaitez que ce test prenne en considération.
IP Address	Valide lorsque l'adresse IP source ou de destination 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 vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération.

Test 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	Default Test Name	Parameters
Local Network Object	Valide lorsque l'événement se produit dans le réseau spécifié.	lorsque le réseau de **destination est** l'un des réseaux suivants	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test prenne en considération l'adresse IP source ou de destination de l'événement. • **one of the following networks** - Indiquez les zones du réseau sur lesquelles vous souhaitez que ce test s'applique.
IP Protocol	Valide lorsque le protocole IP de l'événement est l'un des protocoles configurés.	lorsque le protocole IP est l'un des protocoles **suivants**	**protocols** - Indiquez les protocoles que vous souhaitez ajouter à ce test.
Event Payload Search	Chaque événement contient une copie de l'événement original non normalisé. Ce test est valide lorsque la chaîne de recherche entrée est incluse dans n'importe quel emplacement du contenu de l'événement.	lorsque le contenu de l'événement contient **cette chaîne**	**this string** - Indiquez la chaîne que vous souhaitez inclure pour ce test.

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Default Test Name	Parameters
QID of Event	Un QID est un identificateur unique pour les événements. Ce test est valide lorsque l'identificateur d'événement est un QID configuré.	lorsque le QID d'événement de l'un des **QID suivants**	**QIDs** - Utilisez l'une des options suivantes pour localiser les QID : • Sélectionnez l'option Browse By Category et dans les 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. Valide si le contexte d'événement est l'une des options suivantes : • Local to Local • Local to Remote • Remote to Local • Remote to Remote	lorsque le contexte d'événement représente **ce contexte**	**this context** - Indiquez le contexte que vous souhaitez que ce test prenne en considération. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Event Category	Valide lorsque la catégorie d'événement est la même que celle qui est configurée, par exemple, l'attaque Denial of Service (DoS).	lorsque la catégorie d'événement pour l'événement est l'une des catégories suivantes	**categories** - Indiquez la catégorie d'événement que vous souhaitez que ce test prenne en considération. Pour plus d'informations sur les catégories d'événement, voir le guide d'administration *IBM Security QRadar Network Anomaly Detection*.
Severity	Valide 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 : • **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**.

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Default Test Name	Parameters
Credibility	Valide lorsque la crédibilité est supérieure, inférieure ou égale à la valeur configurée.	lorsque la crédibilité de l'événement est **supérieure à 5 {par défaut}**	Configurez les paramètres suivants : • **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	Valide lorsque la pertinence de l'événement est supérieure, inférieure ou égale à la valeur configurée.	Lorsque la pertinence de l'événement est **supérieure à 5 (par défaut}**	Configurez les paramètres suivants : • **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	Valide 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	Valide 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.
Rate Analysis	QRadar Network Anomaly Detection contrôle les taux d'événement de tous(tes) les adresses/QID IP source et de destination et marque les événements qui annexent le comportement de taux anormaux. Valide lorsque l'événement est marqué pour l'analyse de taux.	Lorsque l'événement a été marqué avec l'analyse de taux.	N/A
Geographic Location	Valide lorsque l'adresse IP source correspond à l'emplacement géographique configurée.	lorsque la source est localisée dans cette région **géographique**	**geographic location** - Sélectionnez un emplacement géographique.

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Default Test Name	Parameters
False Positive Tuning	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 supprimer le réglage d'un faux positif, vous pouvez éditer les valeurs de réglage nécessaires.	Lorsque la signature du faux positif correspond à l'une des signatures suivantes	**signatures** - Indiquez la signature du faux positif que vous souhaitez que ce test doit prenne en considération. Entrez la signature dans le format suivant : <CAT|QID|ANY>:<value>:<source IP>:<dest IP> Où : <CAT|QID|ANY> - Indiquez si vous souhaitez que cette signature de faux positif prenne en considération une catégorie (CAT), IBM Identificateur (QID) ou une autre valeur. <value> - Indiquez la valeur du paramètre <CAT|QID|ANY>. Par exemple, si vous indiquez QID, vous devez indiquer la valeur QID. <source IP> - Indiquez l'adresse IP source que cette signature de faux positif que vous souhaitez que ce test prenne en considération . <dest IP> - Indiquez l'adresse IP de destination que cette signature de faux positif que vous souhaitez que ce test prenne en considération.

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Default Test Name	Parameters
Regex	Valide lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé à une chaîne particulière d'expressions régulières (regex). ***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.*	lorsque le nom d'utilisateur (**username**) correspond à l'expression régulière suivante (**regex)**	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.
IPv6	Valide 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 : • **source IP(v6) | destination IP(v6)** - Indiquez si vous souhaitez que ce test prenne en considération l'adresse IPv6 source ou de destination. • **IP(v6) addresses** - Indiquez les adresses IPv6 que vous souhaitez que ce test prenne en considération.
Reference Set	Valide lorsque l'une ou toutes les propriétés d'événements sont comprises dans l'un ou dans 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 : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération **une** ou **toutes** les propriétés d'événement configurées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération.

Tableau A-3 Règle d'événement : Tests de propriété d'événement (suite)

Test	Description	Default Test Name	Parameters
Reference Map	Valide lorsqu'aucune ou toutes les propriétés d'événement dans une paire de valeur/clé sont contenues dans aucune ou dans toutes les cartes de référence configurées.	lorsqu'**aucune** de **ces propriétés d'événement** ne représente la clé et qu'**aucune** de **ces propriétés d'événement** ne représente la valeur dans **n'importe** laquellede **ces cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération **une** ou **toutes** les propriétés d'événement configuré. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération • **these reference maps** - Indiquez les cartes de référence que vous souhaitez que ce test prenne en considération.
Reference Map of Sets	Valide lorsqu'aucune de toutes ces propriétés d'événement dans une paire de valeur/clé configurée ne sont contenues dans aucun ou dans tous les ensembles de cartes de référence configurées.	lorsqu'**aucune** de **ces propriétés d'événement** ne représente la clé et qu'**aucune** de **ces propriétés d'événement** ne représente la valeur dans **n'importe** lequel de **ces ensembles de cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération **une** ou **toutes** les propriétés d'événement configuré. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération • **these reference map of sets** - Indiquez les ensembles de cartes de référence que vous souhaitez que ce test prenne en considération.
Reference Map of Maps	Valide lorsqu'aucune ou toutes les propriétés d'événement dans une paire configurée de valeur/clé primaire et secondaire ne sont contenues dans aucune ou dans toutes les cartes configurées de carte de référence.	lorsqu'**aucune** de **ces propriétés d'événement** ne représente la clé de la première carte et qu'**aucune** de **ces propriétés d'événement** ne représente la clé de la seconde carte et qu'**aucune** de **ces propriétés** ne représente la valeur dans aucune des méthodes d'analyse des pannes de **ces cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération **une** ou **toutes** les propriétés d'événement configuré. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération • **these reference map of maps** - Indiquez la carte de référence des cartes que vous souhaitez que ce test prenne en considération.
Search Filter	Valide 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 vous souhaitez que ce test prenne en considération.

Tests de propriété communs Le groupe de test de propriété commune comprend :

Tableau A-4 Règle d'événement : Tests de propriété commune

Test	Description	Default Test Name	Parameters
CVSS Risk (Host)	Valide lorsque l'hôte spécifié possède une valeur de risque CVSS correspondant à la valeur configurée.	lorsque l'hôte de **destination** possède une valeur de risque CVSS **supérieure à cette valeur**	Configurez les paramètres suivants : • **source | destination | either** - Indiquez si le test prend en considération 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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.
CVSS Risk (Port)	Valide lorsque le port spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque le port de **destination** comprend une valeur de risque CVSS supérieure à cette **valeur**	• **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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.
Custom Rule Engines	Valide lorsque l'événement est traité par des moteurs spécifiés de règle personnalisée.	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 vous souhaitez que ce test prenne en considération.

