IBM Security QRadar SIEM
Version 7.1.0 (MR2)

Guide d'utilisation

Remarque : avant d'utiliser ces informations et le produit associé, prenez connaissance des informations figurant à la section “Avis et Marques” du document page 379.

SOMMAIRE

A PROPOS DE CE GUIDE

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

Public visé

Ce guide est destiné à tous les utilisateurs QRadar SIEM chargés des enquêtes et de la gestion de la sécurité réseau. Ce guide suppose que vous avez accès à QRadar SIEM et que vous maîtrisez votre réseau d'entreprise et les technologies réseau.

Conventions

Les conventions suivantes s'appliquent dans ce guide :

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

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

AVERTISSEMENT : *Indique que les informations sont capitales. Un avertissement vous alerte de dangers, menaces ou risques de blessure potentiels. Prenez connaissance de tous les avertissements avant de poursuivre.*

Documentation technique

Pour accéder à davantage de documentation technique, de notes techniques et des notes sur l'édition, voir la ***note technique Accès à la documentation IBM Security QRadar.*** (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacter le service clients

Pour savoir comment contacter le service clients, voir la ***note technique Support and Download***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 A PROPOS DE QRADAR SIEM

QRadar SIEM est une plateforme de gestion de la sécurité des réseaux qui favorise la connaissance de la situation et fournit un support de conformité par la combinaison de la connaissance des réseaux basée sur le flux, la corrélation de l'événement de sécurité, et l'évaluation de la vulnérabilité basée sur l'actif.

Navigateurs web pris en charge

Vous pouvez accéder au Console depuis un navigateur Web standard. QRadar SIEM prend en charge certaines versions de Mozilla Firefox et les navigateurs web de Microsoft Internet Explorer.

Lorsque vous accédez au système, une invite à fournir le nom d'utilisateur et le mot de passe s'affiche. Le nom de l'utilisateur ainsi que son mot de passe doivent être configurés à l'avance par QRadar SIEM l'administrateur.

Tableau 1-1 Navigateurs web pris en charge

Navigateur web	Versions prises en charge
Mozilla Firefox	10.0 En raison du court cycle d'édition de Mozilla, nous n'avons pas pu valider le test sur les 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 Affichage de compatibilité qui est activé	• 8.0 • 9.0 Pour recevoir des instructions sur la façon d'activer Affichage de Compatibilité, voir **Activation de Compatibiliy View pour Internet Explorer**.

Activation de Compatibiliy View pour Internet Explorer

Vous devez activer Compatibiliy View si vous utilisez le navigateur web de Microsoft Internet Explorer pour accéder à QRadar SIEM.

Procédure

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

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

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

Connexion à QRadar SIEM

QRadar SIEM est une application web. Pour se connecter à QRadar SIEM, 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, vous devez ajouter une exception à Mozilla Firefox pour vous connecter à QRadar SIEM. Pour plus d'informations, voir votre documentation sur le navigateur web 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 QRadar SIEM. Vous devez sélectionner l'option **Continue to this website** pour vous connecter à QRadar SIEM.

Procédure

Etape 1 Ouvrez votre navigateur Web.

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

https://<Adresse IP>

Où **<Adresse IP>** est l'adresse IP du système QRadar SIEM.

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

Etape 4 Cliquez sur **Connectez-vous à QRadar**.

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

Result

Une clé de licence par défaut vous donne accès à l'interface utilisateur pour une durée de cinq semaines. Une fenêtre indiquant la date d'expiration de la clé de licence temporaire s'affiche. Pour plus d'informations sur l'installation d'une clé de licence, voir le *IBM Security QRadar SIEM Manuel d'Administration.*

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

Onglets de l'interface utilisateur

QRadar SIEM divise la fonctionnalité en onglets. L'onlget **Dashboard** s'affiche lorsque vous vous connectez à QRadar SIEM. Vous pouvez facilement naviguer sur les onglets pour localiser les données ou la fonctionnalité requise(s).

Onglet Dashboard

L'onglet **Dashboard** est l'onglet par défaut qui s'affiche lorsque vous vous connectez à QRadar SIEM. Il fournit un environnement d'espace de travail qui prend en charge plusieurs tableaux de bord sur lesquels vous pouvez visualiser vos affichages de sécurité de réseaux, d'activité ou de données collectées par QRadar SIEM. 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 qui vous permet de vous concentrer sur vos responsabilités d'opération réseau ou de sécurité.

Pour de plus amples informations sur l'utilisation de l'onglet **Dashboard**, voir **Gestion de tableau 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 diverses options de navigation ou grâce aux recherches avancées. L'onglet **Offenses** vous permet d'étudier une violation afin de déterminer la cause première d'un problème. Vous pouvez également résoudre le problème.

Pour plus d'informations sur l'onglet **Offenses**, consultez **Gestion de violations**.

Onglet Log Activity

L'onglet **Log Activity** vous permet d'étudier les journaux d'événement envoyés QRadar SIEM 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 **Demande de l’activité du journal**.

Onglet Network Activity

L'onglet **Network Activity** vous permet d'étudier les flux envoyés à QRadar SIEM 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 **Demande de l’activité du réseau**.

Onglet Assets

QRadar SIEM 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 QRadar SIEM 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, QRadar SIEM 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 de l'actif**.

Onglet Reports

L'onglet **Reports** vous permet de créer, distribuer, et gérer les rapports pour toutes les données au sein de QRadar SIEM. 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 QRadar SIEM.

L'onglet **Reports** vous permet d'apposer une marque à 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, consultez **Gestion de rapports**.

Gestionnaire des Risques IBM Security QRadar

Gestionnaire des Risques IBM Security QRadar est un dispositif installé séparément pour contrôler les configurations d'unité, afin de simuler les changements apportés à votre environnement réseau et de classer les risques et les vulnérabilités par ordre de priorité sur votre réseau. Gestionnaire des Risques IBM Security QRadar utilise les données collectées par 7.1.0 (MR1), les données de configuration provenant des dispositifs de réseau et de sécurité (pare-feux, routeurs, commutateurs, ou IPS), flux de vulnérabilité, les sources de sécurité du vendeur pour identifier les risques de sécurité, de politique, et de conformité au sein de votre infrastructure de sécurité et de la probabilité de ces risques exploités.

Remarque : Pour plus d'informations sur Gestionnaire des Risques IBM Security QRadar, contactez votre représentant commercial local.

Onglet Admin

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

- **Configuration du système** - vous permet de configurer les options systèmes et les options de gestion d'utilisateur.
- **Data sources** - vous permet de configurer les sources du journal, les sources de flux, et les options de vulnérabilité.
- **Remote Networks and Services Configuration** - vous permet de configurer les réseaux distants et les groupes de services.
- **Plug-ins** - donne accès aux composants plug-in, tel que le plug-in Gestionnaire des Risques IBM Security QRadar. Cette option est affichée uniquement si des plug-ins sont installés sur votre console.

- **Deployment Editor** - vous permet de gérer les composants individuels de déploiement QRadar SIEM déploiement.

Toutes les mises à jour de configuration que vous faites dans l'onglet **Admin** sont sauvegardées dans une 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 SIEM Manuel d'Administration.*

Procédures communes QRadar SIEM

Divers contrôles dans l'interface utilisateur de QRadar SIEM sont communs à la plupart des onglets de l'interface utilisateur. Cette section donne des informations sur ces procédures communes.

Affichage de messages

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

Avant de commencer

Pour que les notifications de système s'affichent dans la fenêtre Messages, l'administrateur doit créer une règle basée sur chaque type de message de notification et sélectionner la case à cocher **Notify** dans l'assistant Custom Rules. Pour plus d'informations sur la façon de configurer les notifications d'événement et de créer les règles d'événement, voir le *IBM Security QRadar SIEM Manuel d'Administration.*

A propos de cette tâche

Le menu Messages indique le nombre de notifications de système non lues que vous avez dans votre système. Cet indicateur incrémente le nombre jusqu'à ce que vous rejetiez les notifications de système. Pour chaque notification de système, la fenêtre Messages fournit un récapitulatif et le dateur pour déterminer le moment de création de la notification de système. Vous pouvez placer votre curseur de la souris sur une notification pour visualiser plus de détails. Vous pouvez gérer les notifications de système à l'aide des fonctions dans la fenêtre Messages.

Les notifications de système sont également disponibles dans l'onglet **Dashboard** et dans une fenêtre en incrustation facultative qui peut être affichée dans le coin inférieur gauche de l'interface utilisateur. Les actions que vous effectuez dans la fenêtre Messages sont étendues à l'onglet **Dashboard** et à la fenêtre en incrustation. Par exemple, si vous rejetez une notification de système depuis la fenêtre Messages, la notification de système est retirée de tous les affichages de notification de système. Pour plus d'informations sur les notifications de système du tableau de bord, voir **Eléments de notification du système.**

La fenêtre Messages fournit les fonctions suivantes :

Tableau 1-2 Transmet les fonctions window

Fonction	Description
All	Cliquez sur **All** pour afficher toutes les notifications du système. C'est l'option par défaut, par conséquent vous devez seulement cliquer sur **All** si vous avez sélectionné une autre option et que vous souhaitez afficher à nouveau toutes les notifications du système.
Health	Cliquez sur **Health** pour n'afficher que les notifications du système qui ont un niveau de gravité de l'état.
Errors	Cliquez sur **Errors** pour n'afficher que les notifications du système qui ont un niveau de gravité d'erreurs.
Warnings	Cliquez sur **Warnings** pour n'afficher que les notifications du système qui ont un niveau de gravité d'avertissement.
Information	Cliquez sur **Information** pour n'afficher que les notifications du système qui ont un niveau de gravité d'informations
Dismiss All	Cliquez sur **Dismiss All** pour rejeter toutes les notifications du système depuis le vôtre. Si vous avez filtré la liste des notifications de système à l'aide des icônes **Health**, **Errors**, **Warnings** ou **Information,** le texte sur l'icône **View All** se change en 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 du système dans l'onglet **Log Activity.** Si vous avez filtré la liste des notifications de système à l'aide des icônes **Health**, **Errors**, **Warnings**, ou **Information**, le texte sur l'icône **View All** se change en 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 de système pour rejeter la notification de système depuis le vôtre.

Lorsque vous cliquez sur une notification, les détails suivants de la notification du système sont affichés dans une fenêtre en incrustation :

Tableau 1-3 Détails de notification de système

Paramètre	Description
Flag	Affiche un symbole pour indiquer le niveau de gravité de la notification. Pointez votre curseur sur le symbole pour afficher plus de détails sur le niveau de gravité. • Icône d'informations (i) • Icône d'erreurs (X) • Icône d'avertissement (!) • Icône d'état
Host IP	Affiche l'adresse IP hôte de l'hôte qui a créé cette notification.
Severity	Affiche le niveau de gravité de l'incident qui a créé cette notification de système.
Low Level Category	Affiche la catégorie de bas niveau associée à l'incident qui a généré cette notification de système. Par exemple : interruption de service. Pour plus d'informations sur les catégories, consultez le *IBM Security QRadar SIEM Manuel d'Administration*.
Payload	Affiche le contenu des données utiles associé à l'incident qui a généré cette notification de système.
Created	Affiche le temps qui s'est écoulé depuis la création de la notification de système.

Procédure

Etape 1 Connectez-vous à QRadar SIEM.

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

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

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

- Errors
- Warnings
- Information

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

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

Etape 6 Facultatif. Pour afficher les détails de notification de système, placez votre curseur sur la notification de système.

Tri des résultats Dans 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 l'odre du tri.

Procédure

Etape 1 Connectez-vous à QRadar SIEM.

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

Etape 3 Sélectionnez l'une des options suivantes :

- Cliquez sur l'en-tête de colonne une fois pour trier le tableau en ordre décroissant
- Double-cliquez sur l'en-tête de colonne pour trier le tableau en ordre croissant.

Actualisation et mise en pause de l'interface utilisateur

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

A propos de cette tâche

Les onglets **Dashboard** et **Offenses** s'actualisent automatiquement toutes les 60 secondes. Les onglets **Log Activity** et **Network Activity** s'actualisent automatiquement toutes les 60 secondes si vous affichez l'onglet en mode dernier intervalle (actualisation automatique). Le minuteur, situé dans le coin droit supérieur de l'interface, indique le temps jusqu'à ce que l'onglet soit automatiquement actualisé.

Lorsque vous visualisez l'onglet **Log Activity** ou **Network Activity** en temps réel (streaming) ou en mode Dernière minute (auto refresh), vous pouvez utiliser l'icône **Pause** pour mettre en pause l'affichage actuel.

Vous pouvez également mettre en pause l'affichage actuel dans l'onglet **Dashboard**. Le fait de cliquer n'importe où dans un élément du tableau de bord met l'onglet automatiquement en pause. Le minuteur clignote en rouge pour indiquer que l'affichage en cours est en pause.

Procédure

Etape 1 Connectez-vous à QRadar SIEM.

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

Etape 3 Sélectionnez l'une des options suivantes :

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

Étude des adresses IP

Les onglets **Dashboard**, **Log Activity**, **Offenses** et **Network Activity** offrent plusieurs méthodes pour l'étude d'une adresse IP depuis 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 met à votre disposition des options pour l'étude d'une adresse IP. Vous pouvez ajouter les options du menu contextuel personnalisé au menu. Pour de plus amples informations sur la façon de personnaliser le menu contextuel, voir la note technique : Personnalisation du menu contextuel.

Procédure

Etape 1 Connectez-vous à QRadar SIEM.

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

Etape 3 Placez le curseur sur une adresse IP pour visualiser l'emplacement de l'adresse IP.

Etape 4 Cliquez avec le bouton droit de la souris sur l'adresse IP ou sur le nom de l'actif et sélectionnez l'une des options suivantes :

Option	Description
Naviguez > Affichage via le réseau	Affiche la liste de la fenêtre Réseaux, qui affiche tous les réseaux associés à l'adresse IP sélectionnée.
Naviguez > Affichez le résumé de la source	Affiche la liste de la fenêtre des violations, qui affiche toutes les violations associées à l'adresse IP source sélectionnée.
Naviguez > Affichez le résumé de la destination	Affiche la liste de la fenêtre Violations, qui affiche toutes les violations associées à l'adresse IP de la destination sélectionnée.
Informations > Recherche DNS	Recherche les entrées DNS (serveur de noms de domaine) basées sur l'adresse IP
Informations > Recherche WHOIS	Recherche le propriétaire enregistré d'une adresse IP distante. Le serveur WHOIS par défaut est whois.arin.net.
Informations > Analyse du port	Effectue une analyse de l'Associateur Réseau (NMAP) de l'adresse IP sélectionnée. Cette option est disponible uniquement si NMAP est installé sur votre système. Pour plus d'informations sur l'installation de NMAP, consultez la documentation de votre fournisseur.
Informations > Actif informationnel	Affiche les informations relatives au profil de l'actif. Cette option de menu est uniquement disponible lorsque QRadar SIEM a acquis les données de profil activement via une analyse ou passivement via des sources de flux. Pour plus d'informations, consultez le Manuel d'administration *IBM Security QRadar SIEM.*
Informations > Événements de recherche	Sélectionnez l'option **Search Events** pour rechercher des événements associés à cette adresse IP. Pour plus d'informations, consultez **Rechercher des événements ou des flux.**
Informations > Flux de recherche	Sélectionnez l'option **Search Flows** pour rechercher des flux associés à cette adresse IP. Pour plus d'informations, consultez **Rechercher des événements ou des flux.**.

Option	Description
Informations > Connexions de recherche	Sélectionnez l'option **Search Connections** pour rechercher des connexions associées à cette adresse IP. Cette option est affichée uniquement lorsque le Gestionnaire des Risques IBM Security QRadar a été acheté et autorisé sous licence, et lorsque vous avez établi la connexion entre la console et le dispositif Gestionnaire des Risques IBM Security QRadar. Pour de plus amples informations, consultez le *Gestionnaire des Risques IBM Security QRadar Manuel de l'utilisateur.*
Informations > Recherche de port de commutation	Sélectionnez **Switch Port Lookup** pour déterminer le port de commutation sur un périphérique IOS pour cette adresse IP. Cette option s'applique uniquement aux commutateurs reconnus à l'aide de l'option Discover Devices sur l'onglet **Gestionnaire des Risques IBM Security QRadar**. Pour plus d'informations, consultez le *Gestionnaire des Risques IBM Security QRadar Manuel de l'utilisateur.*
Informations > Affichez la topologie	Sélectionnez l'option **View Topology** pour afficher l'onglet **Gestionnaire des Risques IBM Security QRadar Topology** qui décrit la topologie couche 3 de votre réseau. Cette option est affichée uniquement lorsque le Gestionnaire des Risques IBM Security QRadar a été acheté et autorisé sous licence, et lorsque vous avez établi la connexion entre la console et le dispositif Gestionnaire des Risques IBM Security QRadar. Pour de plus amples informations, consultez le *Gestionnaire des Risques IBM Security QRadar Manuel de l'utilisateur.*

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 du menu incluent :

Option	Description
Affichez les actifs	Affiche la fenêtre Assets Lists, qui affiche les actifs en cours associés au nom d'utilisateur sélectionné. Pour plus d'informations sur l'affichage des actifs, consultez **Gestion de l'actif.**
Affichez l'historique de l'utilisateur	Affiche la fenêtre Assets Lists, qui affiche tous les actifs associés au nom d'utilisateur sélectionné au cours des dernières 24 heures. Pour plus d'informations sur l'affichage des actifs, consultez **Gestion de l'actif.**
Affichez les événements	Affiche la fenêtre List of Events, qui affiche les événements associés au nom d'utilisateur sélectionné. Pour plus d'informations sur la fenêtre List of Events, consultez **Contrôle de l'activité du réseau.**

Remarque : Pour plus d'informations sur la personnalisation du menu contextuel, consultez *La note technique :* Personnalisation du menu contextuel.