Tableau A-4 Règle d'événement : Tests de propriété commune (suite)

Test	Description	Default Test Name	Parameters
Regex	Valide lorsque la propriété configurée est associée à une chaîne d'expressions régulières (regex). ***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 d'expression régulière disponibles sur le Web.*	lorsque l'une de ces propriétés (**these properties**) correspond à l'expression régulière **suivante**	Configurez les paramètres suivants : • **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 chaîne d'expression régulière que vous souhaitez ce test doit prenne en considération.
Hexadecimal	Valide lorsque la propriété configurée est associée à des valeurs hexadécimales particulières.	lorsque l'une de **ces propriétés** comprend l'une de ces valeurs hexadécimales	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.

Tests de 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	Valide 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	Valide 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	Valide 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 vous souhaitez que ce test prenne en considération.
Log Source Groups	Valide 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.

Fonction - tests de séquence 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, dans|dans n'importe quel**ordre, à partir **la même|aucune adresse IP source** vers **la même|aucune adresse IP de destination,** en **quelques secondes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 prenne en considération **certaines** ou **n'importe quelle** source confugurée. • **username | source IP | source port | destination IP | destination port | QID | event ID | log source | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source destination. • **destination IP | username | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 de destination (**the same|any destination IP**), sur ce nombre de secondes (**this many seconds)**	Configurez les paramètres suivants : • **this number** - Indiquez le nombre de règles que vous souhaitez que cette fonction prenneen considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 prenne en considération **certaines** ou **n'importe quelle** source confugurée. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source destination. • **destination IP | username | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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**ce many seconds**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalle que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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)**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de règles que vous souhaitez que ce test prenne en considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **in | in any** - Indiquez si vous souhaitez que ce test prenne en considération les règles dans un ordre spécifique. • **username | source IP | source port | destination IP | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **in | in any** - Indiquez si vous souhaitez que ce test prenne en considération les règles dans un ordre spécifique. • **to | from** - Indiquez la direction que vous souhaitez que ce test prenne en considération. • **username | source IP | source port | destination IP | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 diddérentes 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	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 séries 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**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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 (**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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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)**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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 : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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)**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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 : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Fonction - tests du compteur Les tests de la fonction - 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**	Configurez les paramètres suivants : • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **more than | exactly** - Indiquez si vous souhaitez que ce test prenne en considération exactement le nombre de règle ou plus. • **this many** - Indiquez le nombre de règles que vous souhaitez que ce test prenne en considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **more than | exactly** - Indiquez si vous souhaitez que ce test prenne en considération 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 préxédente. • **this many** - Indiquez le nombre d'adresse IP, de ports, de QID, d'événements, de source de journal ou des catégories que vous souhaitez que ce test prenne en considération. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que vous souhaitez que ce test prenne 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 séries 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)**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Indiquez la source que vous souhaitez que ce test prenne 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 prenne en considération 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 préxédente. • **this many** - Indiquez le nombre que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne 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 : • **MAC | username | hostname** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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	1Allows you to detect a series of events with the same event properties and different event properties within the configured time interval. 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.	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)**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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)**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 diddérentes propriétés d'événement au sein de l'intervalle de temps configuré.	Lorsque **ces règles** correspondent au moins autant de fois aux mêmes propriétés et aux propriétés d'événement **en quelquesminutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**.

Fonction - tests simples Fonction - tests simples :

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 suivates	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.

Tests de la date/heure 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 : • **on | after | before** - Indiquez si vous souhaitez que ce test prenne en considération avant, après ou à la date configurée. La valeur par défaut est **on IP**. • **selected** - Indiquez le jour du mois que vous souhaitez que ce test prenne en considération.
Event Week	Valide 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 vous souhaitez que ce test prenne en considération .
Event Time	Valide 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 : • **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 vous souhaitez que ce test prenne en considération.

Tests de propriété du réseau Le test de la propriété du réseau comprend :

Tableau A-10 Règle d'événement : Tests de propriété de réseau

Test	Description	Default Test Name	Parameters
Local Networks	Valide lorsque l'événement se produit dans le réseau spécifié.	lorsque le réseau local est **l'un des réseaux réseaux suivants**	**one of the following networks** - Indiquez les zones du réseau dans lesquelles vous souhaitez que ce test s'applique.
Remote Networks	Valide lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux distants configurés.	lorsque **l'adresse IP** fait partie de l'un des emplacements de réseaux distants **suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • **remote network locations** - Indiquez les emplacements réseau que souhaitez que ce test prenne en considération.
Remote Services Networks	Valide lorsque l'adresse IP fait partie de l'un ou de tous les emplacements réseaux de services distants configurés.	lorsque **l'adresse IP** fait partie de l'un des emplacements **réseau de services distants suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • **remote services network locations** - Indiquez les emplacements réseau de services que vous souhaitez que ce test prenne en considération.
Geographic Networks	Valide lorsque l'adresse IP fait partie de l'un ou de tous les emplacements réseau géographiques configurés.	lorsqu'une adresse **Source IP** fait partie de l'un des emplacements réseau géographiques suivants	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • **geographic network locations** - Indiquez les emplacements réseau que vous souhaitez que ce test prenne 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 ne 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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 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**) correpondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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**
- **tests d'adresse IP/Port**
- **Tests de propriété**
- **Tests de propriétés communes**
- **Tests de fonction - séquence**
- **Tests de fonction - compteurs**
- **Tests de fonction - simples**
- **Tests de date/heure**
- **Tests de propriété du réseau**
- **Tests de fonction - négatifs**

Tests de profil d'hôte

Les tests 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	Valide 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 : • **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 **activement ou passivement seen**	Configurez les paramètres suivants : • **source | destination** - indiquez si vous souhaitez que ce test s'applique au port 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 prenne en considération 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	Valide lorsque l'hôte source ou de destination est connu pour sa présence via l'analyse active ou passive. Vous pouvez également spécifier si le statut du host est détecté en utilisant l'une des méthodes suivantes : • **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**	Configurez les paramètres suivants : • **source | destination** - indiquez si vous souhaitez que ce test s'applique au port 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 prenne en considération 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	Valide 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 : • **source | destination** - Indiquez si vous souhaitez que ce test s'applique l'hôte source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test prenne en considération les valeurs supérieures ou inférieures à l'âge d'hôte de du profil. • **this number of** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne 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	Valide lorsque l'âge du profil du port source ou de destination est supérieure ou inférieur 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 : • **source | destination** - indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **time intervals** - Indiquez si ce test doit prendre en considération les minutes ou les heures.
Asset Weight	Valide lorsque l'unité (destination) est attaquée ou l'hôte est l'attaquant (source) a une pondération assignée supérieur ou inférieure à la valeur configurée.	Lorsque l'actif cible (**destination**) a une pondération **supérieur à cette pondération**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération.