Heure du système

Dans le coin droit de QRadar SIEM, l'interface utilisateur affiche l'heure du système, qui correspond à l'heure de la console. L'heure de la console synchronise tous les systèmes QRadar SIEM dans le déploiement de QRadar SIEM et est utilisée 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 réparti, la console peut se trouver dans un fuseau horaire différent de celui de votre ordinateur de bureau. Lorsque vous appliquez des filtres et effectuez des recherches sur la base de l'heure sur les onglets **Log Activity** et **Network Activity**, vous devez utiliser l'Heure système de la console lors de la spécification d'un intervalle.

Mise à jour des détails de l'utilisateur

Vous pouvez mettre à jour les détails de l'utilisateur par l'interface utilisateur principale de QRadar SIEM.

Procédure

Etape 1 Pour accéder aux informations relatives à l'utilisateur, cliquez sur **Préférences**.

Etape 2 Au besoin, mettre à jour les paramètres suivants :

Options	Description
Nom d'utilisateur	Affiche votre nom d'utilisateur. Ce champ n'est pas modifiable.
Mot de passe	Saisissez un nouveau mot de passe. Le mot de passe doit répondre aux critères suivants : • Doit contenir au minimum six caractères • Doit contenir au maximum 255 caractères • Contenir au moins un caractère spécial • Contenir un caractère majuscule
Mot de passe (Confirmez)	Entrez à nouveau le mot de passe pour confirmation.
Adresse e-mail	Saisissez votre adresse e-mail. L'adresse e-mail doit répondre aux conditions suivantes : • Adresse e-mail valide • Doit contenir au minimum 10 caractères • Doit contenir 255 caractères au maximum
Activez les notifications contextuelles	Sélectionnez cette case à cocher si vous souhaitez activer les notifications du système contextuel afin qu'elles soient affichées sur votre interface utilisateur.

Accès à l'aide en ligne

Vous pouvez accéder à l'aide en ligne de QRadar SIEM par l'interface utilisateur principale de QRadar SIEM. Pour accéder à l'aide en ligne, cliquez sur **Help > Help Contents.**

Redimensionnement des colonnes

Plusieurs onglets QRadar SIEM, dont les onglets **Offenses**, **Log Activity**, **Network Activity**, **Assets** et **Reports,** vous permettent de redimensionner les colonnes de l'affichage. Placez le curseur 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 du format de page

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

2 GESTION DES TABLEAUX DE BORD

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

Présentation des tableaux de bord

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

Tableaux de bord par défaut

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

Le tableau suivant définit les tableaux de bord par défaut.

Tableau 2-1 Tableaux de bord par défaut

Tableaux de bord par défaut	Eléments
Application Overview	Le tableau de bord **Application Overview** comprend les éléments par défaut suivants : • Inbound Traffic by Country (nombre total d'octets) • Outbound Traffic by Country (nombre total d'octets) • Top Applications (nombre total d'octets) • Top Applications Inbound from Internet (nombre total d'octets) • Top Applications Outbound to the Internet (nombre total d'octets) • Top Services Denied through Firewalls (Event Count) • DSCP - Precedence (nombre total d'octets)

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

Tableaux de bord par défaut	Eléments
Compliance Overview	Le tableau de bord **Compliance Overview** comprend les éléments par défaut suivants : • Top Authentications by User (série temporelle) • Top Authentication Failures by User (Event Count) • Login Failures by User (en temps réel) • Compliance: Username Involved in Compliance Rules (série temporelle) • Compliance: Source IPs Involved in Compliance Rules (série temporelle) • Most Recent Reports
Network Overview	Le tableau de bord **Network Overview** comprend les éléments par défaut suivants : • Top Talkers (temps réel) • ICMP Type/Code (nombre total de paquets) • Top Networks by Traffic Volume (nombre total d'octets) • Firewall Deny by DST Port (Event Count) • Firewall Deny by DST IP (Event Count) • Firewall Deny by SRC IP (Event Count) • Top Applications (nombre total d'octets) • Link Utilization (en temps réel) • DSCP - Precedence (nombre total d'octets)
System Monitoring	Le tableau de bord **System Monitoring** comprend les éléments par défaut suivants : • Top Log Sources (Event Count) • Link Utilization (en temps réel) • System Notifications • Event Processor Distribution (Event Count) • Event Rate (Events per Second Coalesced - Average 1 Min) • Flow Rate (Flows per Second - Peak 1 Min)

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

Tableaux de bord par défaut	Eléments
Threat and Security Monitoring	Le tableau de bord **Threat and Security Monitoring** comprend les éléments par défaut suivants : • Default-IDS/IPS-All: Top Alarm Signatures (en temps réel) • Top Systems Attacked (Event Count) • Top Systems Sourcing Attacks (Event Count) • My Offenses • Most Severe Offenses • Most Recent Offenses • Top Services Denied through Firewalls (Event Count) • Internet Threat Information Center • Flow Bias (nombre total d'octets) • 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 SIEM affectent uniquement votre système.

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

- Créer des tableaux de bord personnalisés qui sont adaptés à vos responsabilités. QRadar SIEM prend en charge jusqu'à 255 tableaux de bord par utilisateur. Toutefois, des problèmes de performance peuvent se produire si vous créez plus de 10 tableaux de bord.
- Ajouter et supprimer des éléments de tableau de bord à partir des tableaux de bord personnalisés ou par défaut.
- Déplacer et positionner des éléments selon vos besoins. Lors du positionnement des éléments, chaque élément se redimensionne automatiquement en fonction du tableau de bord.
- Ajouter des éléments de tableau de bord personnalisés basés sur des données.

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

  Pour créer des éléments personnalisés, vous pouvez créer des recherches enregistrées sur les onglets **Network Activity** ou **Log Activity** et choisir comment représenter les résultats dans le tableau de bord. Chaque tableau de

bord affiche les données actualisées en temps réel. Les graphiques de série temporelle sur le tableau de bord sont actualisés toutes les 5 minutes.

Eléments de tableau de bord disponibles

QRadar SIEM vous permet d'ajouter les éléments de tableau de bord sur vos tableaux de bord par défaut ou personnalisés.

Les catégories d'éléments de tableau de bord suivants sont disponibles :

- **Eléments de recherche de flux**
- **Eléments de violation**
- **Eléments d'activités de journal**
- **Eléments de rapports les plus récents**
- **Eléments de gestionnaire des risques**
- **Elément de récapitulatif du système**
- **Elément de notifications du système**
- **Centre d'information des menaces Internet**
- **Ajouter des éléments du tableau de bord basés sur la recherche à la liste d'ajout d'éléments**

Eléments de recherche de flux

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

QRadar SIEM 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, voir **Ajouter des éléments du tableau de bord basés sur la recherche à la liste d'ajout d'éléments**.

Sur un élément de tableau de bord de recherche de flux, les résultats de recherche affichent des données actualisées en temps réel dans un graphique. Les types de graphiques pris en charge sont la série temporelle, le tableau, le graphique circulaire et à barres. Le type de graphique par défaut est le graphique à barres. Ces graphiques sont configurables. Pour plus d'informations sur la configuration des graphiques, consultez **Configuration de graphiques**.

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

Eléments de violation

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

Remarque : Les violations cachées ou fermées ne sont pas incluses dans les valeurs qui sont affichées dans l'onglet **Dashboard**. Pour plus d'informations sur les événements cachés ou fermés, voir **Gestion des violations**.

Le tableau suivant décrit les éléments de violation :

Tableau 2-2 Eléments de violations

Dashboard item	Description
Most Recent Offenses	Les cinq violations les plus récentes sont identifiées par une barre d'amplitude pour vous informer de leur importance. Pointez votre curseur 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 leur importance. Pointez votre curseur 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 affectées. Les violations sont identifiées par une barre d'amplitude pour vous informer de leur importance. Pointez votre curseur sur l'adresse IP pour afficher des informations détaillées sur l'adresse IP.
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 curseur sur l'adresse IP pour afficher des informations détaillées sur l'adresse IP.
Top Local Destinations	L'élément **Top Local Destinations** affiche les principales destinations locales. Chaque destination est identifiée par une barre d'amplitude pour vous informer de son importance. Pointez votre curseur sur l'adresse IP pour afficher des informations détaillées sur l'adresse IP.
Categories	L'élément **Top Categories Types** affiche les cinq catégories principales associées avec le plus grand nombre de violations.

Eléments d'activités de journal

Les éléments de tableau de bord d'activités de journal vous permettent de surveiller et d'enquêter sur 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 d'activité :

Tableau 2-3 Eléments d'activité journal

Eléments de tableau de bord	Description
Events 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'article est basé. QRadar SIEM comprend des critères de recherche enregistrés par défaut qui sont préconfigurés pour afficher les éléments de recherche d'événements dans le menu de votre onglet **Dashboard.** Vous pouvez ajouter d'autres éléments de tableau de bord de recherche d'événements dans le menu de votre onglet **Dashboard**. Pour plus d'informations, voir **Ajouter des éléments du tableau de bord basés sur la recherche à la liste d'ajout d'éléments**. Sur un élément de tableau de bord **Log Activity**, des résultats de recherche affichent des données de dernière minute en temps réel sur un graphique. Les types de graphiques pris en charge sont la série temporelle, le tableau, le graphique circulaire et à barres. Le type de graphique par défaut est à barres. Ces graphiques sont configurables. Pour plus d'informations sur la configuration des graphiques, consultez **Configuration de graphiques**. Les graphiques de série temporelle sont interactifs. Vous pouvez agrandir et parcourir un calendrier pour étudier l'activité du journal.
Events By Severity	L'élément de tableau de bord **Events By Severity** affiche le nombre d'événements actifs regroupés par ordre de gravité. Cette option vous permet de voir le nombre d'événements qui sont reçus par le niveau de gravité qui a été attribué. La gravité indique le niveau de menace créé par une source de violation par rapport à la préparation de la destination pour l'attaque. La plage de gravité s'étend de 0 (faible) à 10 (élevé). Les types de graphiques pris en charge sont le tableau, le graphique circulaire et à barres.
Top Log Sources	L'élément de tableau de bord **Top Log Sources** affiche les cinq sources principales qui ont envoyé des événements à QRadar SIEM dans les 5 dernières minutes. Le nombre d'événements envoyés à partir de la source de journal spécifiée est indiqué dans le graphique. Cette option vous permet de visualiser des changements potentiels dans le comportement. Par exemple, si une source du journal pare-feu qui ne figure généralement pas dans la liste des 10 meilleures contribue désormais à un grand pourcentage du compte total de messages, il est conseillé d'étudier cet événement. Les types de graphiques pris en charge sont le tableau, le graphique circulaire et à barres.

Eléments de rapports les plus récents

L'élément de tableau de bord **Most Recent Reports** affiche les rapports les plus récemment générés. L'affichage fournit le titre du rapport, l'heure et la date de création du rapport et le format du rapport.

Elément de récapitulatif du système

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

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

Eléments de gestionnaire des risques

Les éléments de tableau de bord du gestionnaire des risques s'affichent uniquement lorsque vous achetez IBM Security QRadar Risk Manager et que vous obtenez la licence. Pour plus d'informations, voir le guide d'utilisation *IBM Security QRadar Risk Manager*.

Vous pouvez afficher un élément de tableau de bord personnalisé en fonction des critères de recherche enregistrés à partir de l'onglet **Risks.** Des éléments de recherche de connexion sont répertoriés dans le menu **Add Item > Risk Manager> Connection Searches.** Le nom de l'élément de recherche de connexion correspond au nom des critères de recherche enregistrés sur lequel l'article est basé.

QRadar SIEM comprend des critères de recherche enregistrés par défaut qui sont préconfigurés pour afficher les éléments de recherche de connexion dans le menu de votre onglet **Dashboard**. Vous pouvez ajouter d'autres éléments de tableau de bord de recherche de connexion dans le menu de votre onglet **Dashboard**. Pour plus d'informations, voir **Ajouter des éléments du tableau de bord basés sur la recherche à la liste d'ajout d'éléments**.

Sur un tableau de bord de recherche de connexions, des résultats de recherche affichent des données de dernière minute en temps réel sur un graphique. Les types de graphiques pris en charge sont la série temporelle, le tableau, le graphique circulaire et à barres. Le type de graphique par défaut est le graphique à barres. Ces graphiques sont configurables.

Pour plus d'informations sur la configuration des graphiques, consultez **Configuration de graphiques**.

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

Elément de notifications du système

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

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 **Health**
  - **Icône** d'information (?)
  - **Icône** d'erreur (X)
  - **Icône** d'avertissement (!)
- **Created** - Indique la durée qui s'est écoulée depuis la création de la notification.
- **Description** - Indique les informations sur la notification.
- **Icône de fermeture (x)**- Vous permet de fermer une notification du système.

Vous pouvez pointer votre souris sur la notification pour afficher plus de détails :

- **Host IP** - Indique l'adresse IP de l'hôte qui a créé la notification.
- **Severity** - Indique le niveau de gravité de l'incident qui a créé cette notification.
- **Low Level Category** - Indique la catégorie associée à l'incident qui a généré cette notification. Par exemple : interruption service. Pour plus d'informations sur les catégories, voir*IBM Security QRadar SIEM - Guide d'administration.*
- **Payload** - Indique le contenu de la charge utile associée à l'incident qui a généré cette notification.
- **Created** - Indique la durée qui s'est écoulée depuis la création de la notification.

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

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

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

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

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

Centre d'information des menaces Internet

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

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

Les recommandations actuelles sont répertoriées dans l'élément de tableau de bord. Pour voir un récapitulatif de la recommandation, cliquez sur l'icône en forme de flèche à côté de la recommandation. La recommandation se développe pour afficher un récapitulatif Cliquez sur l'icône en forme de flèche à nouveau pour masquer le récapitulatif.

Pour étudier la recommandation complète, cliquez sur le lien associé : le site d'IBM Internet Security Systems s'ouvre dans une autre fenêtre du navigateur et affiche les détails de 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 de tableaux de bord qui répondent à vos besoins de sécurité réseau.

Affichage d'un tableau de bord

QRadar SIEM fournit cinq tableaux de bord par défaut auxquels vous pouvez accéder à partir de la zone de liste **Show Dashboard**. Si vous avez précédemment consulté un tableau de bord et que vous retournez à l'onglet **Dashboard**, le dernier tableau de bord consulté est affiché.

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 vous permettant d'afficher un groupe d'éléments de tableaux qui répondent à des besoins particuliers.

A propos de cette tâche

Après avoir créé un tableau de bord 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. Cependant, vous devez ajouter des éléments au tableau de bord. Pour plus d'informations sur les éléments de tableau de bord disponibles, voir **Eléments de tableau de bord disponible.**

Procédure

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

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

Etape 3 Dans la zone **Name**, entrez un seul nom 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 des activités du journal ou du réseau à partir d'un élément du tableau de bord

Vous pouvez rechercher l'activité du journal dans un élément de tableau de bord. Les éléments de tableau de bord basés sur la recherche fournissent un lien vers les onglets **Log Activity** ou **Network Activity**. Pour plus d'informations sur les éléments de tableau de bord, voir **Eléments de tableau de bord disponible.**.

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**.

Résultat

Lorsque vous ouvrez l'onglet **Log Activity** ou l'onglet **Network Activity** depuis l'onglet **Dashboard**, les données et deux graphiques correspondant aux paramètres de votre élément de 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 de graphiques

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

A propos de cette tâche

QRadar SIEM accumule les données. Ainsi, lorsque vous effectuez une recherche sauvegardée de séries temporelles, un cache d'événement ou un flux de données est disponible pour afficher les données de la plage 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 Configurer 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 comprennent tous les paramètres d'événements normalisés et personnalisés ou de flux inclus dans vos paramètres de recherche.

Option	Description
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 à courbes interactif qui représente les enregistrements mis en correspondance selon un intervalle de temps spécifié.
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 cochez cette case, la fonction de graphique commence à accumuler des données pour les graphiques de série temporelle. Cette option est désactivée par défaut. ***Remarque :*** *Cette option est uniquement disponible sur les graphiques de série temporelle. Vous devez disposer des autorisations appropriées pour gérer et afficher des graphiques de série temporelle. Pour plus d'informations sur les autorisations de rôle, consultez le Guided'administration IBM Security QRadar SIEM.*
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 des autorisations appropriées pour gérer et afficher des graphiques de série temporelle. Pour plus d'informations sur les autorisations de rôle, consultez le Guided'administration IBM Security QRadar SIEM.*

Suppression d'éléments

Vous pouvez supprimer des éléments dans un tableau de bord. Lorsque vous supprimer un élément du tableau de bord, celui n'est pas entièrement supprimé deQRadar SIEM. 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 le système de votre bureau.

Lorsque vous détachez un élément de tableau de bord, le tableau de bord d'origine demeure sur l'onglet **Dashboard**, pendant qu'une fenêtre détachée avec un élément de tableau de bord dupliqué reste ouverte et s'actualise lors de la planification des intervalles. Si vous souhaitez fermer l'application QRadar SIEM, la fenêtre détachée reste ouverte pour le contrôle et continue de s'actualiser jusqu'à ce que vous fermiez manuellement la fenêtre ou que vous arrêtiez le système de 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 de tableau de bord, cliquez sur l'icône verte pour détacher l'élément de tableau de bord et l'ouvrir dans une fenêtre séparée.

Renommer 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 de 65 caractères.

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

Etape 6 Cliquez sur **OK**.

Suppression d'un tableau de bord

Vous pouvez supprimer un tableau de bord. Une fois que vous supprimez un tableau de bord, l'onglet **Dashboard** s'actualise et le premier tableau de bord qui est répertorié 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 du système

Vous pouvez indiquer le nombre de notifications que vous souhaitez afficher sur votre élément de tableau de bord **System Notification** et écarter les notifications du système une fois vous les avez lu.

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, consultez **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 système 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 comprenant toutes les notifications système s'affiche. Pour plus d'informations sur les événements, voir **Demande de l'activité du journal**.

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

Ajouter des éléments du tableau de bord basés sur la recherche à la liste d'ajout d'éléments

Dans les onglets **Log Activity** et **Network Activity**, vous pouvez ajouter des éléments de tableau de bord basés sur la recherche dans votre menu **Add Items**.

A propos de cette tâche

Cette procédure s'applique à tous les éléments de tableau de bord basés sur la recherche, y compris les éléments du tableau de bord Risk Manager. Les éléments du tableau de bord Risk Manager s'affichent uniquement lorsque vous avez acheté IBM Security QRadar Risk Manager; obtenu une licence et que vous avez établi la connexion entre la console et le dispositif IBM Security QRadar Risk Manager. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation.*

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 de tableau de bord de recherche, cliquez sur l'onglet **Log Activity**.

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

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

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

Assurez-vous de configurer les paramètres suivants :

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

Etape 4 Cliquez sur **Filter**.

Les résultats de la recherche sont affichés.

Etape 5 Cliquez sur **Save Criteria**. Voir **Enregistrer des critères de recherche sur le tableau Offense.**

Etape 6 Cliquez sur **OK**.

Etape 7 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 SIEM peut corréler les événements et les flux avec les adresses IP cible à travers plusieurs réseaux dans 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 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 de violations, voir **Recherches de violations**.

Prise en compte des droits d'accès aux violations

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, voir le *IBM Security QRadar SIEM Administration Guide*.

Termes clés

En utilisant l'onglet **Offenses**, vous pouvez accéder et 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 une adresse IP source tente d'accéder.

Conservation des violation s

Sur l'onglet **Admin**, vous pouvez configurer les paramètres du système de la période 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 SIEM ajoute 5 jours à n'importe quel seuil. Pour plus d'informations, voir le *IBM Security QRadar SIEMGuide d'administration - Configuration des paramètres système*.

Lorsqu'elles sont fermées, les violations sont retirées de la base de données après l'écoulement de la période de conservation. Si des événements supplémentaires se produisent pour cette 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

A l'aide des différentes vues disponible sur l'onglet **Offenses**, vous pouvez suivre les violations qui déterminent les violations qui se produisent actuellement 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 effectuer une action par rapport à la violation, si nécessaire.

Après avoir commencé à naviguer à travers les différents affichages, la partie supérieure 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.

A partir du menu de navigation sur l'onglet **Offenses**, vous pouvez accéder aux pages suivantes :

Tableau 3-1 Options du 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 groupées par les adresses IP source qui sont impliquées dans une violation.
By Destination IP	Affiche toutes les violations groupées par les adresses IP cible qui sont impliquées dans une violation.
By Network	Affiche toutes les violations groupées par les réseaux qui sont impliqués dans une violation.

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

Options	Description
Rules	Permet d'accéder à la page Rules, à partir de laquelle vous pouvez créer des règles personnalisées. Cette option s'affiche uniquement si vous disposez de la permission de rôle **View Custom Rules**. Pour plus d'informations, voir **Gestion des règles**.

Contrôle des pages All Offenses ou My Offenses

Vous pouvez surveiller les violations sur la page All Offenses ou My Offenses. La page All Offenses affiche une liste de toutes les violations survenues dans votre réseau. La page My Offenses affiche une 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 violation appliqués aux résultats de la recherche. Pour supprimer ces paramètres de recherche, cliquez sur **Clear Filter**. Pour plus d'informations sur la recherche de 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 en utilisant les options suivantes :

- Dans la zone **View Offenses**, sélectionnez une option pour filtrer la liste des violations pour un cadre de temps spécifique.
- Si nécessaire, cliquez sur le lien **Clear Filter** à côté de chaque filtre qui s'affiche sur le volet Current Search Parameters.

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

Etape 5 Sur la page Offense Summary, voir les détails sur la violation. Voir **Paramètres des violations**.

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

Contrôle des violations regroupées par catégorie

Vous pouvez surveiller les violations sur la page By Category details, qui vous fournit une liste des violations fondées 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 Dans le menu de navigation, cliquez sur **By Category**.

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

Etape 4 Pour afficher une liste des violations pour 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 Sur la Offense Summary, voir les détails sur la violation. Voir **Paramètres des violations**.

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

Contrôle des violations regroupées par IP source

Sur la page Source, vous pouvez surveiller les violations groupées par adresse IP source.

A propos de cette tâche

Une adresse IP source spécifie l'hôte qui a généré des violations à la suite d'une tentative d'attaque sur votre système. Toutes les adresses IP source sont listées en premier en fonction de la plus grande ampleur. La liste des 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 afficher la liste des violations en utilisant les options suivantes :

- Dans la zone de liste **View Offenses**, sélectionnez une option pour filtrer la liste des violations pour un cadre de temps spécifique.
- Si nécessaire, cliquez sur le lien **Clear Filter** à côté de chaque filtre qui s'affiche sur le volet.

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

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

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

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

Etape 8 Sur la page Offense Summary, voir les détails sur la violation. Voir **Paramètres des violations**.

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

Contrôle des violations regroupées par IP cible

Sur la page Destinations, vous pouvez surveiller les violations groupées par adresse IP cible locale.

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 en utilisant les options suivantes :

- Dans la zone de liste **View Offenses**, sélectionnez une option pour filtrer la liste des violations pour un cadre de temps spécifique.
- Si nécessaire, cliquez sur le lien **Clear Filter** à côté de chaque filtre qui s'affiche sur le volet Current Search Parameters.

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

Etape 5 Pour afficher une liste de violations 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 Sur la page Offense Summary, voir les détails sur la violation. Voir **Paramètres des violations**.

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

Contrôle des violations regroupées par réseau

Sur la page networks, vous pouvez surveiller les violations groupées 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 Dans 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 la barre d'outils de la page **Destinations** Network.

Etape 6 Pour afficher une liste d'adresses IP source associées à ce réseau, cliquez sur la barre d'outils de la page **Offenses** Network.

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

Etape 8 Sur la page Offense Summary, voir les détails sur la violation. Voir **Paramètres des violations**.

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

Tâches de gestion des violations

Lorsque vous surveillez les 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 violations au format XML ou CSV
- Assigner des violations à d'autres utilisateurs
- Envoyer des notification par courrier électronique
- Marquer une violation pour suivi
- Masquer ou fermer une violation dans n'importe quelle liste de violations

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

Ajout de remarques

Vous pouvez ajouter des remarques à toute violation sur l'onglet **Offenses**. Les notes peuvent inclure les informations que vous souhaitez recueillir pour la violation, telles que les informations sur le numéro de ticket de service clients ou la gestion des violations.

A propos de cette tâche

Les notes peuvent inclure jusqu'à 1996 caractères. Le texte de la note ne recherche pas automatiquement de texte et n'est pas modifiable. Le texte s'affiche exactement sur l'onglet tel qu'il a été entré. Par exemple, si vous entrez le texte sans insérer des retours chariots, le texte de la note s'affiche sur une seule ligne dans le récapitulatif **Notes** et la colonne **Note** inclut une barre de défilement.

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

- **Actions** zone de liste dans la barre d'outils récapitulative de violation.
- **Add Note** icône dans le panneau des 5 dernières 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 Dans la zone de liste **Actions**, sélectionnez **Add Note**.

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

Etape 6 Cliquez sur **Add Note**.

Résultat

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 éviter qu'une violation ne s'affiche sur l'onglet **Offenses**, vous pouvez la masquer.

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 qui inclut les violations masquées. Les résultats de recherche incluent toutes les violations, y compris les violations masquées et non masquées. Les violations sont spécifiées comme masquées 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 masquées :

- **a** Dans la zone de liste **Search**, sélectionnez **New Search**.
- **b** Dans la zone de liste **Exclude option** sur le volet Search Parameters, décochez la case **Hidden Offenses**.
- **c** Cliquez sur **Search**.

Etape 4 Localisez et sélectionnez la violation masquées 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 la fermer.

A propos de cette tâche

Après avoir fermé (supprimé) des violations, les violations ne sont plus affichées dans une zone de liste (par exemple, All Offenses) sur l'onglet **Offenses**. Les violations fermées sont supprimées de la base de données après l'écoulement de la durée de conservation. La valeur par défaut de la durée de conservation de la violation est 3 jours. Si des événements supplémentaires se produisent pour cette 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.

Lorsque vous fermez les violations, vous devez sélectionner une raison pour fermer la violation 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. Cette note s'affichera dans l'onglet Notes de cette violation. Si vous disposez de l'autorisation Manage Offense Closing permission, vous pouvez ajouter des causes personnalisées dans la zone de liste **Reason for Closing**. Pour plus d'informations, voir le *IBM Security QRadar SIEMGuide 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 fermer puis sélectionnez **Close** dans la zone de liste **Actions**.
- Dans la zone liste **Actions**, sélectionnez **Close Listed**.

Etape 4 Dans la zone de liste **Reason for Closing**, sélectionnez une raison. 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**.

Résultat

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

Protection des violations

Vous pouvez éviter que les violations spécifiées ne soient retirées de la base de données après l'écoulement de la période de conservation.

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 éviter que les violations spécifiées ne soient retirées de la base de données après l'écoulement de la période de conservation. Pour plus d'informations sur la période de conservation des violations, voir le *IBM Security QRadar SIEMGuide d'administration*.

Remarque : *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 SIEMGuide 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**.

Résultat

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 qui étaient précédemment protégées contre la suppression après l'écoulement de la période de conservation d'une violation.

A propos de cette tâche

Pour énumérer 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 réutiliser 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 SIEM.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 Choisissez 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 zone de liste pour l'affichage immédiat, sélectionnez l'option **Open with** et sélectionnez une application dans la zone de liste.
- Pour sauvegarder 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 SIEM 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, voir le *IBM Security QRadar SIEM Guide d'administration*.

Vous pouvez attribuer des violations aux utilisateurs soit dans l'onglet **Offenses** ou des pages Offense Summary. Cette procédure donne 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 masquer.

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**.

Résultat

la violation est attribuée 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 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 cibles
- 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 SIEM
- 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 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'élément 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. Ceci vous permet de contrôler un article 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**.

Résultat

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 pour vous fournir les fonctions nécessaires pour effectuer certaines actions ou enquêter les facteurs qui contribuent à une violation.**Tableau 3-2** fournit des descriptions pour les fonctions de 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 est uniquement disponible sur le volet Last 5 Notes de la page Offense Summary.
Actions	Les options disponibles dans la zone de liste **Actions** varient en fonction de la page, le tableau ou l'élément (tel qu'une violation ou une adresse IP source). La zone de liste **Actions** peut ne pas s'afficher exactement comme listée 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'élément 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 le récapitulatif de la 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 remarques**. • **Assign** - Sélectionnez cette option pour affecter une violation 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 pour une violation. • **Annotation** - 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 de la règle. Pour plus d'informations sur les règles, voir *IBM Security QRadar SIEMGuide d'administration*. • **Time** - Indique la date et l'heure de création de l'annotation. • **Weight** - Indique la pondération de cette annotation.
Anomaly	Cliquez sur **Anomaly** pour afficher les résultats de recherche enregistrée qui ont déterminé la génération de cette violation par la règle de détection d'anomalie. ***Remarque :*** *Ce bouton s'affiche uniquement si la violation a été générée par une règle de détection d'anomalie.*
Catégories	Cliquez sur **Categories** pour afficher les informations sur la violation. 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** sur la barre d'outils List of Event Categories. Pour plus d'informations sur les catégories, voir le *IBM Security QRadar SIEMGuide d'administration*.
Connections	Cliquez sur **Connections** pour continuer à enquêter sur les connexions. ***Remarque :*** *Cette option n'est disponible que si vous avez acheté et mis sous licence IBM Security QRadar Risk Manager. Pour plus d'informations, voir le IBM Security QRadar Risk ManagerGuide d'utilisation.* Lorsque vous cliquez sur l'icône **Connections,** la page de recherche de critères de connexion s'affiche dans une nouvelle page, pré-remplie avec les critères de recherche d'événements suivants. Vous pouvez personnaliser les paramètres de recherche, si nécessaire. Cliquez sur **Search** pour afficher les informations de connexion.
Destinations	Cliquez sur **Destinations** pour afficher la liste des adresses locales IP cible pour une violation, une IP source ou un réseau. ***Remarque :*** *Si les adresses IP cible associées à cette violation sont distantes, une page séparée s'ouvre pour fournir des informations pour les adresses IP cible distantes.*

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

Fonction	Description
Display	La page Offense Summary affiche plusieurs tableaux d'informations associées à une violation. Pour localiser une table, vous pouvez défiler vers la table que vous souhaitez consulter ou sélectionner l'option dans la zone de liste **Display**.
Evénements	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 **Rechercher des événements et des flux.**
Flows	Cliquez sur **Flows** pour continuer à enquêter sur les flux associés à cette violation. Lorsque vous cliquez sur **Flows**, les résultats de la recherche de flux sont affichés. Voir **Rechercher des événements et des flux.**.
Log Sources	Cliquez sur **Log Sources** pour afficher toutes les sources de journal pour cette violation.
Networks	Cliquez sur **Networks** pour afficher tous les réseaux de destination pour cette violation.
Notes	Cliquez sur **Notes** pour afficher toutes les notes d'une violation, une adresse IP source, une adresse IP destination, ou réseau. Pour plus d'informations sur les notes, voir **Ajout de remarques**.
Offenses	Cliquez sur **Offenses** pour afficher une liste des violations associées à une adresse IP source, une adresse IP destination ou un réseau.
Print	Cliquez sur **Print** pour imprimer une violation.
Rules	Cliquez sur **Rules** pour afficher toutes les règles qui ont contribué à une violation. La règle qui a créé la violation est listée en premier. Si vous disposez des autorisations appropriées pour modifier une règle, double-cliquez sur la règle pour lancer la page Edit Rules. Pour plus d'informations sur les rôles d'utilisateur voir le *IBM Security QRadar SIEMGuide d'administration*. 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 en fonction du paramètre Offense Count. Si vous changez l'ordre de tri ou le tri par un paramètre différent, 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.