Tableau A-12 Règle de flux : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
OSVDB IDs	Valide 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 : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. Pour plus d'informations concernant les ID de OSVDB, consultez *http://osvdb.org/*.

tests d'adresse IP/Port Les tests d'adresse IP/Port comprennent :

Tableau A-13 Flow Rules: IP / Port Test Group

Test	Description	Nom du test par défaut	Paramètres
Source Port	Valide 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 vous souhaitez que ce test prenne en considération.
Destination Port	Valide 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 vous souhaitez que ce test prenne en considération.
Local Port	Valide 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 vous souhaitez que ce test prenne en considération.
Remote Port	Valide lorsque le port distant du flux est l'un des ports distants configurés.	lorsque le port distant représente l'un des ports suivants	**ports** - Indiquez les ports que vous souhaitez que ce test prenne en considération.
Adresse IP source	Valide 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 vous souhaitez que ce test prenne en considération.
Destination IP Address	Valide lorsque l'adresse IP de destination du flux est l'une des adresses IP configurées.	lorsque l'IP de destination fait partie des adresses IP suivantes	**IP addresses** - Indiquez les adresses IP que vous souhaitez que ce test prenne en considération.
Local IP Address	Valide 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 vous souhaitez que ce test prenne en considération.

Tableau A-13 Flow Rules: IP / Port Test Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote IP Address	Valide 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 vous souhaitez que ce test prenne en considération.
IP Address	Valide 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 vous souhaitez que ce test prenne en considération.
Source or Destination Port	Valide 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 vous souhaitez que ce test prenne en considération.

Tests de propriété 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	Valide 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 à ce test.
Flow Context	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. Valide si le contexte d'événement est l'une des options suivantes : • Local to Local • Local to Remote • Remote to Local • Remote to Remote	Lorsque le contexte du flux est **this context**	**this context** - Indiquez le contexte que vous souhaitez que ce test prenne en considération. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Valide 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	Valide 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**.
Geographic Location	Valide lorsque l'adresse IP correspond à l'emplacement géographique configurée.	lorsque la source est localisée dans cette région **géographique**	**geographic location** - Sélectionnez un emplacement géographique.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	Valide lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé à une chaîne particulière d'expressions régulières (regex). ***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.*	lorsque le nom d'utilisateur (**username**) correspond à l'expression régulière suivante (**regex)**	Configurez les paramètres suivants : • **hostname | source hostname |destination hostname | source payload | destination payload** - Indiquez tla valeur que vous souhaitez associer avec ce test. La valeur par défaut est **username**. • **regex** - Indiquez la ligne de l'expression régulière que vous souhaitez que ce test prenne en considération.
IPv6	Valide 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 : • **source IP(v6) | destination IP(v6)** - Indiquez si vous souhaitez que ce test prenne en considération l'adresse IPv6 source ou de destination. • **IP(v6) addresses** - Indiquez les adresses IPv6 que vous souhaitez que ce test prenne en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Set	Valide 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 : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération **une** ou **toutes** les propriétés d'événement configuré. • **these flow properties** - Indiquez les propriétés du flux que vous souhaitez que ce test prenne en considération • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération l'un(**any**) ou tous (**all**)les ensembles de référence configurés. • **these reference set(s)** - Indiquez les ensembles de référence que vous souhaitez que ce test prenne en considération.
Reference Map	Valide lorsqu'aucune ou toutes les propriétés de flux dans une paire de valeur/clé sont contenues dans aucune ou dans toutes les cartes de référence configurées.	lorsqu**aucune** de **ces propriétés deflux** ne représentent la clé et qu'**aucune** de **ces propriétés deflux** ne représente la valeur dans **aucune** de **ces cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test ne prenne en considération **aucune** ou **toutes les** propriétés de flux configurées. • **these flow properties** - Indiquez les propriétés du flux que vous souhaitez que ce test prenne en considération • **these reference maps** - Indiquez les cartes de référence que vous souhaitez que ce test prenne en considération.
Reference Map of Sets	Valide lorsqu'aucune ou toutes les propriétés de flux dans une paire de valeur/clé configuréesont contenues dans aucune ou tous les ensembles de référence configurés.	lorsqu'**aucune** de **ces propriétés de flux** ne représente la clé et qu'**aucune** de **ces propriétés de flux** ne représente la valeur dans **aucune** de **ces ensembles de cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test ne prenne en considération **aucune** ou **toutes les** propriétés de flux configurées. • **these flow properties** - Indiquez les propriétés du flux que vous souhaitez que ce test prenne en considératio. • **these reference map of sets** - Indiquez les ensembles de cartes de référence que vous souhaitez que ce test prenne en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Map of Maps	Valide lorsqu'aucune ou toutes les propriétés de flux dans une paire configurée de valeur/clé primaire et secondaire ne sont contenues dans aucune ou dans toutes les ensembles de cartes de référence configurés.	lorsqu'**aucune** de **ces propriétés de flux** ne représente la clé de la première carte et qu'**aucune** de **ces propriétés de flux** ne représente la clé de la seconde carte et qu'**aucune** de **ces propriétés de flux** ne représente la valeur dans aucune de ces ensembles de cartes de référence	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test ne prenne en considération **aucune** ou **toutes les** propriétés de flux configurées. • **these flow properties** - Indiquez les propriétés du flux que vous souhaitez que ce test prenne en considération • **these reference map of maps** - Indiquez la carte de référence des cartes que vous souhaitez que ce test prenne en considération.
Flow Bias	Valide 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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **inbound IP**.
Byte / Packet Count	Valide lorsque le nombre d'octets ou de paquets correspond au montant configuré.	Lorsque les **octets de la source** sont **supérieurs à ce montant**	Configurez les paramètres suivants : • **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 les nombre d'octets ou de paquets est supérieure, inférieure ou égal à la valeur configurée. • **0** - Indiquez la valeur que vous souhaitez que ce test prenne 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
Host Count	Valide lorsque le nombre des hôtes correspondent au montant configuré.	Lorsque le numéro des hôtes **source** est **supérieur à ce montant**.	Configurez les paramètres suivants : • **source | destination | local | remote** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.
Packet Rate	Valide 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 : • **source | destination | local | remote** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.
Flow Duration	Valide 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 : • **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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
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 inclue 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 : • testsource | destination | local | remote - Indiquez si vous souhaitez que ce critère prenne en considération 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 **regex**. • **string** - Indiquez la ligne du texte que vous souhaitez inclure dans le test.
Flow Source Name	Valide 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 vous souhaitez que ce test prenne en considération.
Flow Interface	Valide 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 vous souhaitez que ce test prenne en considération.
Flow Type	Valide 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 vous souhaitez que ce test prenne en considération.
Byte/Packet Ratio	Valide 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 : • source | destination | local | remote - Indiquez si vous souhaitez que ce critère prenne en considération 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 vous souhaitez que ce test prenne en considération.
ICMP Type	Valide 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 vous souhaitez que ce test prenne en considération.
ICMP Code	Valide 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 vous souhaitez que ce test prenne en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
DSCP	Valide 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 : • source | destination | local | remote | either - Indiquez si vous souhaitez que ce test prenne en considération soit le DSCP source, destination, local, ou distant. La valeur par défaut est **destination IP**. • **these values** - Indiquez les valeurs DSCP que vous souhaitez que ce test prenne en considération.
IP Precedence	Valide lorsque la priorité IP correspond aux valeurs configurées	lorsque la priorité IP **destination** est l'une de **these values**	Configurez les paramètres suivants : • source | destination | local | remote | either - Indiquez si vous souhaitez que ce test prenne en considération soit le DSCP source, destination, local, ou distant. La valeur par défaut est **destination IP**. • **these values** - Indiquez les valeurs de priorité IP que vous souhaitez que ce test prenne en considération.
Packet Ratio	Valide lorsque le raton du paquet configuré correspond à la valeur configurée. Ce test vous permet de spécifier les valeurs dans le rapport du paquet.	lorsque le rapport de paquet **source**/**destination** est **supérieure à cette valeur**	Configurez les paramètres suivants : • source | destination | local | remote - Spécifiez la direction que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
TCP Flags	Valide lorsque les indicateurs TCP correspondent aux valeurs configurées.	lorsque les indicateurs TCP **destination sont exactement these flags**	Configurez les paramètres suivants : • source | destination | local | remote - Indiquez si vous souhaitez que ce critère prenne en considération 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 prenne en considération exactement soit tous ou aucun des indicateurs TCP configurés. La valeur par défaut **are exactly**. • **these flags** - Indiquez les indicateurs TCP que vous souhaitez que ce test prenne en considération.
IF Index	Valide lorsque IF Index correspond aux valeurs configurées	lorsque la liste des indexes (interface) IF **input** comprend **all** de **these values**	Configurez les paramètres suivants : • **input | output | either** - Indiquez la direction que vous souhaitez que ce test prenne en considération. La valeur par défaut **input**. • **all | any** - Indiquez si vous souhaitez que ce test prenne en considération tout ou n'importe quelle valeur IF Index configurée.. • **these values** - Indiquez les indexes IF que vous souhaitez que ce test prenne en considération.
TCP Flag Combination	Valide 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 : • source | destination | local | remote - Indiquez si vous souhaitez que ce critère prenne en considération 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 vous souhaitez que ce test prenne en considération. Indicateurs séparés par des virgules.