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

Fonction	Description
Search	Cette option est uniquement disponible sur la barre d'outils du tableau List of Local Destinations. Cliquez sur **Search** pour filtrer les adresses IP de destination de filtre pour une adresse IP source. Pour filtrer les cibles : **1** Cliquez sur **Search**. **2** Saisissez les 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**.
Show Inactive Categories	Sur la page By Category details, 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 cliquez 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 notes d'une violation, une adresse IP source, une adresse IP destination, ou réseau.
Summary	Si vous avez cliqué pour 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 cette violation.
View Attack Path	Cliquez sur **View Attack Path** pour continuer à enquêter sur le chemin d'attaque de la violation. Lorsque vous cliquez sur l'icône **View Attack Path**, la page Topologie en cours s'affiche sur une nouvelle page. ***Remarque :*** *Cette option n'est disponible que si vous avez acheté et mis sous licence IBM Security QRadar Risk Manager. Pour plus d'informations, voir le IBM Security QRadar Risk ManagerGuide d'utilisation.*

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

Fonction	Description
View Topology	Cliquez sur **View Topology** pour continuer à enquêter sur la source de la violation. Lorsque vous cliquez sur l'icône **View Topology**, la page Current Topology est affichée sur une nouvelle page. ***Remarque :*** *Cette option s'affiche uniquement lorsque IBM Security QRadar Risk Manager a été acheté et mis sous licence. Pour plus d'informations, voir le IBM Security QRadar Risk ManagerGuide d'utilisation.*

Paramètres des violations

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

Tableau 3-3 Paramètres de violation

Paramètre	Emplacement	Description
Annotation	Tableau des 5 principales annotations	Indique les détails pour cette 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'informations sur les règles, voir le *IBM Security QRadar SIEM Guide d'administration.*
Anomaly	Tableau des 10 derniers événements (Evénements d'anomalie)	Sélectionnez cette option pour afficher les résultats de recherche enregistrée qui ont poussé la règle de détection à générer cet événement.
Anomaly Text	Tableau des 10 derniers événements (Evénements d'anomalie)	Indique une description du comportement anormal qui a été détecté par la règle de détection d'anomalie.
Anomaly Value	Tableau des 10 derniers événements (Evénements d'anomalie)	Indique la valeur qui a poussé la règle de détection d'anomalie à générer cette violation.
Application	Tableau des 10 derniers flux	Indique l'application associée à ce flux.
Application Name	tableau Offense Source, si Offense Type est App ID	Indique l'application associée au flux qui a créé cette violation.
ASN Index	Tableau Offense Source, si Offense Type est Source ASN ou Destination ASN	Indique la valeur ASN associée au flux qui a créé la violation.
Asset Name	Tableau Offense Source, si Offense Type 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 de l'actif**.
Asset Weight	Tableau Offense Source, si Offense Type 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 de l'actif**.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Assigned to	Offense table	Indique l'utilisateur affecté à cette violation. Si aucun utilisateur n'est affecté, cette zone indique Not assigned. Cliquez sur **Not assigned** pour affecter cette violation à un utilisateur. Pour plus d'informations, voir **Affectation des violations aux utilisateurs**.
Category	Tableau des 10 derniers flux	Indique la catégorie de cet événement.
Category Name	Page By Category Details	Indique le nom de catégorie de haut niveau. Pour plus d'informations les catégories de haut niveau, voir le *IBM Security QRadar SIEM Guide d'administration*.
Chained	• Tableau Offense Source, si Offense Type est Destination IP • Tableau des 5 principales IP cible	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 pour une autre violation. Si l'adresse IP cible est enchaînée, cliquez sur **Yes** pour afficher les violations enchaînées.
Creation Date	Tableau des 5 dernières notes	Indique la date et l'heure de création de cette note.
Credibility	Tableau des violations	Indique la crédibilité de cette violation, telle que déterminée par le classement de crédibilité de dispositifs 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 avoir appliqué un filtre.*
Description	• Page All Offenses • Page My Offenses • Tableau des violations • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses • Tableau Offense Source, si Offense Type est Log Source • Tableau Top 5 Log Sources	Indique la description de la violation ou de la source de journal.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Destination IP	• Tableau des 10 derniers flux • Tableau des 10 derniers flux	Indique l'adresse IP de destination de cet événement ou flux.
Destination IP	• Tableau des 5 principales IP cible • 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, voir le *IBM Security QRadar SIEM Guide d'administration.*
Destination IP(s)	Tableau des violations	Indique les adresses IP et le nom del'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 del'actif (si disponible) des destinations locales ou distantes. Si plus d'une adresse IP cible est associée à cette 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 cette lation. 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 SIEM Guide d'administration*.
Destination IPs	Page By Network Details	Indique le nombre des adresses IP cible associées ce réseau.
Destination Port	Tableau des 10 derniers flux	Indique le port de destination du flux.
Destination(s)	• Tableau des 5 principales IP cible • 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 pour cette adresse IP source.
Dst Port	Tableau des 10 derniers flux	Indique le port de destination de l'événement.
Duration	Tableau des violations	Indique le volume de temps écoulé depuis la première détection de cette violation.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Event Name	• Tableau Offense Source, si Offense Type est Event Name • Tableau des 10 derniers événements • Tableau des 10 derniers événements (Evénements d'anomalie)	Indique le nom de l'événement, comme indiqué dans la carte QID, associé à l'événement ou au flux qui a créé cette 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 de violation dans cette 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 de destination ou réseau.
Event/Flow Count	Tableau Offense	Indique le nombre d'événements et de flux qui se sont produits pour cette violation et le nombre de catégories. Cliquez sur le lien événements afin d'étudier davantage les événements associés à cette 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 cette 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 SIEM 7.1.0 (MR1), 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 pour cette violation.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Events/Flows	• Tableau Offense Source, si Offense Type 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 des 5 principales IP cible • Page By Source IP Details • Page By Destination IP - List of Sources • Page By Network - List of Sources • Page Source Details • Tableau des 5 principales IP cible • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Network - List of Local Destinations • Tableau des 5 principaux utilisateurs • Tableau Top 5 Log Sources • Tableau des 5 principales catégories • Page By Network Details • Tableau des 5 principales catégories	Indique le nombre d'événements ou de flux associés à l'adresse IP source, l'adresse IP de destination, le nom d'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, Application, le réseau ou la catégorie. Cliquez sur le lien pour afficher plus de détails.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
First event/flow seen on	Page Source Details	Indique la date et l'heure auxquelles l'adresse IP source a généré le premier événement ou flux.
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 le marquage d'une violation pour suivi, voir **Marquage d'élément 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 remarques**. • **Protected** - Indique que cette 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 que la violation ait reçu le dernier événement. En outre, toutes les violations deviennent inactives après la mise à niveau de votre logiciel QRadar SIEM. 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 de violation (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 effectuée sur l'adresse IP source IP, l'adresse IP de destination ou 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 pour cette 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 vers QRadar SIEM 7.1.0 (MR1).*
Group	• Tableau Offense Source, si Offense Type est Log Source • Tableau Top 5 Log Sources	Indique à quel groupe la source de journal appartient.
Group(s)	Tableau Offense Source, si Offense Type est Rule	Indique le groupe de règles auquel appartient la règle.
High Level Category	Tableau Offense Source, si Offense Type est Event Name	Indique la catégorie de haut niveau de l'événement. Pour plus d'informations sur les catégories de haut niveau, voir le *IBM Security QRadar SIEMGuide d'administration*.
Host Name	Table Offense Source, si Offense Type est Source IP ou Destination IP	Indique le nom d'hôte associé à l'adresse IP source ou destination. Si aucun nom d'hôte n'est identifié, cette zone indique Unknown.
Host Name	Tableau Offense Source, si Offense Type est Hostname	Indique le nom d'hôte associé au flux qui a créé cette violation.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
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 SIEM affecte à la violation.
IP	• Tableau Offense Source, si Offense Type est Source IP ou Destination IP • Page Source Details	Indique l'adresse IP source associée à l'événement ou le 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 SIEMGuide d'administration*.
IPv6	Tableau Offense Source, si Offense Type est Source IPv6 ou Destination IPv6	Indique la valeur IPv6 associée au flux ou à l'événement qui a créé la violation.

Tableau 3-3 Paramètres de violation (suite)

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

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Last Known MAC	Tableau Offense Source, si Offense Type est Username ou Hostname	Spécifie la dernière adresse MAC connue de l'utilisateur ou nom d'hôte. Si aucun MAC n'est identifié, cette zone indique Unknown. ***Remarque :*** *Cette zone n'affiche pas les informations historiques.*
Last Known Machine	Tableau Offense Source, si Offense Type est Username, Source MAC Address, Destination MAC Address, ou Hostname	Spécifie le nom de la machine actuelle associée à l'utilisateur, MAC adress ou host name. 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 Offense Type est Source MAC Address, Destination MAC Address ou Hostname	Indique l'utilisateur en cours de l'utilisateur de l'adresse MAC ou 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 Offense Type 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.
Last Packet Time	Tableau des 10 derniers flux	Indique la date et l'heure d'envoi du dernier paquet pour ce flux.
Local Destination Count	Table des 5 principales catégories Page By Category Details	Indique le nombre des adresses IP locales associées à la catégorie.
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 Offense Type est Source IP ou Destination IP • Tableau des 5 principales IP source • Page By Source IP Details • Page Source Details • Page By Destination IP - List of Sources • Page By Network - List of Sources	Indique l'emplacement du réseau de l'adresse IP source, ou l'adresse IP destination. Si l'emplacement est local, vous pouvez cliquer sur le lien pour afficher les réseaux.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Log Source	Tableau des 10 derniers événements	Indique la source de journal qui a détecté l'événement.
Log Source Identifier	Tableau Offense Source, si Offense Type est Log Source	Indique le nom d'hôte de la source de journal.
Log Source Name	Tableau Offense Source, si Offense Type 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 cette 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, voir le IBM Security QRadarGuide d'utilisation des 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 plus d'une source de journal est associée à la violation, cette zone indique Multiple et le nombre de sources de journal.
Low Level Category	Tableau Offense Source, si Offense Type est Event Name	Indique la catégorie de bas niveau de l'événement. Pour plus d'informations sur les catégories de bas niveau, voir le *IBM Security QRadar SIEMGuide d'administration*.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
MAC	• Tableau Offense Source, si Offense Type est Source IP ou Destination IP • Tableau des 5 principales IP source • Tableau des 5 principales IP cible • 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 la source ou l'adresse IP de destination lorsque la violation a commencé. Si l'adresse MAC est inconnue, cette zone indique Unknown.
MAC Address	Tableau Offense Source, si Offense Type est Source MAC Address ou Destination MAC Address	Indique l'adresse MAC associée à l'événement qui a créé la violation. Si aucune adresse MAC n'est identifiée, cette zone indique Unknown.
Magnitude	• Page All Offenses • Page My Offenses • Tableau des violations • Page By Source IP - List of Offenses • Page By Network - List of Offenses • Page By Destination IP - List of Offenses • Tableau des 5 principales catégories • Tableau des 10 derniers événements • 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 incluent 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 de violation (suite)

Paramètre	Emplacement	Description
Magnitude	• Tableau Offense Source, si Offense Type est Source IP ou Destination IP • Tableau des 5 principales IP cible • Tableau des 5 principales IP cible • 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 destination. 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 des 5 principales sources de journal • Tableau des 5 principaux utilisateurs • Table des 5 principales catégories • Page Network	Indique le nom de la source de journal, l'utilisateur, la catégorie, l'adresse IP du réseau ou le nom.
Network	Page By Network Details	Indique le nom du réseau.
Network(s)	Tableau des violations	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 plus d'un réseau de destination, le terme Multiple s'affiche. Cliquez sur le lien pour afficher des détails supplémentaires.
Remarques	• Tableau Offense Source, si Offense Type est Rule • Tableau des 5 dernières notes	Indique les notes de la règle.

Tableau 3-3 Paramètres de violation (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 inclut le filtre **Exclude Hidden Offenses**, le nombre de violations qui s'affiche dans le paramètre **Offense Count** peut être correct. Si vous voulez voir le compte total dans le volet By Category, cliquez sur **Clear Filter** à côté du **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 de violation (suite)

Paramètre	Emplacement	Description
Offense Type	• Page All Offenses • Page My Offenses • Tableau des violations • 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 de source de journal, la règle qui a généré la violation met en corrélation les événements basés sur le 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 cette adresse IP source ou destination. Pour afficher des informations supplémentaires à propos de la violation, cliquez sur le nom ou le terme qui s'affiche. Si de multiples 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 de violation (suite)

Paramètre	Emplacement	Description
Offenses	• Tableau Offense Source, si Offense Type 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 des 5 principales IP source • Tableau des 5 principales IP cible • Tableau Top 5 Log Sources • Tableau des 5 principaux utilisateurs • 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 Destination	Indique le nombre de violations associées à l'adresse IP source, l'adresse IP de destination, l'adresse IP, le nom d'événement, le nom d'utilisateur, l'adresse MAC, la source de journal, le nom d'hôte, port, adresse IPv6, ASN, la règle ou l'application. Cliquez sur le lien pour afficher plus détails.
Offenses Launched	Page By Network Details	Indique le nombre de violations originaires de ce réseau.
Offenses Targeted	Page By Network Details	Indique le nombre de violations ciblées pour le réseau.
Port	Tableau Offense Source, si Offense Type est Source Port ou Destination Port	Indique le port associé à l'événement ou le flux qui a créé la violation.
Relevance	Offense table	Indique l'importance relative de cette violation.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Response	Tableau Offense Source, si Offense Type est Rule	Indique le type de réponse pour la règle.
Rule Description	Tableau Offense Source, si Offense Type est Rule	Indique le récapitulatif des paramètres de la règle.
Rule Name	Tableau Offense Source, si Offense Type est Rule	Indique le nom de la règle associée à l'événement ou le flux qui a créé la violation. ***Remarque :*** *L'information affichée pour les violations de règles est dérivée de l'onglet Rules. Pour plus d'informations sur les règles, voir le IBM Security QRadar SIEMGuide d'administration.*
Rule Type	Tableau Offense Source, si Offense Type est Rule	Indique le type de règle pour la violation.
Severity	• Tableau Offense Source, si Offense Type est Event Name • Offense table	Indique la gravité de l'événement ou une 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 des adresses IP source associées à des 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 des 5 principales IP source • Tableau des 10 derniers flux	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 SIEMGuide d'administration*.
Source IP(s)	Offense table	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 de violation (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 des adresses IP source. Si les consultations du serveur DNS sont activées sur l'onglet **Admin,** vous pouvez afficher le nom du serveur DNS en déplaçant votre souris sur l'adresse IP ou sur le nom de l'actif. Pour plus d'informations, voir le *IBM Security QRadar SIEMGuide d'administration*.
Source IPs	Page By Network Details	Indique le nombre des adresses IP associées à ce réseau.
Source Port	Tableau des 10 derniers flux	Indique le port source du flux.
Source(s)	• Tableau des 5 principales IP cible • Page By Source IP - List of Local Destinations • Page By Destination IP Details	Indique le nombre des adresses IP source pour cette adresse IP de destination.
Source(s)	• Page Destination • Page Network	Indique les adresses IP source de la violation associée à cette adresse IP destination ou 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 des adresses IP source avec cette adresse IP de destination.
Start	Offense table	Indique la date et l'heure du premier événement ou flux pour cette 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 cette violation.
Status	Tableau Offense Source, si Offense Type est Log Source	Indique l'état de la source de journal.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Status	Offense table	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 que la violation ait reçu le dernier événement. En outre, toutes les violations deviennent inactives après la mise à niveau de votre logiciel QRadar SIEM. 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 cette 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 cette 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 cette 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 des 10 derniers événements • Tableau des 10 derniers événements (Evénements d'anomalie)	Indique la date et l'heure où le premier événement a été détecté dans l'événement normalisé. Cette date et heure est spécifiée par le périphérique qui a détecté l'événement.
Time	Tableau des 5 principales annotations	Indique la date et l'heure de création de cette annotation.
Total Bytes	Tableau des 10 derniers flux	Indique le nombre total d'octets pour le flux.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Total Events/Flows	• Tableau des 5 principales sources de journal • Tableau des 5 principaux utilisateurs	Indique le nombre total d'événements pour la source de journal ou l'utilisateur.
User	• Tableau Offense Source, si Offense Type est Source IP ou Destination IP ou Username • Tableau des 5 principales IP source • Tableau des 5 principales IP cible • 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 une adresse IP destination. Si aucun utilisateur n'est identifié, cette zone indique Unknown.
Username	Tableau Offense Source, si Offense Type 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 les plus récentes 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 cette violation.*
Username	Tableau des 5 dernières notes	Indique l'utilisateur qui a créé cette note.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
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 plus d'un nom d'utilisateur est associé à la violation, cette zone indique Multiple et le nombre de noms d'utilisateur. Si aucun nom d'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. Dans la zone de liste, sélectionnez l'intervalle à partir duquel vous souhaitez filtrer.
Vulnerabilities	Tableau Offense Source, si Offense Type est Source IP ou Destination IP	Indique le nombre de vulnérabilités identifiées associées à cette adresse IP source ou destination. 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 des 5 principales IP source • Page By Source IP Details • Page By Network - List of Sources • Tableau des 5 principales IP cible • Page By Source IP - List of Local Destinations • Page By Destination IP Details • Page By Network - List of Local Destinations	Indique si cette adresse IP source ou destination dispose de vulnérabilités.

Tableau 3-3 Paramètres de violation (suite)

Paramètre	Emplacement	Description
Weight	• Tableau des 5 principales IP source • Tableau des 5 principales IP cible • 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 des 5 principales annotations	Indique la pondération de l'adresse IP source, destination ou annotation. La pondération d'une adresse IP est attribuée à l'onglet **Assets**. Pour plus d'informations, voir **Gestion de l'actif**.

4 ETUDE DES ACTIVITÉS DE JOURNAL

A l'aide de l'onglet **Log Activity**, vous pouvez surveiller et étudier 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 périphérique pare-feu ou un routeur, qui décrit une action sur un réseau ou un hôte. L'onglet **Log Activity** spécifie les événements qui sont associés aux violations.

Vous devez avoir le droit d'afficher l'onglet **Log Activity**. Pour plus d'informations sur les autorisations et l'affectation de rôles, consultez le guide d'administration *IBM Security QRadar SIEM*.

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 Options de la barre d'outils de l'onglet Log Activity

Option	Description
Search	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 la recherche. Pour plus d'informations sur la fonction de recherche, consultez **Recherches de données.**
Quick Searches	Dans cette zone de liste, vous pouvez exécuter des recherches précédemment enregistrées. Les options sont uniquement affichées dans la zone de liste **Quick Searches** lorsque vous avez enregistré les critères de recherche qui spécifient l'option **Include in my Quick Searches**.
Add Filter	Cliquez sur **Add Filter** pour ajouter un filtre pour les résultats de la recherche actuelle.
Save Criteria	Cliquez sur **Save Criteria** pour enregistrer les critères de la recherche actuelle.

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

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

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

Option	Description
Rules	L'option Rules n'est disponible que si vous disposez de l'autorisation d'afficher ces règles. Cliquez sur **Rules** pour configurer les règles d'événements personnalisés. Les options incluent : • **Rules** - Sélectionnez cette option pour afficher ou créer une règle. Si vous ne disposez que de l'autorisation d'afficher ces règles, la page de synthèse de l'assistant Rules s'affiche. Si vous avez l'autorisation de maintenir des règles personnalisées, l'assistant Rules s'affiche et vous pouvez modifier la règle. ***Remarque :*** *Les options de règles de détection des anomalies ne sont visibles que si vous avez l'autorisation* ***Log Activity > Maintain Custom Rules****.* Pour activer les options de règle de détection d'anomalie (Add Threshold Rule, Add Behavioral Rule et Add Anomaly Rule), vous devez enregistrer un critère de recherche agrégé parce que le critère de recherche sauvegardé indique les paramètres nécessaires. • **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 SIEM. 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. Lorsque vous sélectionnez l'option **Add Threshold Rule**, l'assistant des règles s'affiche, prérempli avec les options appropriées pour la création d'une règle de seuil. • **Add Behavioral Rule** - Sélectionnez cette option pour créer une règle de 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 unchangement en pourcentage de la quantité de temps où un objet est actif. Par exemple, vous pouvez créer une règle comportementale pour comparer le volume moyen du trafic pour les 5 dernières minutes par rapport au volume moyen du trafic au cours de la dernière heure. S'il existe plus d'un changement de 40%, la règle génère une réponse. Lorsque vous sélectionnez l'option **Add Behavioral Rule**, l'assistant des règles s'affiche, prérempli avec les options appropriées pour la création d'une règle de comportementale.