Tableau A-14 Règles de flux : Flow Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Search Filter	Valide 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 vous souhaitez que ce test prenne en considération.
Flow Payload	Valide 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 : • **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 prenne en considération les flux qui ont ou n'ont pas de contenu.

Tests de propriétés communes 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)	Valide 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 : • **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 soit supérieure, inférieure ou égale à la valeur configurée. • **0** - Indiquez la valeur que vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.

Tableau A-15 Règles de flux : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
CVSS Risk (Port)	Valide lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	Lorsque le port de **destination** comprend une valeur de risque CVSS supérieure à cette **valeur**	• **source | destination | either** - Indiquez si le test prend en considération le port source ou de destination du fluxt. • **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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.
Custom Rule Engine	Valide 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 vous souhaitez que ce test prenne en considération.
Regex	Valide lorsque la propriété configurée est associée à une chaîne d'expressions régulières (regex). ***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.*	lorsque ces propriétés (**these properties**) correspondent à l'expression régulière suivante	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.

Tableau A-15 Règles de flux : Tests de propriété commune (suite)

Test	Description	Nom du test par défaut	Paramètres
Hexadecimal	Valide lorsque la propriété configurée est associée à des valeurs hexadécimales particulières.	lorsque l'une de ces propriétés (**these properties**) comprend l'une de ces valeurs hexadécimales (**these hexadecimal values)**	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.

Tests de fonction - séquence La fonction : les tests de séquence comprennent :

Tableau A-16 Flow Rules: Functions Sequence Group

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 de règles sélectionnées exigeant une source et une destination en une période de temps configurée.	lorsque toutes ces **règles, dans|dans n'importe quel**ordre, issues de **la même|aucune adresse IP source** vers **la même|aucune adresse IP de destination,** en **quelques secondes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **in | in any** - Indiquez si vous souhaitez que ce test prenne en considération **dans un ordre particulier** ou **ou autrement**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source configurée. • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source destination. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **seconds**.

Tableau A-16 Flow Rules: Functions Sequence Group (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Flow Function	Vous permet d'utiliser les blocs de construction enregistrés ou d'autres règles pour effectuer ce test. Vous pouvez utiliser cette fonction pour détecter un nombre de règles spécifiées, en séquence, exigeant une source ou une destination dans un intervalle de temps configuré.	lorsqu'au moins **ce nombre** de ces **règles, dans cet ordre ou dans n'importe quel** ordre, **à partir de la même|n'importe quelle adresse IP source** vers la même|n'importe quelle adresse IP de destination en un nombre donné de secondes	Configurez les paramètres suivants : • **this number** - Indiquez le nombre de règles que vous souhaitez que cette fonction prenneen considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 prenne en considération **certaines** ou **n'importe quelle** source confugurée. • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source destination. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération.

Tableau A-16 Flow Rules: Functions Sequence Group (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 : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalle que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **seconds**.
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et les diddérentes 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération.

Tableau A-16 Flow Rules: Functions Sequence Group (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	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération.

Tableau A-16 Flow Rules: Functions Sequence Group (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	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération.

Tableau A-16 Flow Rules: Functions 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 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)**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 Flow Rules: Functions Sequence Group (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 : • **these** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these** - Indiquez les règles que vous souhaitez que ce test prenne 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 Flow Rules: Functions Sequence Group (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)**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 Flow Rules: Functions Sequence Group (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 : • **this many** - Indiquez le nombre de flux que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération.

Tableau A-16 Flow Rules: Functions Sequence Group (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)**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 Flow Rules: Functions Sequence Group (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 : • **this many** - Indiquez le nombre de flux que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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.

Tests de fonction - compteurs 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**	Configurez les paramètres suivants : • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **more than | exactly** - Indiquez si vous souhaitez que ce test prenne en considération exactement le nombre de règle ou plus. • **this many** - Indiquez le nombre de règles que vous souhaitez que ce test prenne en considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **more than | exactly** - Indiquez si vous souhaitez que ce test prenne en considération 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 préxédente. • **this many** - Indiquez le nombre d'adresses IP, ports ou noms d'utilisateur que vous souhaitez que ce test prenne en considération. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que vous souhaitez que ce test prenne 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 séries 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'aucune de ces **règles** avec la même adresse **IP source** à plusieurs **reprises** , à travers **le plus souvent| exactement cette adresse IP de destination** en **quelques minutes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne 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 prenne en considération 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 préxédente. • **this many** - Indiquez le nombre que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne 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	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 pour détecter lorsque 100 événements avec la même adresse IP source se produisent dans 5 minutes.	Lorsque au moins autant d'événements (**this many** flows) sont affichés avec les mêmes propriétés (**flow properties**) dans autant de minutes (**this many minutes)**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**.
Flow Property Function	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. 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.	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)**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 diddérentes 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**.

Tests de fonction - simples Les tests de fonction - simples comprennent :

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 : • **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 vous souhaitez que ce test prenne en considération.

Tests de date/heure 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	Valide 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 : • **on | after | before** - Indiquez si vous souhaitez que ce test prenne en considération avant, après ou à la date configurée. La valeur par défaut est **on IP**. • **selected** - Indiquez le jour du mois que vous souhaitez que ce test prenne en considération.
Flow Week	Valide 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 vous souhaitez que ce test prenne en considération .
Flow Time	Valide 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 : • **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 vous souhaitez que ce test prenne en considération.

Tests de propriété du 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	Valide 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 du réseau sur lesquelles vous souhaitez que ce test s'applique.

Tableau A-20 Règles de flux : Network Property Tests (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Networks	Valide 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 : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 prenne en considération.
Remote Services Networks	Valide 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 des emplacements **réseau de services**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 réseau de services que vous souhaitez que ce test prenne en considération.
Geographic Networks	Valide 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 : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 réseau géographiques que vous souhaitez que ce test prenne en considération.

Tests de fonction - négatifs Les tests de fonction - 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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**) correpondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération.

Tests de règles 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 d'adresse IP/Port**
- **Tests de propriété commune**
- **Tests de fonctions - séquence**
- **Tests de fonction - compteur**
- **Tests de fonction - simples**
- **Tests sur la date/heure**
- **Tests sur la propriété du réseau**
- **Tests de fonction négative**

Tests de profil d'hôte Les tests du profil d'hôte comprennent :

Tableau A-22 Common Rule: Host Profile Tests

Test	Description	Default Test Name	Parameters
Host Profile Port	Valide lorsque le port est ouvert sur une source ou une destination locale configurée. Vous pouvez également indiquer si le statut du port est détecté via l'utilisation de l'une des méthodes suivantes : • **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 **soit activement ou passivement affiché**	Configurez les paramètres suivants : • **source | destination** - indiquez si vous souhaitez que ce test s'applique au port 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 prenne en considération l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.
Host Existence	Valide lorsque l'hôte source ou de destination est connu pour sa présence via l'analyse active ou passive. Vous pouvez également spécifier si le statut du host est détecté en utilisant l'une des méthodes suivantes : • **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**	Configurez les paramètres suivants : • **source | destination** - indiquez si vous souhaitez que ce test s'applique au port 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 prenne en considération l'analyse actif ou passif ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.

Tableau A-22 Common Rule: Host Profile Tests (suite)

Test	Description	Default Test Name	Parameters
Age de profil d'hôte	Valide 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 : • **source | destination** - Indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test prenne en considération les valeurs supérieures ou inférieures à l'âge du port du profile. • **this number of** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **time intervals** - Indiquez si vous souhaitez que ce test prenne en considération les minutes ou les heures.
Host Port Age	Valide lorsque l'âge du profil du port d'hôte source ou de destination est supérieur ou inférieur au temps configuré.	lorsque l'âge du port de profil de l'hôte **source** est supérieur à ce nombre d'intervalles de temps	Configurez les paramètres suivants : • **source | destination** - indiquez si vous souhaitez que ce test s'applique au port source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **time intervals** - Indiquez si vous souhaitez que ce test doit prenne en considération les minutes ou les heures.

Tableau A-22 Common Rule: Host Profile Tests (suite)

Test	Description	Default Test Name	Parameters
Asset Weight	Valide lorsque l'unité (de destination) est attaquée ou l'hôte est l'attaquant (source) contient une pondération assignée supérieure ou inférieure à la valeur configurée.	Lorsque l'actif **de destination** a une pondération **supérieur à cette pondération**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération.
OSVDB IDs	Valide 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 : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. Pour plus d'informations concernant les ID de OSVDB, consultez *http://osvdb.org/*.

Tests d'adresse IP/Port Les tests d'adresse IP/Port comprennent :

Tableau A-23 Règle commune : IP / Groupe de test du port

Test	Description	Nom du test par défaut	Paramètres
Source Port	Valide 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 vous souhaitez que ce test prenne en considération.
Destination Port	Valide 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 vous souhaitez que ce test prenne en considération.

Tableau A-23 Règle commune : IP / Groupe de test du port (suite)

Test	Description	Nom du test par défaut	Paramètres
Local Port	Valide 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 vous souhaitez que ce test prenne en considération.
Remote Port	Valide lorsque le port cible de l'événement ou du flux fait partie des ports distants configurés.	lorsque le port distant représente l'un des ports suivants	**ports** - Indiquez les ports que vous souhaitez que ce test prenne en considération.
Adresse IP source	Valide 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 vous souhaitez que ce test prenne en considération.
Destination IP Address	Valide lorsque l'adresse IP de destination de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'IP de destination fait partie des adresses IP suivantes	**IP addresses** - Indiquez les adresses IP que vous souhaitez que ce test prenne en considération.
Local IP Address	Valide 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 vous souhaitez que ce test prenne en considération.
Remote IP Address	Valide 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 vous souhaitez que ce test prenne en considération.
IP Address	Valide 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 vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération.

Tests de propriété commune Les tests de propriété commune comprennent :

Tableau A-24 Common Rules: Common Property Tests

Test	Description	Default Test Name	Parameters
IP Protocol	Valide 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 à ce test.

Tableau A-24 Common Rules: Common Property Tests (suite)

Test	Description	Default Test Name	Parameters
Payload Search	Ce test est valide lorsque la ligne de recherche entrée est inclue n'importe où dans le contenu source ou de destination de l'événement ou du flux.	lorsque Flow Source ou Destination Payload contient cette ligne (**this string)**	**this string** - Indiquez la chaîne que vous souhaitez inclure pour ce test.
Context	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. Valide si le contexte représente l'une des options suivantes : • Local to Local • Local to Remote • Remote to Local • Remote to Remote	lorsque le contexte est ce contexte **f**	**this context** - Indiquez le contexte que vous souhaitez que ce test prenne en considération. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Valide 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	Valide lorsque l'adresse IP de destination 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.
Geographic Location	Valide lorsque l'adresse IP correspond à l'emplacement géographique configurée.	lorsque la source est localisée dans cette région **géographique**	**geographic location** - Sélectionnez un emplacement géographique.

Tableau A-24 Common Rules: Common Property Tests (suite)

Test	Description	Default Test Name	Parameters
Regex	Valide lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé à une chaîne particulière d'expressions régulières (regex). ***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.*	lorsque le nom d'utilisateur (**username**) correspond à l'expression régulière suivante (**regex)**	Configurez les paramètres suivants : • **hostname | source hostname |destination hostname | source payload | destination payload** - Indiquez tla valeur que vous souhaitez associer avec ce test. La valeur par défaut est **username**. • **regex** - Indiquez la ligne de l'expression régulière que vous souhaitez que ce test prenne en considération.
IPv6	Valide 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 : • **source IP(v6) | destination IP(v6)** - Indiquez si vous souhaitez que ce test prenne en considération l'adresse IPv6 source ou de destination. • **IP(v6) addresses** - Indiquez les adresses IPv6 que vous souhaitez que ce test prenne en considération.

Tableau A-24 Common Rules: Common Property Tests (suite)

Test	Description	Default Test Name	Parameters
Reference Set	Valide 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 : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération **une** ou **toutes** les propriétés d'événement configuré. • **these properties** - Indiquez les propriétés d'événement ou de flux que vous souhaitez que ce test prenne en considération. • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération l'un(**any**) ou tous (**all**)les ensembles de référence configurés. • **these reference set(s)** - Indiquez les ensembles de référence que vous souhaitez que ce test prenne en considération.
Reference Map	Valide lorsqu'aucune ou toutes les propriétés d'événement dans une paire configurée de valeur/clé ne sont contenues dans aucun ou dans toutes les cartes de référence configurées.	lorsqu'**aucune** de **ces propriétés deflux** ne représente la clé et qu'**aucune** de **ces propriétés deflux** ne représente la valeur dans **aucune** de **ces cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test ne prenne en considération **aucune** ou **toutes** les propriétés configurées d'événement et de flux communes. • **these properties** - Indiquez les propriétés d'événement et de flux communes que vous souhaitez que ce test prenne en considération. • **these reference maps** - Indiquez les cartes de référence que vous souhaitez que ce test prenne en considération.