Tableau 4-1 Options de la barre d'outils de l'onglet Log Activity (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 en pourcentage de la quantité de temps où un objet est actif Par exemple, si une zone de votre réseau qui ne communique jamais avec l'Asie et 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 règle s'affiche, prérempli avec les options appropriées pour la création d'une règle d'anomalie. Pour plus d'information sur les règles, consultez le guide d'administration *IBM Security QRadar SIEM.*
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 des événements**. • **Export to XML > Full Export (All Columns)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour s'achever. Voir **Exportation des événements**. • **Export to CSV > Visible Columns** - Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles dans l'onglet Log Activity. Il s'agit de l'option recommandée. Voir **Exportation des événements**. • **Export to CSV > Full Export (All Columns)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour s'achever. Voir **Exportation des événements**. • **Delete** - Sélectionnez cette option pour supprimer un résultat de la recherche. Voir **Managing event and flow search results**. • **Notify** - Sélectionnez cette option pour spécifier que vous souhaitez recevoir une notification par courriel à l'issue de la recherche sélectionnée. Cette option est activée uniquement pour les recherches en cours. ***Remarque :*** *Les options **Print**, **Export to XML** et **Export to CSV** sont désactivées en mode de transmission en continu et lors de l'affichage des résultats de la recherche partielle.*

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

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

Syntaxe de filtre rapide

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

- **Log Activity toolbar** - Sur la barre d'outils, la zone **Quick Filter** vous permet de saisir une chaîne de recherche de texte et cliquez sur l'icône **Quick Filter** pour appliquer votre filtre rapide à la liste affichée des événements.
- **Add Filter dialog box** - De la boîte de dialogue **Add Filter**, accessible en cliquant sur l'icône **Add Filter** sur l'onglet **Log Activity**, vous pouvez sélectionner **Quick Filter** en tant que votre paramètre filtre et tapez une ligne de recherche de texte. Cela vous permet d'appliquer votre filtre rapide à la liste affichée des événements ou des flux. Pour plus d'information sur la boîte de dialogue Add Filter, consultez **Syntaxe de filtre rapide**.
- **Event and Flow search pages** - Depuis les pages de recherche de flux et des événements, vous pouvez ajouter un filtre rapide à votre liste de filtres à inclure dans vos critères de recherche. Pour plus d'informations sur la configuration des critères de recherche, consultez **Rechercher des événements et des flux.**

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

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

- Conditions de groupe à l'aide d'expressions logiques, tels 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 de critères de recherche qui comprend l'expression logique NOT, vous devez inclure au moins un autre type de l'expression logique, dans le cas contraire, votre filtre ne retournera aucun résultat. Par exemple : `(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
- Les caractères suivants doivent être précédés d'une barre oblique inverse pour indiquer que le personnage fait partie de votre terme de recherche : + - && || ! () {} [] ^ " ~ * ? : \. Par exemple : `"%PIX\-5\-304001"`

Options du menu contextuel

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

Les options du menu contextuel sont :

Tableau 4-2 Options du menu contextuel

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

Barre d'état

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

Lorsque QRadar SIEM 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 la recherche.

Contrôle des activités de journal

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

Si vous avez configuré les critères de recherche par défaut, les résultats de cette recherche sont affichés automatiquement lorsque vous accédez à l'onglet **Log Activity**. Pour plus d'information sur l'enregistrement du critère de recherche, consultez **Sauvegarde des critères de recherche d'événements et de flux.**

Affichage des événements en sreaming

Mode de transmission en continu vous permet d'afficher les données d'événement entrant dans votre système. Ce mode vous donne une vue en temps réel de votre activité actuelle en affichant les 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 transmission en continu, les filtres sont maintenus dans le mode de diffusion en continu. Toutefois, le mode de diffusion en continu ne supporte pas les recherches qui incluent des événements groupés. Si vous activez le mode de diffusion en continu sur les événements groupés ou les critères de recherche groupés, l'onglet **Log Activity** affiche les événements normalisés. Voir **Affichage des événements normalisés**.

Pour sélectionner un événement afin d'afficher les détails ou d'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 sont affichés.

Procédure

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

Etape 2 Dans la zone de liste View, sélectionnez **Real Time (streaming).**

Pour obtenir des informations sur les options de la barre d'outil, voir **Tableau 4-1**. Pour plus d'informations sur les paramètres affichés en mode de transmission continu, voir **Tableau 4-7**.

Etape 3 Facultatif. Mettez en pause ou lisez les événements en mode de diffusion en 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 des événements normalisés

QRadar SIEM recueille des événements au format brut et normalise les événements à afficher sur 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 sur l'onglet. Lorsque QRadar SIEM normalise les événements, le système normalise les noms. Par conséquent, le nom qui s'affiche sur l'onglet **Log Activity** peut ne pas correspondre au nom qui s'affiche dans l'événement.

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

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

Tableau 4-3 Onglet Log Activity - Paramètres par défaut (Normalisés)

Paramètre	Description
Current Filters	La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche. Pour effacer les valeurs de filtre, cliquez sur **Clear Filter.** ***Remarque :*** *Ce paramètre ne s'affiche qu'après avoir appliqué un filtre.*
View	Dans cette zone de liste, vous pouvez sélectionner la plage de temps que vous souhaitez filtrer.
Current Statistics	Pas en temps réel (en continu) ou en mode Last Minute (auto refresh), les statistiques actuelles sont affichées, notamment : ***Remarque :*** *Cliquez sur la flèche à côté* ***Current Statistics*** *pour afficher ou masquer les statistiques* • **Total Results** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Data Files Searched** - Indique le nombre total des fichiers de données recherchées au cours de l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total de fichiers de données compressées recherchées au cours de l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'index recherchés au cours de l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques actuelles sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les événements, vous serez peut être invité à fournir des informations statistiques actuelles.*

Tableau 4-3 Onglet Log Activity - Paramètres par défaut (Normalisés) (suite)

Paramètre	Description
Charts	Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'option de regroupement et l'intervalle de temps. Cliquez sur **Hide Charts** si vous souhaitez supprimer les graphiques de votre affichage. Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir **Affichage des violations associées**. ***Remarque :*** *Si vous utilisez Mozilla Firefox comme navigateur et une extension du navigateur ad blocker est installée, les graphiques ne s'affichent pas. Pour afficher des graphiques, vous devez supprimer l'extension de navigateur ad blocker. Pour plus d'informations, consultez la documentation de votre navigateur.*
Icône Offenses	Cliquez sur l'icône **Offenses** pour afficher les détails de la violation associée à cet événement. Pour plus d'informations, voir **Gestion des graphiques**.
Event Name	Indique le nom normalisé de l'événement.
Log Source	Indique la source du journal qui a envoyé l'événement à QRadar SIEM. S'il existe plusieurs sources de journal associées à cet événement, cette zone définit le terme multiples et le nombre de sources du journal.
Event Count	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.
Time	Indique la date et le moment où QRadar SIEM a reçu l'événement.
Low Level Category	Indique la catégorie de bas niveau associée à cet événement. Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration *IBM Security QRadar SIEM*.
Source IP	Indique l'adresse IP source de l'événement.
Source Port	Indique le port source de l'événement.
Destination IP	Indique l'adresse IP de destination de l'événement.
Destination Port	Indique le port de destination de l'événement.
Username	Indique le nom d'utilisateur associé à cet événement. Les noms d'utilisateurs sont souvent disponibles dans les événements d'authentification associés. Pour tous les autres types d'événements où le nom d'utilisateur n'est pas disponible, cette zone spécifie N/A.

Tableau 4-3 Onglet Log Activity - Paramètres par défaut (Normalisés) (suite)

Paramètre	Description
Magnitude	Indique l'ampleur de cet événement. Les variables comprennent la crédibilité, la pertinence et la gravité. Pointez votre souris sur la barre de l'ampleur pour afficher des valeurs et l'amplitude calculée. Pour plus d'information sur la crédibilité, la pertinence et la gravité, consultez **Glossaire**.

Procédure

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

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

Etape 3 Dans la zone de liste **View**, sélectionnez le délai que vous souhaitez afficher.

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

Etape 5 Cliquez deux fois sur l'événement que vous souhaitez afficher de façon plus détaillée. Voir **Détails d'événement**.

Affichage des événements bruts

Vous pouvez afficher les données d'événements bruts. Il s'agit des données d'événement non analysées à partir de la source du journal.

A propos de cette tâche

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

Tableau 4-4 Paramètres des événements bruts

Paramètre	Description
Current Filters	La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche. Pour effacer les valeurs de filtre, cliquez sur **Clear Filter.** ***Remarque :*** *Ce paramètre ne s'affiche qu'après avoir appliqué un filtre.*
View	Dans la zone de liste, sélectionnez la plage de temps que vous souhaitez filtrer.
Current Statistics	Pas en temps réel (en continu) ou en mode Last Minute (auto refresh), les statistiques actuelles sont affichées, notamment : ***Remarque :*** *Cliquez sur la flèche à côté* ***Current Statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Data Files Searched** - Indique le nombre total des fichiers de données recherchées au cours de l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total de fichiers de données compressées recherchées au cours de l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'index recherchés au cours de l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques actuelles sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service clients pour identifier et résoudre les événements, vous serez peut être invité à fournir des informations statistiques actuelles.*

Tableau 4-4 Paramètres des événements bruts (suite)

Paramètre	Description
Charts	Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'option de regroupement et l'intervalle de temps. Cliquez sur **Hide Charts** si vous souhaitez supprimer les graphiques de votre affichage. Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir **Affichage des violations associées**. ***Remarque :*** *Si vous utilisez Mozilla Firefox comme navigateur et une extension du navigateur ad blocker est installée, les graphiques ne s'affichent pas. Pour afficher des graphiques, vous devez supprimer l'extension de navigateur ad blocker. Pour plus d'informations, consultez la documentation de votre navigateur.*
Icône Offenses	Cliquez sur cette icône pour afficher les détails de violation associée à cet événement. Pour plus d'informations, voir **Affichage des violations associées**.
Start Time	Indique l'heure du premier événement, tel que rapporté à QRadar SIEM par la source du journal.
Log Source	Indique la source du journal qui origine cet événement. S'il existe plusieurs sources de journal associées à cet événement, cette zone spécifie le terme Multiple et le nombre de sources du journal.
Payload	Indique les informations de contenu d'événement original au format UTF-8.

Procédure

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

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

Etape 3 Dans la zone de liste **View**, sélectionnez le cadre de l'heure que vous souhaitez afficher.

Etape 4 Cliquez deux fois sur l'événement que vous souhaitez afficher de façon plus détaillée. Voir **Détails d'événement**.

Affichage des événements regroupés

A l'aide de l'onglet **Log Activity**, vous pouvez afficher les événements groupés par diverses options. Dans 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** n'est pas affichée dans le mode de transmission en continu parce que le mode de transmission en continu ne supporte pas les événements groupés. Si vous entrez 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 des événements regroupés

Option du groupe	Description
Low Level Category	Affiche une liste résumée des événements regroupés par la catégorie bas niveau de l'événement. Pour plus d'informations sur les catégories, consultez le guide d'administration *IBM Security QRadar SIEM.*
Event Name	Affiche une liste résumée des événements regroupés par le nom normalisé de l'événement.
Destination IP	Affiche une liste résumée des événements regroupés par l'adresse IP de destination de l'événement.
Destination Port	Affiche une liste résumée des événements regroupés par l'adresse du port de destination de l'événement.
Source IP	Affiche une liste résumée des événements regroupés par l'adresse IP source de l'événement.
Custom Rule	Affiche une liste résumée des événements regroupés par la règle personnalisée associée.
Username	Affiche une liste résumée des événements regroupés par le nom d'utilisateur associé à l'événement.
Log Source	Affiche une liste résumée des événements regroupés par les sources de journal qui envoient l'événement à QRadar SIEM.
High Level Category	Affiche une liste résumée des événements regroupés par la catégorie de haut niveau de l'événement. Pour plus d'informations sur les catégories, consultez le guide d'administration *IBM Security QRadar SIEM*.
Network	Affiche une liste résumée des événements regroupés par le réseau associé à l'événement.
Source Port	Affiche une liste résumée des événements regroupés par l'adresse source du port de l'événement.

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

Tableau 4-6 Paramètres des événements regroupés

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

Tableau 4-6 Paramètres des événements regroupés (suite)

Paramètre	Description
Current Statistics	Pas en temps réel (en continu) ou en mode Last Minute (auto refresh), les statistiques actuelles sont affichées, notamment : ***Remarque :*** *Cliquez sur la flèche à côté* ***Current Statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Data Files Searched** - Indique le nombre total des fichiers de données recherchées au cours de l'intervalle de temps spécifié. • **Compressed Data Files Searched** - Indique le nombre total de fichiers de données compressées recherchées au cours de l'intervalle de temps spécifié. • **Index File Count** - Indique le nombre total de fichiers d'index recherchés au cours de l'intervalle de temps spécifié. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques actuelles sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service clients pour identifier et résoudre les événements, vous serez peut être invité à fournir des informations statistiques actuelles.*

Tableau 4-6 Paramètres des événements regroupés (suite)

Paramètre	Description
Charts	Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'option de regroupement et l'intervalle de temps. Clicquez 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 pour les paramètres qu'ils représentent. À l'aide de la fonction de légende, vous pouvez effectuer les actions suivantes : • Déplacez le pointeur de votre souris sur un élément de légende pour afficher plus d'informations sur les paramètres qu'il représente. • Cliquez avec le bouton droit de la souris sur l'élément de la légende afin d'étudier cet élément. Pour plus d'informations sur les options du menu contextuel, consultez **A propos de QRadar SIEM.** • Cliquez sur un graphique circulaire pour masquer l'élément dans le graphique. Cliquez de nouveau sur l'élément de légende pour afficher l'élément masqué. Vous pouvez également cliquer sur l'élément de graphique correspondant pour masquer/afficher l'élément. • Cliquez sur **Legend** si vous souhaitez déplacer la légende de votre affichage du graphique. ***Remarque :*** *Les graphiques s'affichent uniquement après avoir sélectionné un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir* **Affichage des violations associées**. ***Remarque :*** *Si vous utilisez Mozilla Firefox comme navigateur et une extension du navigateur ad blocker est installée, les graphiques ne s'affichent pas. Pour afficher des graphiques, vous devez supprimer l'extension de navigateur ad blocker. Pour plus d'informations, consultez la documentation de votre navigateur.*
Source IP (Unique Count)	Indique l'adresse IP de source associé à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone définit le terme multiples et le nombre d'adresses IP.
Destination IP (Unique Count)	Indique l'adresse IP de destination associée à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone définit le terme multiples et le nombre d'adresses IP.
Destination Port (Unique Count)	Indique les ports de destination associés à cet événement. S'il existe plusieurs ports associés à cet événement, cette zone définit le terme multiples et le nombre de ports.
Event Name	Indique le nom normalisé de l'événement.

Tableau 4-6 Paramètres des événements regroupés (suite)

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

Procédure

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

Etape 2 Dans la zone de liste View**, sélectionnez l'intervalle de temps que vous souhaitez afficher.**

Etape 3 Dans la zone de liste **Display**, sélectionnez le paramètre par lequel vous souhaitez grouper les événements. Voir le **Tableau 4-5**.

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

Etape 4 Pour afficher la page List of Events d'un groupe, cliquez deux fois sur l'événement que vous souhaitez étudier.

La page List of Events ne conserve pas les configurations de graphique que vous avez peut être définies sur l'onglet **Log Activity**. Pour plus d'informations sur les paramètres de la page List of Events, voir le **Tableau 4-3**.

Etape 5 Pour afficher les détails d'un événement, cliquez deux fois sur l'événement que vous souhaitez étudier. Pour plus d'informations sur les détails d'événements, voir le **Tableau 4-7**.