Tableau A-24 Common Rules: Common Property Tests (suite)

Test	Description	Default Test Name	Parameters
Reference Map of Sets	Valide lorsqu'aucune ou toutes les propriétés d'événement ou de flux dans une paire configurée de valeur/clé ne sont contenues dans aucun ou tous les ensembles configurés de cartes de référence.	lorsqu'aucune de **ces propriétés** ne représente la clé et qu'**aucune** de **ces propriétés** ne représente la valeur dans **aucun** de **ces ensembles de cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test ne prenne en considération **aucune** ou **toutes** les propriétés configurées d'événement et de flux communes. • **these properties** - Indiquez les propriétés d'événement et de flux communes que vous souhaitez que ce test prenne en considération. • **these reference map of sets** - Indiquez les ensembles de cartes de référence que vous souhaitez que ce test prenne en considération.
Reference Map of Maps	Valide lorsqu'aucune ou toutes les propriétés de flux dans une paire configurée de valeur/clé principales et secondaires sont contenues dans aucun ou toutes les ensembles configurés de cartes de référence.	lorsqu'**aucune** de **ces propriétés** ne représente la clé de la première carte et qu'**aucune** de **ces propriétés** représente la clé de la seconde carte et **qu'aucune** de **ces propriétés** ne représente la valeur dans aucun de **ces ensembles de cartes de référence**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test ne prenne en considération **aucune** ou **toutes** les propriétés configurées d'événement et de flux communes. • **these properties** - Indiquez les propriétés d'événement et de flux communes que vous souhaitez que ce test prenne en considération. • **these reference map of maps** - Indiquez la carte de référence des cartes que vous souhaitez que ce test prenne en considération.

Tableau A-24 Common Rules: Common Property Tests (suite)

Test	Description	Default Test Name	Parameters
CVSS Risk (Host)	Valide 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 : • **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 soit supérieure, inférieure ou égale à la valeur configurée. • **0** - Indiquez la valeur que vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.
CVSS Risk (Port)	Valide lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	Lorsque le port de **destination** comprend une valeur de risque CVSS supérieure à cette **valeur**	• **source | destination | either** - Indiquez si le test prend en considération le port source ou de destination du fluxt. • **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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **0**.
Search Filter	Valide 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 vous souhaitez que ce test prenne en considération.

Tableau A-24 Common Rules: Common Property Tests (suite)

Test	Description	Default Test Name	Parameters
Regex	Valide lorsque la propriété configurée est associée à une chaîne d'expressions régulières (regex). ***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.*	lorsque ces propriétés (**these properties**) correspondent à l'expression régulière suivante	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.
Custom Rule Engines	Valide 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 vous souhaitez que ce test prenne en considération.
Hexadecimal	Valide lorsque la propriété configurée est associée à des valeurs hexadécimales particulières.	lorsque l'une de ces propriétés (**these properties**) comprend l'une de ces valeurs hexadécimales (**these hexadecimal values)**	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.

Tests de fonctions - séquence Les tests de fonctions - 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, dans|dans n'importe quel**ordre, à partir **la même|aucune adresse IP source** vers **la même|aucune adresse IP de destination,** en **quelques secondes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 prenne en considération **certaines** ou **n'importe quelle** source confugurée. • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source destination. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 : • **this number** - Indiquez le nombre de règles que vous souhaitez que cette fonction prenne en considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **in | in any** - Indiquez si ce test doit prendre en considération **dans un ordre particulier** ou **dans n'importe quel** ordre. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source configurée. • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **certaines** ou **n'importe quelle** source destination. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test prenne en considération 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 en **un nombre donné de secondes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **seconds**.
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et différentes propriétés d'événement dans l'intervalle de temps configuré.	Lorsque **ces règles** correspondent au moins parfois à dans un nombre donné de **minutes** une fois que ces règles correspondent.	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre de fois auquel les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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** correspondent au moins parfois **à** aux mêmes **propriétés d'événement** en un nombre **donné de minutes une fois que ces règles correspondent**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre de fois auquel les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 produisant à plusieurs reprises la configuration avec les mêmes et les différentes propriétés d'événement s'effectuant dans un intervalle de temps configuré après une série de règles spécifiques.	Lorsque ces règles correspondent au moins parfois aux mêmes propriétés d'événement et aux propriétés d'événement différentes en un nombre donné de minutes après que ces règles correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre de fois auquel les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 produisant à plusieurs reprises la configuration dans un intervalle de temps configuré après l'exécution d'une séries de règles spécifiques avec les mêmes propriétés d'événement.	Lorsque ces règles correspondent au moins parfois en un nombre donné de minutes une fois que ces règles correspondent aux mêmes propriétés d'événement	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre de fois auquel les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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** correspondent parfois aux mêmes propriétés d'événement en un nombre donné de minutes une fois que ces règles correspondent aux mêmes propriétés d'événement	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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** correspondent au moins parfois aux mêmes propriétés d'événement et aux propriétés d'événement différentes en **un nombre donné de minutes** après que **ces règles** correspondent aux mêmes propriétés d'événement	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre de fois pendant lequel les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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 .	lorsque parfois un nombre donné d'événements s'affiche avec les mêmes propriétés d'événement et des propriétés d'événement différentes en nombre calculé de minutes une fois que ces règles correspondent	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération. Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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.	lorsque moins un nombre donné d'événements s'affiche avec les mêmes propriétés d'événement dans un nombre calculé de minutes une fois que ces règles correspondent avec les mêmes propriétés d'événement	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne 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.	Lorsque parfois un nombre donné d'événements s'affiche au moins avec les mêmes propriétés d'événement et des propriétés d'événement différentes autant de fois que ces règles correspondent avec les mêmes propriétés d'événement	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées.

Tests de fonction - compteur Les tests de la fonction - du 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**	Configurez les paramètres suivants : • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne en considération. La valeur par défaut est **source IP**. • **more than | exactly** - Indiquez si vous souhaitez que ce test prenne en considération exactement le nombre de règle ou plus. • **this many** - Indiquez le nombre de règles que vous souhaitez que ce test prenne en considération. • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **more than | exactly** - Indiquez si vous souhaitez que ce test prenne en considération 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 préxédente. • **this many** - Indiquez le nombre d'adresse IP, de ports, de QID, d'événements, de source de journal ou des catégories que vous souhaitez que ce test prenne en considération. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que vous souhaitez que ce test prenne 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 séries 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'aucune de ces **règles** avec la même adresse **IP source** à plusieurs **reprises** , à travers **le plus souvent| exactement cette adresse IP de destination** en **quelques minutes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **1source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que vous souhaitez que ce test prenne 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 prenne en considération 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 préxédente. • **this many** - Indiquez le nombre que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne 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	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 : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**.
Event Property Function	1Allows you to detect a series of events with the same event properties and different event properties within the configured time interval. 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.	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)**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que vous souhaitez que ce test prenne en considération. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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 : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne 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** correspondent au moins plusieurs fois aux mêmes propriétés d'événement et aux propriétés **d'événement différentes** en quelques **minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événement que vous souhaitez que ce test prenne en considération Les options comprennent toutes les propriétés d'événement normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**.

Tests de fonction - simples Les tests de la fonction - simples :

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 : • **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 vous souhaitez que ce test prenne en considération.

Tests sur la date/heure Les tests sur la date et l'heure comprennent :

Tableau A-28 Règle commune : Tests Date/Heure

Test	Description	Default Test Name	Parameters
Event/Flow Day	Valide lorsque l'événement ou le flux se produit sur les jours du mois configurés.	Lorsque le(s) flux ou le ou les événements se produisent **sur** un jour du mois **sélectionné**	Configurez les paramètres suivants : • **on | after | before** - Indiquez si vous souhaitez que ce test prenne en considération avant, après ou à la date configurée. La valeur par défaut est **on IP**. • **selected** - Indiquez le jour du mois que vous souhaitez que ce test prenne en considération.
Event/Flow Week	Valide 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 vous souhaitez que ce test prenne en considération .
Heure d'Evénement/Flux	Valide 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 : • **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 vous souhaitez que ce test prenne en considération.