Détails d'événement

Vous pouvez afficher la liste des événements dans différents modes, notamment le mode de diffusion en flux ou dans des groupes d'événements. Dans n'importe quel mode que vous choisissez pour afficher les événements, vous pouvez localiser et afficher les détails d'un événement unique. La page des détails d'événements fournit les informations suivantes :

Tableau 4-7 Détails d'événements

Paramètre	Description
Event Information	
Event Name	Indique le nom normalisé de l'événement.
Low Level Category	Indique la catégorie de bas niveau de cet événement. Pour plus d'informations sur les catégories, consultez le guide d'administration *IBM Security QRadar SIEM.*
Event Description	Indique une description de l'événement, si disponible.
Magnitude	Indique l'ampleur de cet événement. Pour plus d'informations sur l'ampleur, consultez le **Glossaire**.
Relevance	Indique l'importance de cet événement. Pour plus d'informations sur la pertinence, consultez le **Glossaire**.
Severity	Indique la gravité de cet événement. Pour plus d'informations sur la gravité consultez le **Glossaire**.
Credibility	Indique la crédibilité de cet événement. Pour plus d'informations sur la crédibilité, consultez le **Glossaire**.
Username	Indique le nom d'utilisateur associé à cet événement, si disponible.
Start Time	Indique l'heure à laquelle l'événement a été reçu de la source du journal.
Storage Time	Indique l'heure à laquelle l'événement a été stocké dans la base de données QRadar SIEM.
Log Source Time	Indique l'heure du système tel que rapportée par la source du journal à l'événement du contenu.
Anomaly Detection Information - Ce panneau s'affiche uniquement si cet événement a été généré par une règle de détection d'anomalie. Pour plus d'informations sur les règles de détection d'anomalie, consultez le guide d'administration *IBM Security QRadar SIEM.* Cliquez sur l'icône **Anomaly** pour afficher les résultats de la recherche sauvegardée qui a entraîné la règle de détection d'anomalie afin de générer cet événement.	
Rule Description	Indique la règle de détection d'anomalie qui a généré cet événement.
Anomaly Description	Indique une description du comportement anormal qui a été détecté par la règle de détection d'anomalie.
Anomaly Alert Value	Indique la valeur d'alerte d'anomalie.
Informations sur la source et destination	
Source IP	Indique l'adresse IP source de l'événement.
Destination IP	Indique l'adresse IP de destination de l'événement.

Tableau 4-7 Détails d'événements (suite)

Paramètre	Description
Source Asset Name	Indique le nom d'actif de la source de l'événement défini par l'utilisateur. Pour plus d'information sur les actifs, consultez **Gestion de l'actif.**
Destination Asset Name	Indique le nom de l'actif de la destination de l'événement défini par l'utilisateur. Pour plus d'informations sur les actifs, consultez **Gestion de l'actif.**
Source Port	Indique le port source de cet événement.
Destination Port	Indique le port de destination de cet événement.
Pre NAT Source IP	Pour un pare-feu ou un autre périphérique capable de traduire des adresses réseau (NAT), ce paramètre définit l'adresse IP source avant que les valeurs NAT ont été appliquées. NAT traduit l'adresse IP dans un réseau à une adresse IP différente sur un autre réseau.
Pre NAT Destination IP	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP de destination avant que les valeurs soient appliquées.
Pre NAT Source Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port source avant que les valeurs soient appliquées.
Pre NAT Destination Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port de destination avant que les valeurs soient appliquées.
Post NAT Source IP	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP source avant que les valeurs NAT soient appliquées.
Post NAT Destination IP	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP de destination avant que les valeurs NAT soient appliquées.
Post NAT Source Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port source avant que les valeurs NAT soient appliquées.
Post NAT Destination Port	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port de destination avant que les valeurs NAT soient appliquées.
IPv6 Source	Indique l'adresse IPv6 source de l'événement.
IPv6 Destination	Indique l'adresse IPv6 de destination de l'événement.
Source MAC	Indique l'adresse MAC source de l'événement.
Destination MAC	Indique l'adresse MAC de destination de l'événement.
Information sur Payload	

Tableau 4-7 Détails d'événements (suite)

Paramètre	Description
Payload	Indique le contenu utile de l'événement. Cette zone fournit trois onglets pour afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur **UTF**. • Hexadecimal - Cliquez sur **HEX**. • Base64 - Cliquez sur **Base64**.
Informations supplémentaires	
Protocol	Indique le protocole associé à cet événement.
QID	Indique le QID de cet événement. Chaque événement possède un QID unique. Pour plus d'information sur le mappage du QID, consultez **Modification de mappage d'événement**.
Log Source	Indique la source du journal qui a envoyé l'événement à QRadar SIEM. S'il existe plusieurs sources de journal associées à cet événement, cette zone définit le terme multiples et le nombre de sources du journal.
Event Count	Indique le nombre total d'événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs du même type d'événement pour la même source et adresse IP de destination sont détectés dans une période de temps courte.
Custom Rules	Indique les règles personnalisées qui correspondent à cet événement. Pour plus d'information sur les règles, consultez le guide d'administration *IBM Security QRadar SIEM.*
Custom Rules Partially Matched	Indique les règles personnalisées qui correspondent partiellement à cet événement. Pour plus d'information sur les règles, consultez le guide d'administration *IBM Security QRadar SIEM.*
Annotations	Indique l'annotation pour cet événement. Les annotations sont des descriptions texte que les règles peuvent ajouter automatiquement aux événements au sein d'une réponse de règle. Pour plus d'information sur les règles, consultez le guide d'administration *IBM Security QRadar SIEM*.
Identity Information - QRadar SIEM collecte les informations d'identité, le cas échéant, des messages du journal source. Les informations d'identité fournissent des détails supplémentaires au sujet des actifs sur votre réseau. Les sources de journal génèrent uniquement des informations d'identité si le message de journal envoyé à QRadar SIEM contient une adresse IP et au moins un des éléments suivants : nom d'utilisateur ou adresse MAC. Les sources du journal ne génèrent pas toutes des informations d'identité. Pour plus d'informations sur l'identité et les actifs, consultez **Gestion de l'actif.**	
Identity Username	Indique le nom d'utilisateur de l'actif associé à cet événement.
Identity IP	Indique l'adresse IP de l'actif associée à cet événement.
Identity Net Bios Name	Indique le nom du système d'entrée/sortie de la base du réseau (Net Bios) de l'actif associé à cet événement.

Tableau 4-7 Détails d'événements (suite)

Paramètre	Description
Identity Extended Field	Indique des informations supplémentaires sur l'élément associé à cet événement. Le contenu de cette zone est un texte défini par l'utilisateur et repose sur les périphériques sur votre réseau qui sont disponibles pour fournir des informations d'identité. On peut citer : l'emplacement physique des noms de ports, des politiques pertinentes, des commutateurs de réseau et des noms de port.
Has Identity (Flag)	Indique True si QRadar SIEM a collecté des informations identifiées pour l'actif associé à cet événement. Pour plus d'information sur les périphériques qui envoient les informations d'identité, consultez le guide de configuration *IBM Security QRadar DSM*.
Identity Host Name	Indique le nom d'hôte de l'actif associé à cet événement.
Identity MAC	Indique l'adresse MAC de l'actif associée à cet événement.
Identity Group Name	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 de l'événement fournit les fonctions suivantes :

Tableau 4-8 Barre d'outils des détails d'événements

Fonction	Description
Return to Events List	Cliquez sur **Return to Event List** pour revenir à la liste des événements.
Offense	Cliquez sur **Offense** pour afficher les violations associées à cet événement.
Anomaly	Cliquez sur **Anomaly** pour afficher les résultats de recherche enregistrée qui a provoqué la règle de détection d'anomalie pour générer cet événement. ***Remarque :*** *Cette icône s'affiche uniquement si cet événement a été généré par une règle de détection d'anomalie.*
Map Event	Cliquez sur **Map Event** pour éditer le mappage d'événement. Pour plus d'informations, voir **Modification de mappage d'événement**.
False Positive	Cliquez sur **False Positive** pour ajuster QRadar SIEM à empêcher les événements du faux positif de générer les violations.
Extract Property	Cliquez sur **Extract Property** pour créer une propriété d'événement personnalisé à partir de l'événement sélectionné. Pour plus d'informations, voir **Propriétés personnalisées d'événements et de flux.**
Previous	Cliquez sur **Previous** pour afficher l'événement précédent dans la liste d'événement.

Tableau 4-8 Barre d'outils des détails d'événements (suite)

Fonction	Description
Next	Cliquez sur **Next** pour afficher l'événement suivant dans la liste d'événement.
PCAP Data	***Remarque :*** *Cette option ne s'affiche que si votre console QRadar SIEM est configuré pour s'intégrer avec Juniper JunOS Platform DSM. Pour plus d'information sur la gestion des données PCAP, consultez* **Gestion des données PCAP***.* Dans la zone de liste **PCAP Data**, sélectionnez l'une des options suivantes : • **View PCAP Information** - Sélectionnez cette option pour afficher les informations PCAP. Pour plus d'informations, voir **Affichage des informations PCAP**. • **Download PCAP File** - Sélectionnez cette option pour télécharger le fichier PCAP pour votre système de bureau. Pour plus d'informations, voir **Téléchargement du fichier PCAP sur votre système de bureau**.
Print	Cliquez sur **Print** pour imprimer les détails d'événement.

Affichage des violations associées

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

A propos de cette tâche

Si un événement correspond à un rôle, une violation peut être générée sur l'onglet **Offenses**. Pour plus d'information sur les règles, consultez le guide d'administration *IBM Security QRadar SIEM*.Pour plus d'informations sur la gestion des violations, voir **Gestion de violations**.

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

Procédure

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

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

Etape 3 Cliquez sur l'icône **Offense** à côté de l'événement que vous souhaitez étudier.

Etape 4 Affichez la violation associée.

Modification de mappage d'événement

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

A propos de cette tâche

À des fins de normalisation, QRadar SIEM mappe automatiquement les événements de sources de journal vers des catégories de niveaux supérieur et inférieur. Pour plus d'informations sur les catégories d'événements, consultez le guide d'administration *IBM Security QRadar SIEM*.

Lorsque QRadar SIEM reçoit des événements de sources du journal que le système ne parvient pas à catégoriser, QRadar SIEM catégorise ces événements comme étant inconnus. Ces événements se produisent pour plusieurs raisons, notamment :

- **User-defined Events** - Certaines sources de journal comme Snort, vous permettent de créer des événements définis par l'utilisateur.
- **New Events or Older Events** - Les sources de journal des fournisseurs peuvent mettre à jour leurs logiciels avec des éditions de maintenance pour prendre en charge de nouveaux événements que QRadar SIEM ne peut prendre en charge.

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

Procédure

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

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

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

Etape 4 Cliquez sur 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 à mapper à cet événement, vous pouvez rechercher un QID particulier :

a Sélectionnez l'une des options suivantes :

- Pour rechercher un QID par catégorie, sélectionnez la catégorie de haut niveau de la zone de liste **High-Level Category**.
- Pour rechercher un QID par catégorie, sélectionnez la catégorie de bas niveau de la zone de liste **Low-Level Category**.

- Pour rechercher un QID par type de source de journal, sélectionnez un type de source de journal de la zone de liste **Log Source Type**.
- Pour rechercher un QID par nom, entrez le nom dans la zone **QID/Name**.

b Cliquez sur **Search**.

Une liste des QID s'affiche.

c Sélectionnez le QID que vous souhaitez associé à cet événement.

Etape 7 Cliquez sur **OK**.

Réglage des faux positifs

Vous pouvez utiliser la fonction False Positive Tuning pour empêcher les événements defaux positifs à partir des violations crées. Vous pouvez régler les événements de faux positifs à partir de la liste des événements ou de la page des détails d'événements.

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, consultez le guide d'administration *IBM Security QRadar SIEM*. Pour plus d'informations sur les faux positifs, consultez le **Glossaire**.

Procédure

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

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

Etape 3 Sélectionnez l'événement que vous souhaitez régler.

Etape 4 Cliquez sur **False Positive**.

Etape 5 Dans le panneau Event/Flow Property de la fenêtre False Positive, sélectionnez l'une des options suivantes :

- Event/Flow(s) with a specific QID of <Event>
- Any Event/Flow(s) with a low-level category of <Event>
- Any Event/Flow(s) with a high-level category of <Event>

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

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

Etape 7 Cliquez sur **Tune**.

Gestion des données PCAP

Si votre console QRadar SIEM est configuré pour s'intégrer à Juniper JunOS Platform DSM, QRadar SIEM peut recevoir, traiter et stocker les données Packet Capture (PCAP) d'une source de journal Juniper SRX-Series Services Gateway.

Pour plus d'informations sur Juniper JunOS Platform DSM, consultez le guide de configuration *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 de pouvoir afficher des données PCAP sur l'onglet **Log Activity**, la source du journal Juniper SRX-Series Services Gateway doit être configurée à l'aide du protocole PCAP Syslog Combination. Pour plus d'informations sur la configuration des protocoles de la source du journal, consultez le guide d'utilisation *IBM Security QRadar Log Sources*.

A propos de cette tâche

Lorsque vous effectuez une recherche qui inclut la colonne **PCAP Data**, une icône est affichée dans la colonne PCAP Data des résultats de recherche si les données PCAP sont disponibles pour un événement. L'icône **PCAP** vous permet d'afficher les données PCAP ou de télécharger le fichier PCAP sur votre système de bureau.

Procédure

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

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

Etape 3 Facultatif. Pour rechercher des événements contenant des données PCAP, configurez les critères de recherche suivants :

- **a** Dans la première zone de liste, sélectionnez **PCAP data**.
- **b** Dans la seconde zone de liste, sélectionnez **Equals**.
- **c** Dans la troisième zone de liste, sélectionnez **True**.
- **d** Cliquez sur **Add Filter**.

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

- **a** Depuis la liste **Available Columns** dans le panneau Column Definition, cliquez sur **PCAP Data**.
- **b** Cliquez sur l'icône **Add Column** sur l'ensemble inférieur des icônes pour déplacer la colonne **PCAP Data** à la liste **Columns**.
- **c** Facultatif. Cliquez sur l'icône **Add Column** dans le haut de l'ensemble des icônes pour déplacer la colonne **PCAP Data** d'une liste **Group By**.

Etape 5 Cliquez sur **Filter**.

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

Etape 7 Cliquez deux fois sur l'événement à étudier.

Etape suivante

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

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

Affichage des informations PCAP

Dans le menu de la barre d'outils PCAP Data**, vous pouvez afficher les informations PCAP ou télécharger le fichier PCAP sur votre système de bureau.**Vous pouvez consulter 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 colonne **PCAP Data**. Voir **Affichage de la colonne de données PCAP**.

A propos de cette tâche

Avant de pouvoir afficher des données PCAP, QRadar SIEM doit extraire le fichier PCAP afin de 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.

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

Procédure

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

- Sélectionnez l'événement et 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 étudier, puis sélectionnez **PCAP Data > View PCAP Information** dans la barre d'outils des détails d'événement.

Etape 2 Si vous voulez télécharger les informations sur votre système de bureau, choisissez l'une des options suivantes :

- Cliquez sur **Download PCAP File** pour télécharger le fichier PCAP d'origine pour être utilisé dans une application externe.

- Cliquez sur **Download PCAP Text** pour télécharger le plan d'action en format.TXT.

Etape 3 Sélectionnez l'une des options suivantes :

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

Etape 4 Cliquez sur **OK**.

Téléchargement du fichier PCAP sur votre système de bureau

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

Avant de commencer

Avant d'afficher des informations 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 étudier, choisissez l'une des options suivantes :

- Sélectionnez l'événement et cliquez sur l'icône **PCAP**.
- **Cliquez avec le bouton droit de la souris sur l'icône PCAP**, puis sélectionnez More Options **> Download PCAP File**.
- Cliquez deux fois sur l'événement que vous souhaitez étudier, puis sélectionnez **PCAP Data >** Download PCAP File **depuis la barre d'outils des détails de l'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 dans la zone de liste.
- Si vous souhaitez enregistrer la liste, sélectionnez l'option **Save File.**

Etape 3 Cliquez sur **OK**.

Exportation des événements

Vous pouvez exporter des événements en 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 sur l'onglet **Log Activity**.

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

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

- **Export to XML > Visible Columns** - Sélectionnez cette option pour exporter uniquement les colonnes visibles dans 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 s'achever.
- **Export to CSV > Visible Columns** - Sélectionnez cette option pour exporter uniquement les colonnes visibles dans 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 s'achever.

Etape 4 Si vous souhaitez reprendre vos activités lors de l'exportation, cliquez sur Notify When Done**.**

Résultat

Vous recevez une notification une fois l'exportation terminée. Si vous n'avez pas sélectionner l'icône **Notify When Done**, la fenêtre d'état s'affiche.

5 ETUDE DES ACTIVITÉS DU RÉSEAU

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

Présentation de l'onglet Network Activity

L'affichage de l'onglet **Network Activity** nécessite une autorisation. Pour plus d'informations sur les autorisations et l'affectation de rôles, voir le document *IBM Security QRadar SIEM - Guide d'administration*.

L'onglet **Network Activity** vous permet de contrôler visuellement et d'étudier les données de flux en temps réel, ou d'effectuer des recherches avancées pour filtrer les flux affichés. Un flux est une session de communication entre deux hôtes. Vous pouvez afficher les informations des flux afin de déterminer comment le trafic est communiqué et ce qui est communiqué (si l'option de capture de contenu est activée). Les informations sur le flux peuvent également comprendre certains détails tels que les protocoles, les valeurs ASN ou les valeurs IFIndex (Interface Index).

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 Options de la barre d'outils de l'onglet Network Activity to

Option	Description
Search	Cliquez sur **Search** pour effectuer des recherches avancées sur les flux. Ces options incluent : • **New Search** - Sélectionnez cette option pour créer une nouvelle recherche de flux. • **Edit Search** - Sélectionnez cette option pour sélectionner et éditer la recherche de flux. • **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**.
Quick Searches	Dans la zone de liste, vous pouvez exécuter les recherches sauvegardées. Les options ne sont affichées dans la zone de liste **Quick Searches** qu'après sauvegarde des critères de recherche qui indiquent l'option **Include in my Quick Searches**.