Tests sur la propriété du réseau Le test sur 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	Valide 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 du réseau sur lesquelles vous souhaitez que ce test s'applique.

Tableau A-29 Règles commune : Tests de propriété du réseau (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Networks	Valide 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 : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 prenne en considération.
Remote Services Networks	Valide 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 des emplacements **réseau de services**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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	Valide lorsque l'adresse IP fait partie de l'un ou de tous les emplacements des réseaux géographiques configurés.	Lorsqu'une adresse **Source IP** fait partie de l'un des emplacements réseau géographiques suivants	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test prenne en considération 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 prenne en considération.

Tests de fonction négative 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.	lorsque toutes ces **règles** correspondent au nombre calculé de **minutes** une fois que **celles-ci** correspondent aux mêmes propriétés de flux	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **flow properties** - Indiquez les propriétés de flux que vous souhaitez que ce test prenne en considération. 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**) correpondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne en considération. • **this many** - Indiquez le nombre d'intervalles que vous souhaitez que ce test prenne en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que vous souhaitez que ce test prenne 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 d'adresse IP/Port**
- **Tests de fonction**
- **Tests sur la date/heure**
- **Tests de source du journal**
- **Tests de propriété de violation**

Tests d'adresse IP/Port

Les tests d'adresse IP/Port comprennent :

Tableau A-31 Règles de violation : Groupe de test IP/Port

Test	Description	Nom du test par défaut	Paramètres
Offense Index	Valide 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 vous souhaitez que ce test prenne en considération. Vous pouvez saisir plusieurs entrées à l'aide d'une liste séparée par des virgules.
Destination IP Address	Valide 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 : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération l'une (**any**) ou toutes (**all**) les destinations listées. La valeur par défaut est **any**. • **IP addresses** - Indiquez les adresses IP que vous souhaitez que ce test prenne en considération. Vous pouvez saisir plusieurs entrées à l'aide d'une liste séparée par des virgules.

Tests 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 : • **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 vous souhaitez que ce test prenne en considération.

Tests sur la date/heure Les tests sur la date et l'heure comprennent :

Tableau A-33 Règles de violation : Tests Date/Heure

Test	Description	Nom du test par défaut	Paramètres
Offense Day	Valide 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 : • **on | after | before** - Indiquez si vous souhaitez que cette règle prenne en considération dans, avant ou après la date sélectionnée. La valeur par défaut est **on IP**. • **selected** - Indiquez la date que vous souhaitez que ce test prenne en considération.
Offense Week	Valide 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 : • **on | after | before** - Indiquez si vous souhaitez que cette règle prenne en considération sur, avant ou après le jour sélectionné. La valeur par défaut est **on IP**. • **these days of the week** - Indiquez les jours que vous souhaitez que ce test prenne en considération.

Tableau A-33 Règles de violation : Tests Date/Heure (suite)

Test	Description	Nom du test par défaut	Paramètres
Offense Time	Valide 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 : • **on | after | before** - Indiquez si vous souhaitez que ce test prenne en considération avant, après ou à l'heure spécifiée. La valeur par défaut est **after IP**. • **this time** - Indiquez l'heure que vous souhaitez que ce test prenne en considération.

Tests de 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	Valide 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 souhaite que ce test détecte.
Number of Log Source Type	Valide 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 : • **greater than | equal to** - Indiquez si vous souhaitez que le niveau de menace devient supérieur ou égal à la valeur configurée. • **this number** - Indiquez le nombre des types de la source du journal que vous souhaitez que ce test prenne 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	Valide 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 : • **any | all** - Indiquez si vous souhaites que ce test prenne en considération l'un (**any**) ou tous (**all**) les réseaux. La valeur par défaut est **any**. • **the following networks** - Indiquez les réseaux que vous souhaitez que ce test prenne en considération.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Offense Category	Valide 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**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test prenne en considération l'une (**any**) ou toutes (**all**) les catégories. La valeur par défaut est **any**. • **list of categories** - Indiquez les catégories que vous souhaites que ce test prenne en considération. Pour plus d'informations sur les catégories d'événements, voir *IBM Security QRadar Network Anomaly Detection Administration Guide*.
Severity	Valide 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})**	Configurez les paramètres suivants : • **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 souhaites que le test prenne en considération. La valeur par défaut est **5**.
Credibility	Valide 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)**	Configurez les paramètres suivants : • **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 souhaites que le test prenne en considération.
Relevance	Valide 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}**	Configurez les paramètres suivants : • **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 souhaites que le test prenne en considération.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Offense Context	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. Valide lorsque le contexte de violation est l'une des options suivantes : • Local to Local • Local to Remote • Remote to Local • Remote to Remote	lorsque le contexte de violation est ce contexte (**this context)**	**this context** - Indiquez le contexte que vous souhaitez que ce test prenne en considération. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Valide 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	Valide 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 devient locale ou distante . La valeur par défaut **remote IPs**.
Destination Count in an Offense	Valide 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)**	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne en considération.
Event Count in an Offense	Valide 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)**	Configurez les paramètres suivants : • **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 vous souhaitez que ce test prenne 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	Valide 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 : • **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 vous souhaitez que ce test prenne en considération.
Total Count in an Offense	Valide 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 : • **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 vous souhaitez que ce test prenne en considération.
Category Count in an Offense	Valide 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 : • **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 vous souhaitez que ce test prenne en considération. Pour plus d'informations sur les catégories d'événements, voir *IBM Security QRadar Network Anomaly Detection Administration Guide*.
Offense ID	Valide 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 vous souhaitez que ce test prenne en considération.
Offense Creation	Valide 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	Valide 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)**	Configurez les paramètres suivants : • **Magnitude | Severity | Credibility | Relevance| Destination count | Source count | Category count | Annotation count | Event count** - Indiquez la propriété que vous souhaitez que ce test prenne 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 prenne en considération le pourcentage ou les unités.

Tests de règle de détection des anomalies

Cette section fournit des informations sur les tests que vous pouvez appliquer aux règles de détection d'anomalie notamment :

- **Tests de règle sur les anomalies**
- **Tests de règle comportementale**
- **Tests de règle de seuil**

Tests de règle sur les anomalies

Cette section fournit des informations sur les tests de règle d'événement que vous pouvez appliquer aux règles notamment :

- **Tests sur les anomalies**
- **Tests du seuil de temps**

Tests sur les anomalies

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	Valide 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. 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. ***Remarque :*** *L'accumulateur envoie des données au moteur de règle de détection d'anomalie à intervalles d'une minute. Pour plus d'informations sur l'accumulateur, voir IBM Security QRadar Network Anomaly Detection Administration Guide.*	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)**	Configurez les paramètres suivants : • **this accumulated property** - Indiquez la propriété accumulée que vous souhaitez que ce test prenne en considération. • **1 min** - Indiquez l'intervalle de temps que vous souhaitez que ce test prenne en considération. La valeur par défaut est **1 min**. • **40** - Indiquez le pourcentage que vous souhaitez que ce test prenne en considération. Le pourcentage par défaut est **40**. • **1 min** - Indiquez l'intervalle de temps qu'utilise ces test pour comparer la durée de l'intervalle. L'intervalle par défaut est **1 min**.
Minimum Value	Valide 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 (**some value)**	**some value** - Indiquez la valeur que vous souhaitez considérée pour l'intervalle d'accumulation configuré.

Tests du 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	Valide 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 : • **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	Valide 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 vous souhaitez que ce test prenne en considération.
Time Range	Valide 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 : • **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 comportementale

Cette section fournit des informations sur les tests de règle de comportement que vous pouvez appliquer aux règles notamment :

- **Tests comportementaux**
- **Tests sur le délai de temps**

Tests comportementaux

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 vous souhaitez que ce test prenne en considération.

Tableau A-38 Règles de comportement : Tests de comportement (suite)

Test	Description	Nom du test par défaut	Paramètres
Current Traffic Level	Valide 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 vous souhaitez que ce test prenne en considération. La valeur par défaut est **70**.
Current Traffic Trend	Valide lorsque la tendance du trafic représente un effet saisonnier spécifique dans les données pour chaque intervalle de temps. Par exemple, la tendance de trafic en cours peut tester lorsque les données augmente le même increases the same amount from week 2 to week 3 as it did from week 1 to week 2.	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	**30** - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que vous souhaitez que ce test prenne en considération. Le pourcentage par défaut est **30**.
Current Traffic Behavior	Valide lorsque le comportement du trafic change dans les données pour chaque intervalle de temps. 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.	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	**30** - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que vous souhaitez que ce test prenne en considération. Le pourcentage par défaut est **30**.
Deviation	Valide lorsque la propriété accumulée s'écarte du modèle du trafic prévu.	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).	**50** - Indiquez le pourcentage de déviration que vous souhaitez que ce test prenne en considération. La valeur par défaut est **50**.

Tableau A-38 Règles de comportement : Tests de comportement (suite)

Test	Description	Nom du test par défaut	Paramètres
Season Length	Valide lorsqye la durée de la saison représente l'intervalle de temps que vous souhaitez tester. 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, définissez la durée de la saison sur un jour.	Lorsque la durée de la saison est un jour	**a day | a week | a month** - Indiquez la durée de la saison que vous souhaitez que ce test prenne en considération.
Minimum Value	Valide 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 sur le délai 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	Valide 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 : • **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	Valide 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 vous souhaitez que ce test prenne en considération.
Time Range	Valide 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 : • **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 champ**
- **Tests de délai de temps**

Tests de seuil de champ

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	Valide 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**)	• **this accumulated property** - Indiquez la propriété accumulée que vous souhaitez que ce test prenne 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 vous souhaitez que ce test prenne 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	Valide 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)	• **this accumulated property** - Indiquez la propriété accumulée que vous souhaitez que ce test prenne en considération. • **0** - Indiquez la valeur que vous souhaitez que ce test prenne en considération en tant que début d'intervalle. La valeur par défaut est **0**. • **0** - Indiquez la valeur que vous souhaitez que ce test prenne 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 délai 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	Valide 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 : • **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	Valide 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 vous souhaitez que ce test prenne en considération.
Time Range	Valide 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 : • **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

accumulator 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).

capture de contenu 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**.

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.

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.
client	L'hôte qui est à l'origine de la communication.
Common Vulnerability Scoring System (CVSS)	Un score CVSS est une valeur permettant d'évaluer la gravité d'une vulnérabilité. QRadar Network Anomaly Detection utilise les scores CVSS pour mesurer les inquiétude justifiées par une vulnérabilité par rapport à d'autres vulnérabilités.
comportement	Indique les conditions normales dans lesquelles le système ou réseau fonctionne.
coalescing interval	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.
Code HMAC (message d'authentification)	Code cryptographique qui utilise une fonction de hachage crypté et une clé secrète.
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.
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 doive 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.

Device Support Module (DSM) Les modules de support de périphérique (DSMs) vous permettent d'intégrer QRadar Network Anomaly Detection avec des sources de journaux.

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.

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.

DSM Voir Device Support Module (DSM).

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 protocol, les octets, la paquets, les balises, la direction, l'ID d'application et les donnée de contenu (facultatif).

données utiles Données d'application réelles (excluant les informations d'en-tête ou administratives) contenues dans un flux IP..

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 QFlow Collector détecte le même flux, ce dernier est appelé un flux double. Cependant, dans ce cas, le 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.
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.
HMAC	Voir Code HMAC (Hash-based Message Authentication Code).
Host Context	Surveille tout les composants QRadar Network Anomaly Detection pour s'assurer que chaque composant fonctionne comme prévu.
FQNN	Voir Nom de réseau complet.
ICMP	Voir ICMP (Protocole de message de gestion inter-réseau).
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.
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.

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 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.

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.

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.

multidiffusion IP La multidiffusion IP réduit le trafic sur un réseau en délivrant un flux unique d'informations à plusieurs utilisateurs en même temps.

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.

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 compagnie 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.

OSVDB 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.

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 DHCP	Voir Protocole DHCP.
Protocole DHCP	Un protocole qui permet l'attribution dynamique d'adresses IP pour l'équipement installé chez le client.
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 de message de gestion inter-réseau(ICMP)	protocole de couche réseau Internet entre un hôte et une passerelle.
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 See Simple Object Access Protocol.

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.

QID QRadar Network Anomaly Detection Identificateur. Mappage d'un événement unique d'un périphérique externe à un identificateur unique IBM.

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.

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 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 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 user's.
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 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 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).
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.
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.
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 *N* 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 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

Contenu de la présente annexe :

La présente section contient les mentions importantes, les marques et les informations de conformité.

Avis

Les présentes informations ont été élaborées pour des produits et de$ services proposés aux Etats-Unis.

IBM peut ne pas offrir les produits, les services ou les fonctions décrits dans ce document dans d'autres pays. Renseignez-vous auprès de votre interlocuteur IBM local habituel sur les produits et les services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service ne vise pas à indiquer ou suggérer que seul ce produit, logiciel ou service peut être utilisé. Tout autre produit, logiciel ou service équivalent du point de vue fonctionnel peut être utilisé, s'il n'enfreint pas les droits de propriété intellectuelle d'IBM. Cependant, l'utilisateur est tenu de vérifier et d'évaluer le fonctionnement du produit, logiciel 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 du présent document ne vous accorde aucun droit sur ces brevets. Vous pouvez envoyer vos demandes de licences par écrit à :

Directeur Octroi de licences d'IBM.
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 :

Octroi de licences de propriété intellectuelle
Loi sur la propriété juridique et intellectuelle
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique pas au Royaume-Uni ni aux pays où ces dispositions sont incompatibles avec la loi en vigueur : INTERNATIONAL BUSINESS MACHINES CORPORATION FOURNIT LA PRESENTE PUBLICATION "DANS L'ETAT" SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, INCLUANT SANS S'Y LIMITER LES GARANTIES IMPLICITES DE NON-CONTREFACON, DE VALEUR MARCHANDE OU D'ADAPTATION A UN USAGE PARTICULIER. 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.

Les présentes informations peuvent contenir des imprécisions 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, améliorer ou modifier les produits et/ou 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 titulaires de licence 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 conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document ainsi que tous les documents sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions Client d'IBM, au contrat d'octroi de licences de logiciels ou à tout autre accord équivalent entre nous.

Les données de performance indiquées dans le présent 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 réels 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 tarifs indiqués sont des prix de vente actuels conseillés par IBM et sont susceptibles d'être modifiés sans préavis. Les prix distributeurs peuvent donc varier.

Les présentes informations peuvent contenir des exemples de données et de rapports utilisés dans les activités quotidiennes de l'entreprise. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits uniquement à des fins illustratives ou explicatives.Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Si vous visualisez la copie électronique de ces informations, il se peut que les photographies et illustrations en couleur n'apparaissent pas.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp., enregistrés dans de nombreux pays à travers le monde. Il se peut que d'autres produits et services soient 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, et /ou d'autres pays.

INDEX

P

Q

R

S

T

U

V