Tableau 5-1 Options de la barre d'outils de l'onglet Network Activity to (suite)

Option	Description
Add Filter	Cliquez sur **Add Filter** pour ajouter un filtre aux résultats de recherche en cours.
Save Criteria	Cliquez sur **Save Criteria** pour sauvegarder le critère de recherche suivant.
Save Results	Cliquez sur **Save Results** pour sauvegarder les résultats de recherche en cours. Cette option ne s' affiche que lorsque la recherche est effectuée. Cette option est activée en mode de diffusion en flux.
Cancel	Cliquez sur **Cancel** pour annuler une recherche en progression. Cette option est désactivée en mode de diffusion en flux.
False Positive	Cliquez sur **False Positive** pour ouvrir la fenêtre False Positive Tuning, qui vous permet d'ajuster les flux connus en tant que faux positifs à partir de la création des violations. Pour plus d'informations sur les faux positifs, voir le **Glossaire**. Cette option est désactivée en mode de diffusion en flux. Voir **Exportation de flux.**

Tableau 5-1 Options de la barre d'outils de l'onglet Network Activity to (suite)

Option	Description
Rules	L'option Rules est uniquement visible si vous avez la permission d'afficher les règles personnalisées. Cliquez sur **Rules** pour configurer les règles de flux personnalisées. Ces options incluent : • **Rules** - Sélectionnez cette option pour afficher ou créer une règle. Si vous avez la permission de consulter les règles, la page récapitulatif de Rules Wizard s'affiche. Si vous avez la permission de maintenir des règles personnalisées, le Rules Wizard s'affiche et vous pouvez éditer la règle. ***Remarque :*** *Les options de règles de détection d'anomalies sont uniquement visibles 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 ajouter un critère de recherche agrégé parce que le critère de recherche sauvegardé indique 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. Les seuils peuvent être basés sur toutes les données collectées par QRadar SIEM. Par exemple, si vous créez une règle de seuil indiquant que pas plus de 220 clients peuvent se connecter au serveur entre 8h et 15h, les règles peuvent générer une alerte lorsque le 221ème client tente de se connecter. Lorsque vous sélectionnez l'option **Add Threshold Rule**, l'assistant des règles s'affiche, rempli avec les options appropriées pour la création d'une règle de seuil. • **Add Behavioral Rule** - Sélectionnez cette option afin de créer une règle de seuil. Une règle de comportement teste le trafic de flux en cas de changement de volume dans le comportement qui se produit dans les modèles saisonniers réguliers. Par exemple, si un serveur de message communique typiquement avec 100 hôtes par seconde à minuit et qu'ensuite il commence à communiquer avec 1000 hôtes par seconde, une règle comportementale génère une alerte. Lorsque vous sélectionnez l'option **Add Behavioral Rule**, l'assistant des règles s'affiche, rempli avec les options appropriées pour la création d'une règle comportementale. • **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, c'est-à-dire un trafic qui subitement s'arrête ou un changement de pourcentage dans un temps donné où un objet est actif.

Tableau 5-1 Options de la barre d'outils de l'onglet Network Activity to (suite)

Option	Description
	Par exemple, vous pouvez créer une règle d'anomalie pour comparer le volume moyen du trafic des cinq dernières minutes avec le volume moyen du trafic sur la dernière heure. S'il existe plus d'un changement de 40%, la règle génère une réponse. Lorsque vous sélectionnez l'option **Add Anomaly Rule**, Rules Wizard s'affiche, pré-rempli avec les options appropriées pour la création d'une règle d'anomalies. Pour plus d'informations sur les règles voir le *IBM Security QRadar SIEM Guide d'administration.*
Actions	Cliquez sur **Actions** pour effectuer les options suivantes : • **Show All** - Sélectionnez cette option pour déplacer tous les filtres sur le critère de recherche et pour afficher tous les flux infiltrés. • **Print** - Sélectionnez cette option afin d'imprimer les flux affichés sur la page. • **Export to XML** - Sélectionnez cette option pour exporter les flux en format XML. Voir **Exportation 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 email à la fin des recherches sélectionnées. Cette option est uniquement activée pour les recherches en cours. ***Remarque :*** *Les options **Print**, **Export to XML** et **Export to CSV** sont activées en mode diffusion en flux et lors de l'affichage des résultats de recherche partielle.*
Quick Filter	Entrez vos critères de recherche dans la zone **Quick Filter** et cliquez sur l'icône **Quick Filter** ou appuyez sur Enter de votre clavier. Tous les flux qui correspondent aux critères de recherche sont affichés dans la liste des flux. Une recherche de texte s'exécute sur le contenu de l'événement afin de déterminer celui qui correspond à votre critère 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 de filtre rapide**.

Syntaxe de filtre rapide

Le filtre rapide vous permet de rechercher les contenus des flux à l'aide de la ligne recherche de texte. La fonctionnalité Quick Filter est disponible dans les emplacements suivants sur l'interface utilisateur :

- **Network Activity toolbar** - Sur la barre d'outils, une zone **Quick Filter** vous permet d'entrer une ligne de recherche de texte et de cliquer sur l'icône **Quick Filter** afin d'appliquer votre filtre rapide à la liste des flux en cours.
- **Add Filter dialog box** - A partir de la boîte de dialogue **Add Filter**, accédez en cliquant sur l'icône **Add Filter** sur l'onglet **Network Activity**, vous pouvez sélectionner **Quick Filter** en tant que paramètre de filtre et entrer une ligne de recherche de texte. Ceci vous permet d'appliquer votre filtre rapide à la liste de flux actuellement affichée. Pour plus d'informations sur la boîte de dialogue **Add Filter**, voir **Recherches de données**.
- **Flow search pages** - A partir des pages, vous pouvez ajouter un filtre rapide à votre liste de filtre à inclure dans vos critères de recherche. Pour plus d'informations sur la configuration des critères de recherche, voir **Recherches de données**.

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

- Les termes de recherche peuvent inclure n'importe quel texte brut que vous vous attendez à trouver dans le contenu. Par exemple, `Firewall`
- Inclure plusieurs termes entre guillemets doubles pour indiquer que vous souhaitez rechercher l'expression 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, sinon, votre filtre ne trouvera aucun résultat. Par exemple : `(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
- Les caractères suivants doivent être précédés par une barre oblique inversée afin d'indiquer que le caractère fait partie du terme de recherche : + - && || ! () {} [] ^ " ~ * ? : \. Par exemple : `"%PIX\-5\-304001"`

Options du menu contextuel

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

Les options du menu contextuel sont :

Tableau 5-2 Effectuez un clic avec le bouton droit de la souris sur les options de menu

Option	Description
Filter on	Sélectionnez cette option pour filtrer les flux sélectionnés, en fonction du paramètre sélectionné dans le flux.
False Positive	Sélectionnez cette option afin d'ouvrir la fenêtre False Positive Tuning, qui vous permet d'ajuster les flux connus pour être des faux positifs à partir de la création des violations. Cette option est désactivée en mode de diffusion en flux. Voir **Exportation de flux.**
More options:	Sélectionnez cette option pour étudier une adresse IP. Voir **Etude des adresses IP**. ***Remarque :*** *Cette option s'affiche en mode de diffusion en flux*

Barre d'état

Lors de la diffusion des flux, la barre d'état affiche la moyenne des résultats reçus par seconde. Ceci est le nombre de résultats que la console a reçus avec succès du processeur d'événement. Si ce nombre est supérieur à 40 résultats par seconde, ne s'afficheront uniquement que 40 résultats. Le reste est mémorisé dans la mémoire tampon Pour afficher les informations sur l'état, placez le pointeur de votre souris sur la barre d'état.

Lorsque QRadar SIEM ne diffusent pas les flux, la barre d'état le nombre de résultats de recherche actuellement affichés ainsi que le temps nécessaire pour le traitement des résultats de recherche de recherche.

Enregistrements des dépassements

Si vous possédez des droits d'administration, vous pouvez indiquer le nombre maximal de flux que vous souhaitez envoyer à partir de QFlow Collector vers les processeurs d'événement. Toutes les données collectées après l'atteinte de la limite de flux configuré sont regroupées dans un enregistrement de flux unique. Cet enregistrement de flux s'affiche ensuite sur l'onglet **Network Activity** avec l'adresse IP source de 127.0.0.4 et l'adresse IP de destination de 127.0.0.5. Cet enregistrement de flux indique le dépassement sur l'onglet **Network Activity**.

Contrôle des l'activité du 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 des flux en streaming**. Vous pouvez spécifier un intervalle pour filtrer les flux utilisant 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 **Sauvegarde des critères de recherche d'événements et de flux.**

Affichage des flux en streaming

Le mode de diffusion en flux vous permet d'afficher les données entrantes à votre système. Ce mode fournit un affichage en temps réel de votre activité de flux en cours 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, l'onglet **Network Activity** affiche les flux normalisés. Voir **Affichage des flux normalisés**.

Lorsque vous souhaitez sélectionner un flux pour afficher les détails ou effectuer une action, vous devez mettre en pause ce mode avant de cliquer deux fois sur un événement. Lorsque la diffusion en flux est mise en pause, les derniers 1000 flux s'affichent.

Procédure

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

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

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

Etape 3 Facultatif. Mettre en pause ou lire la diffusion en flux. Sélectionnez l'une des options suivantes :

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

Affichage des flux normalisés

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

A propos de cette tâche

La normalisation inclut la préparation des données de flux pour afficher des informations lisibles sur l'onglet.

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

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

Tableau 5-3 Paramètres de l'onglet Network Activity b

Paramètre	Description
Current Filters	En haut du tableau s'affichent les détails des filtres appliqués aux résultats de la recherche. Pour supprimer ces valeurs de filtres, cliquez sur **Clear Filter**. ***Remarque :*** *Ce paramètre ne s'affiche qu'après que vous avez appliqué un filtre.*
View	Dans la zone de liste, vous pouvez sélectionner l'intervalle à partir duquel vous souhaitez filtrer.

Tableau 5-3 Paramètres de l'onglet Network Activity b (suite)

Paramètre	Description
Current Statistics	Lorsque vous n'êtes pas définis sur le mode Temps réel (streaming) ou sur le mode dernière minute (auto refresh), les statistiques en cours s'affichent, notamment : ***Remarque :*** *Cliquez sur la flèche à côté de* ***Current statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total des résultats qui correspondent à vos critères de recherche. • **Data Files Searched** - Indique le nombre total des fichiers de données recherchés dans l'intervalle de temps. • **Compressed Data Files Searched** - Indique le nombre total des fichiers de données compressés dans l'intervalle de temps. • **Index File Count** -Indique le nombre total de fichiers d'indexation recherchés dans l'intervalle de temps. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes Lorsque vous contactez le service client pour identifier et résoudre les flux, vous pouvez être invités à fournir les informations de statistiques en cours.*
Charts	Affiche les graphiques configurables représentant les enregistrements correspondant 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 un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir **Configuration des graphiques.** ***Remarque :*** *Si vous utilisez Mozilla Firefox comme navigateur et qu'un bloqueur de publicités est installé, les graphiques ne s'affichent pas.Pour afficher les graphiques, vous devez supprimer le bloqueur de publicités. Pour plus d'informations, voir la documentation du navigateur.*
Offense icon	Cliquez sur l'icône **Offenses** pour voir les détails des actifs associés au flux.

Tableau 5-3 Paramètres de l'onglet Network Activity b (suite)

Paramètre	Description
Flow Type	Indique le type de flux. Les types de flux sont mesurés par le ratio de l'activité entrante vers l'activité sortante. Les types de flux incluent : • **Standard Flow**- Trafic Bidirectionnel • **Type A** - un-vers-plusieurs (unidirectional), par exemple, un hôte unique effectuant une analyse de réseau. • **Type B** - plusieurs-vers-un (unidirectional), par exemple, une attaque DoS (DDoS) distribuée. • **Type C** - un-vers-un (unidirectional), par exemple, un hôte vers une analyse de port d'hôte.
First Packet Time	Indique la date et l'heure où QRadar SIEM a reçu le flux.
Storage time	Indique l'heure où le flux a été enregistré sur la base de donnés de QRadar SIEM.
Source IP	Indique l'adresse IP de la source du flux.
Source Port	Indique le port source du flux.
Destination IP	Indique l'adresse IP de destination du flux.
Destination Port	Indique le port de destination du flux.
Source Bytes	Indique le nombre d'octets envoyés à partir du hôte source.
Destination Bytes	Indique le nombre d'octets envoyés à partir du hôte de destination.
Total Bytes	Indique le nombre total d'octets associés au flux.
Source Packets	Indique le nombre total de paquets envoyés à partir de l'hôte de la source.
Destination Packets	Indique le nombre total de paquets envoyés à partir de l'hôte de destination.
Total Packets	Indique le nombre total de paquets associés au flux.
Protocol	Indique le protocole associé au flux.
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'applications, voir *IBM Security QRadar Application Configuration Guide*.
ICMP Type/Code	Indique le type et le code de internet Control Message Protocol (ICMP), si applicable. Si le flux est du type ICMP et que les informations du code sont en un format connu, la zone s'affiche en tant que `Type <A>, Code <B>` où `<A>` et `<B>` sont les valeurs numériques du type et du code.
Source Flags	Indique les balises de Transmission Control Protocol(TCP) détectées dans le paquet source, si applicable.
Destination Flags	Indique les balise du TCP détectées dans le paquet de destination, si applicable.

Tableau 5-3 Paramètres de l'onglet Network Activity b (suite)

Paramètre	Description
Source QoS	Indique le niveau de service de Quality of service (QoS) du flux. QoS permet au serveur de fournir les différents niveaux de service pour les flux. QoS fournit les différents niveaux des services de base : • **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 la classification de trafic. • **Guaranteed Service** - Ce niveau de service garantit la réservation des ressources du réseau pour certains flux.
Destination QoS	Indique le niveau QS du service pour le flux cible.
Flow Source	Indique le système qui a détecté le flux. Pour plus d'informations sur les sources de flux, voir le *IBM Security QRadar SIEM Guide d'administration*.
Flow Interface	Indique l'interface qui reçoit le flux.
Source If Index	Indique le nombre d'index interface (IFIndex) source.
Destination If Index	Indique le nombre d'IFIndex de destination.
Source ASN	Indique les valeurs Autonomous System Number (ASN) source.
Destination ASN	Indique les valeurs ASN de destination.

Procédure

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

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

Etape 3 Dans la zone de liste **View**, sélectionnez le délai que vous souhaitez afficher.

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

Etape 5 Faites un double clic sur le flux que vous souhaitez afficher avec plus de détails. voir **Détails des flux**.

Affichage des flux regroupés

L'onglet **Network Activity**, vous permet d'afficher les flux groupés par diverses options. Dans 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 de diffusion en flux parce que ce mode ne prend pas en charge les flux groupés. Si vous entrez le mode de diffusion en flux à l'aide d'un critère de recherche non groupé, cette option s'affiche.

La zone de liste Display fournit les options suivantes :

Tableau 5-4 Options de flux groupés

Option du groupe	Description
Flux unis	Affiche les divers flux dans un seul modèle ininterrompu via différents intervalles, dans un enregistrement unique. Par exemple, si un flux est de cinq minutes de longueur, le flux uni s'affiche en tant qu'un seul flux de cinq minutes de longueur. Sans le flux uni, le flux s'affiche en tant que cinq flux : un flux pour chaque minute. Les flux unis affichent une liste résumée de flux groupés par informations du flux uni.
Source or Destination IP	Affiche une liste résumée des flux groupés par une adresse IP associée avec le flux.
Source IP	Affiche une liste résumée des flux groupés par une adresse IP source du flux.
Destination IP	Affiche une liste résumée le la liste des flux groupés par adresse IP de destination du flux.
Source Port	Affiche une liste résumée des flux groupés par le port source du flux.
Destination Port	Affiche une liste résumée des flux groupés par port de destination du flux.
Source Network	Affiche une liste résumée des flux groupés par le réseau source du flux.
Destination Network	Affiche une liste résumée des flux groupés par le réseau de destination du flux.
Application	Affiche une liste résumée des flux groupés par l'application d'origine du flux.
Geographic	Affiche une liste résumée des flux groupés par emplacement géographique.
Protocol	Affiche une liste résumée des flux groupés par le protocole associé avec le flux.
Flow Bias	Affiche une liste résumée des flux groupés par la direction du flux.
ICMP Type	Affiche une liste résumée des flux groupés par le type d'ICMP du flux.

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

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

Tableau 5-5 Paramètres de flux groupés

Paramètre	Description
Grouping By	Indique le paramètre sur lequel le paramètre est groupé.
Current Filters	En haut du tableau s'affichent les détails du filtre appliqué aux résultats de la recherche. Pour supprimer ces valeurs de filtres, cliquez sur **Clear Filter**.
View	Dans la zone de liste, vous pouvez sélectionner l'intervalle à partir duquel vous souhaitez filtrer.
Current Statistics	Lorsque vous n'êtes pas définis sur le mode Temps réel (streaming) ou sur le mode dernière minute (auto refresh), les statistiques en cours s'affichent, notamment : ***Remarque :*** *Cliquez sur la flèche à côté de* ***Current statistics*** *pour afficher ou masquer les statistiques.* • **Total Results** - Indique le nombre total des résultats qui correspondent à vos critères de recherche. • **Data Files Searched** - Indique le nombre total des fichiers de données recherchés dans l'intervalle de temps. • **Compressed Data Files Searched** - Indique le nombre total des fichiers de données compressés dans l'intervalle de temps. • **Index File Count** -Indique le nombre total de fichiers d'indexation recherchés dans l'intervalle de temps. • **Duration** - Indique la durée de la recherche. ***Remarque :*** *Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes Lorsque vous contactez le service client pour identifier et résoudre les flux, vous pouvez être invités à fournir les informations de statistiques en cours.*
Charts	Affiche les graphiques configurables représentant les enregistrements correspondant 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 un laps de temps du Last Interval (auto refresh) ou au-dessus et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir **Configuration des graphiques**. ***Remarque :*** *Si vous utilisez Mozilla Firefox comme navigateur et qu'une extension de blocage des fenêtre publicitaires est installée, les graphiques ne s'afficheront pas. Pour afficher les graphiques, vous devez supprimer l'extension de blocage des fenêtre publicitaires. Pour plus d'informations, voir la documentation du navigateur.*

Tableau 5-5 Paramètres de flux groupés (suite)

Paramètre	Description
Source IP (Unique Count)	Indique l'adresse IP de la source du flux.
Destination IP (Unique Count)	Indique l'adresse IP de destination du flux. S'il existe plusieurs adresses IP de destination associées à ce flux, cette zone indique les divers termes et leur nombre d'adresses IP.
Source Port (Unique Count)	Indique le port de source du flux.
Destination Port (Unique Count)	Indique le port de destination du flux. S'il existe plusieurs ports de destination associés à ce flux, cette zone indique les divers termes et le nombre des ports.
Source Network (Unique Count)	Indique le réseau source du flux. S'il existe plusieurs réseau source associés au flux, cette zone indique le terme Multiple et le nombre de réseau.
Destination Network (Unique Count)	Indique le port de destination du flux. S'il existe plusieurs réseaux de destination associés au flux, cette zone indique le terme Multiple et le nombre de réseaux.
Application (Unique Count)	Indique l'application détectée des flux. S'il existe multiple applications associées à ce flux, cette zone indique le terme et le nombre d'applications.
Source Bytes (Sum)	Indique le nombre d'octets de la source.
Destination Bytes (Sum)	Indique le nombre d'octets de la destination.
Total Bytes (Sum)	Indique le nombre total d'octets associés au flux.
Source Packets (Sum)	Indique le nombre de paquets de la source.
Destination Packets (Sum)	Indique le nombre de paquets de la destination.
Total Packets (Sum)	Indique le nombre total de paquets associés au flux.
Count	Indique le nombre de flux envoyés ou reçus.

Procédure

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

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

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

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

Etape 4 Pour afficher la Page List of Flows pour un groupe, cliquez deux fois sur le groupe de flux que vous souhaitez étudier.

La page List of Flows ne retient pas les configurations de graphique que vous avez peut être défini sur l'onglet **Network Activity**. Pour plus d'informations sur les paramètres List of Flows, voir **Tableau 5-3**.

Etape 5 Pour afficher les détails d'un flux, cliquez deux fois sur le flux que vous souhaitez étudier. Pour plus d'informations sur la page de détails de flux, voir **Tableau 5-6**.

Détails des flux

Vous pouvez afficher une liste de flux selon divers modes, y compris en mode de diffusion en flux ou en groupes de flux. Quelque soit le mode que vous choisissez pour consulter les flux, vous pouvez localiser et afficher les détails d'un flux unique. La page Flow details fournit les informations suivantes :

Tableau 5-6 Détails de flux

Paramètre	Description
Information sur les flux	
Protocol	Indique le protocole associé à ce flux. Pour plus d'informations sur les protocoles, voir le *IBM Security QRadar Guide de configuration d'application*.
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'applications, voir le *IBM Security QRadar Guide de configuration d'application*.
Magnitude	Indique l'ampleur de ce flux. Pour plus d'informations sur l'ampleur, voir le **Glossaire**.
Relevance	Indique la pertinence de ce flux. Pour plus d'informations sur la pertinence, voir le **Glossaire**.
Severity	Indique la gravité de ce flux. Pour plus d'informations sur la gravité voir le **Glossaire**.
Credibility	Indique la crédibilité de ce flux. Pour plus d'informations sur la crédibilité, voir le **Glossaire**.
First Packet Time	Indique l'heure de début du flux, telle que reportée à la source du flux QRadar SIEM. Pour plus d'informations sur les sources de flux, voir le *IBM Security QRadar SIEM Guide d'administration*.
Last Packet Time	Indique l'heure de fin du flux, telle que reportée à la source du flux QRadar SIEM. Pour plus d'informations sur les sources de flux, voir le *IBM Security QRadar SIEM Guide d'administration*.
Storage Time	Indique l'heure où le flux a été enregistré sur la base de données QRadar SIEM.
Event Name	Indique le nom normalisé du flux.
Low Level Category	Indique la catégorie de bas niveau de ce flux. Pour plus d'informations sur les catégories, voir le *IBM Security QRadar SIEM Guide d'administration*.
Event Description	Indique une description du flux, si disponible.
Informations sur la source et la destination	
Source IP	Indique l'adresse IP de la source du flux.
Destination IP	Indique l'adresse IP de destination du flux.

Tableau 5-6 Détails de flux (suite)

Paramètre	Description
Source Asset Name	Indique l'actif de la source du flux. Pour plus d'informations sur les actifs, voir **Gestion de l'actif**.
Destination Asset Name	Indique le nom d'actif de destination du flux. Pour plus d'informations sur les actifs, voir **Gestion de l'actif**.
IPv6 Source	Indique l'adresse IPv6 de la source du flux.
IPv6 Destination	Indique l'adresse IPv6 de la destination du flux.
Source Port	Indique le port source du flux.
Destination Port	Indique le port de destination du flux.
Source QoS	Indique le niveau de service du flux source.
Destination QoS	Indique le niveau QS du service pour le flux cible.
Source ASN	Indique le nombre des valeurs ASN de la source. ***Remarque :*** *Si le flux possède des enregistrements en double provenant des divers sources de flux, les nombres des valeurs ASN source correspondant sont répertoriés.*
Destination ASN	Indique le nombre des valeurs ASN de destination. ***Remarque :*** *Si le flux possède des enregistrements en double provenant des diverses sources de flux, les nombres des valeurs ASN de destination correspondant sont répertoriés.*
Source If Index	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.*
Destination If Index	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.*
Source Payload	Indique le nombre de paquet et d'octets pour le contenu de la source.
Destination Payload	Indique le nombre de paquet et d'octets pour le contenu de destination.
Informations sur le contenu	

Tableau 5-6 Détails de flux (suite)

Paramètre	Description
Source Payload	Indique le contenu de la source du flux. La zone offre trois formats pour afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur **UTF**. • Hexidecimal - Cliquez sur **HEX**. • Base64 - Cliquez sur **Base64**. ***Remarque :*** *Si votre source de flux est Netflow v9 ou IPFIX, des zones non interprétées de ces sources peuvent être affichées dans la zone* ***Source Payload****. Le format de cette zone non interprétée est <name>=<value>. Par exemple,* ***MIN_TTL=x****.*
Destination Payload	Indique le contenu de la destination du flux. La zone offre trois formats pour afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur **UTF**. • Hexidecimal - Cliquez sur **HEX**. • Base64 - Cliquez sur **Base64**.

Tableau 5-6 Détails de flux (suite)

Paramètre	Description
Informations supplémentaires	
Flow Type	Indique le type de flux. Les types de flux sont mesurés par le ratio de l'activité entrante vers l'activité sortante. Les types de flux incluent : • **Standard** - trafic bidirectionnel • **Type A** - Un -vers-plusieurs (unidirectional) • **Type B** - Plusieurs-vers-un (unidirectional) • **Type C** - un-vers-un (unidirectional)
Flow Direction	Indique la direction du flux. Les directions du flux comprennent : • **L2L** - trafic interne du réseau local vers un autre réseau local. • **L2R** - Trafic interne d'un réseau local vers un réseau distant. • **R2L** - Trafic interne d'un réseau distant vers un réseau local. • **R2R** - Trafic interne d'un réseau distant vers un réseau distant.
Custom Rules	Indique les règles personnalisées qui correspondent à ce flux. Pour plus d'informations sur les règles, voir le Guide d'a*dministration de IBM Security QRadar SIEM.*
Les règles personnalisées partiellement correspondantes	Indique les règles personnalisées qui correspondent partiellement à ce flux. Pour plus d'informations sur règles, voir le *IBM Security QRadar SIEM Guide d'administration.*
Flow Source/Interface	Indique le nom de la source du flux du système qui a détecté le flux. ***Remarque :*** *Si ce flux possède plusieurs enregistrements de divers sources de flux, les sources de flux correspondantes sont répertoriées.*
Annotations	Indique l'annotation ou les notes pour ces flux. Les annotations sont des descriptions de texte que les règles peuvent automatiquement ajouter aux flux dans le cadre de la réponse de règle. Pour plus d'informations sur règles, voir le *IBM Security QRadar SIEM Guide d'administration.*

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
Return to Results	Cliquez sur **Return to Results** pour retourner à la liste des flux.
Offense	Cliquez sur **Offense** pour afficher les violations auxquelles le flux est corrélé.

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

Fonction	Description
Extract Property	Cliquez sur **Extract Property** pour créer une propriété de flux personnalisé à partir du flux sélectionné. Pour plus d'informations, voir **Etude des activités du réseau**.
False Positive	Cliquez sur **False Positive** pour ouvrir la fenêtre False Positive Tuning, qui vous permet d'ajuster les flux connus en tant que faux positifs à partir de la création des violations. Cette option est désactivée en mode de diffusion en flux. Voir **Exportation des flux**.
Previous	Cliquez sur **Previous** pour afficher le flux précédent dans la liste d'événements.
Next	Cliquez sur **Next** pour afficher le flux suivant dans la liste d'événements.
Print	Cliquez sur **Print** pour imprimer les détails d'un flux.

Réglage des faux positifs

Vous ne pouvez pas utiliser la fonction False Positive Tuning pour éviter que les flux de faux positifs ne créent pas de violations. Vous pouvez régler les flux de faux positifs à partir de la page de liste de flux ou de détails des flux.

A propos de cette tâche

Vous devez disposer des droits appropriés pour créer des règles personnalisées afin de régler les faux positifs. Pour plus d'informations sur les rôles, voir le *IBM Security QRadar SIEMGuide d'administration*. Pour plus d'informations sur les faux positifs, voir le **Glossaire**.

Procédure

Etape 1 Cliquez sur l'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 la diffusion en flux.

Etape 3 Sélectionnez le flux que vous souhaitez régler.

Etape 4 Cliquez sur **False Positive**.

Etape 5 Dans le volet Event/Flow Property sur la fenêtre False Positive, sélectionnez l'une des questions suivantes :

- Event/Flow(s) avec un QID spécifique <Event>
- Toutes les Event/Flow avec une catégorie de bas niveau du <Event>
- Toutes les Event/Flow avec une catégorie de haut niveau du <Event>

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

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

- Any Source to any Destination

Etape 7 Cliquez sur **Tune**.

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

Exportation des flux

Vous pouvez exporter les flux en format XML ou en format CSV. La durée nécessaire pour exporter vos données dépend du nombre de paramètres spécifiés.

Procédure

Etape 1 Cliquez sur l'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 la diffusion en flux.

Etape 3 A partir de la zone de liste **Actions**, sélectionnez les options suivantes :

- **Export to XML > Visible Columns** - Sélectionnez cette option pour exporter uniquement les colonnes visibles dans l'onglet **Log Activity**. Cette option est recommandée.
- **Export to XML > Full Export (All Columns)** - Sélectionnez cette option pour exporter les paramètres de flux. Le processus d'exportation de flux peut prendre un moment.
- **Export to CSV > Visible Columns** - Sélectionnez cette option pour exporter uniquement les colonnes visibles dans l'onglet **Log Activity**. Cette options est recommandée.
- **Export to CSV > Full Export (All Columns)** - Sélectionnez cette option pour exporter les paramètres de flux. Le processus d'exportation de flux peut prendre un moment.

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

Résultat

Lorsque l'exportation est terminée, vous recevez une notification vous informant que l'exportation est terminée. Si vous n'avez pas sélectionné l'icône **Notify When Done**, la fenêtre état s'affiche.

6 GESTION DES GRAPHIQUES

Les graphiques sur les onglets **Log Activity** et **Network Activity** vous permettent d'afficher vos données à l'aide de différentes options de configuration de graphique.

Présentation des graphiques

Si vous sélectionnez une plage de temps ou une option de regroupement pour afficher vos données sur les onglets **Log Activity** et **Network Activity**, les graphiques s'affichent au-dessus de la liste des événements et des flux. En mode streaming, les graphiques ne s'affichent pas.

Vous pouvez configurer un graphique pour sélectionner les données à tracer. Vous pouvez configurer les graphiques indépendamment l'un de l'autre pour afficher les résultats de votre recherche de différentes perspectives.

Les types de graphiques incluent :

- **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 à courbes interactif qui représente les enregistrements mis en correspondance selon un intervalle de temps spécifié. Pour plus d'informations sur la configuration des critères de recherche de séries de temporelles, voir **Présentation des graphiques de série temporelle**.

Une fois un graphique configuré, vos configurations de graphique sont conservées lorsque vous:

- Modifiez votre vue dans la zone de liste **Display**.
- Appliquez un filtre.
- Sauvegardez 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 succursale.
- Sauvegardez les résultats de votre recherche.

Remarque : Si vous utilisez le navigateur Web Mozilla Firefox et qu'une extension de blocage de fenêtres publicitaires est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer le bloqueur de publicités du navigateur. Pour plus d'informations, voir la documentation de votre navigateur.

Présentation des graphiques de série temporelle

Les graphiques de séries temporelles sont des représentations graphiques de l'activité de votre journal ou de votre réseau dans le temps. Les sommets et les creux correspondent aux volumes d'activité élevés et faibles. Les graphiques de série temporelle sont utiles pour l'analyse des tendances de données à court et à long terme. À l'aide de graphiques de série temporelle, vous pouvez accéder, naviguer et enquêter sur l'activité du journal ou du réseau de divers points de vue et perspectives.

Remarque : Vous devez avoir les droits de rôle appropriés pour gérer et afficher les graphiques des séries temporelles. Pour plus d'informations sur les droites de rôle, consultez le guide d'administration *IBM Security QRadar SIEM.*

Pour afficher les graphiques de séries temporelles, vous devez créer et sauvegarder une recherche qui comprend les séries temporelles et les options de groupement. QRadar SIEM prend en charge jusqu'à 100 recherches de séries temporelles. QRadar SIEM comprend les recherches enregistrées des séries temporelles par défaut, auxquelles vous pouvez accéder dans la liste des recherches disponibles de la page de recherche d'événements ou de flux. Vous pouvez facilement identifier les recherches de séries temporelles enregistrées dans le menu **Quick Searches** car 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 aux 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 balayer une ligne de temps sur un graphique de série temporelle pour étudier l'activité du journal ou du réseau. Le tableau suivant fournit des fonctions vous permettant d'afficher des graphiques de série temporelle :

Tableau 6-1 Fonctions de graphiques de série temporelle

Fonction	Description
Affichez 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 et ensuite utilisez la roulette de votre souris pour agrandir le graphique (rouler la roulette de la souris vers le haut). • Mettez en évidence la zone du graphique que vous souhaitez agrandir. Lorsque vous relâchez le bouton de la souris, le graphique affiche un segment temporel plus petit. Vous pouvez maintenant cliquer-déplacer le graphique pour l'analyser. Lorsque vous agrandissez le graphique de séries temporelles, le graphique s'actualise pour afficher un segment de temps plus petit
Affichez un intervalle de temps de données plus large	A l'aide de la fonction zoom, vous pouvez rechercher des segments de temps plus larges ou retourner à l'intervalle maximal. Vous pouvez étendre un intervalle de temps en utilisant l'une des options suivantes : • Cliquez sur **Zoom Reset** dans le coin supérieur gauche du graphique. • Placez le pointeur de votre souris sur le graphique, puis utilisez la roulette de votre souris pour agrandir l'affichage (rouler la roulette de la souris vers le bas).
Scan the chart	Lorsque vous avez agrandi un graphique de séries temporelles, vous pouvez cliquer-déplacer le graphique vers la gauche ou vers la droite pour analyser la chronologie.

Légendes des graphiques

Chaque graphique fournit une légende, qui correspond à une référence visuelle pour vous permettre d'associer les objets de graphique aux paramètres qu'ils représentent.

En utilisant la fonctionnalité de la légende, vous pouvez effectuer les actions suivantes :

- Déplacez le pointeur de votre souris sur un élément de légende ou le bloc de couleurs de légende pour afficher plus d'informations sur les paramètres qu'il représente.
- Cliquez avec le bouton droit de la souris sur l'élément de la légende afin d'étudier cet élément. Pour plus d'informations sur les options de menu contextuel, voir **A propos de QRadar SIEM**.
- Cliquez sur un graphique circulaire ou un diagramme à barres pour masquer l'élément dans le graphique. Cliquez de nouveau sur l'élément de légende pour

afficher l'élément masqué. Vous pouvez également cliquer sur l'élément de graphique correspondant pour masquer/afficher l'élément.

- Cliquez sur **Legend**, ou sur la flèche à côté si vous souhaitez supprimer la légende de votre affichage du graphique.

Configuration des graphiques

Vous pouvez utiliser les options de configuration pour modifier le type de graphique, le type d'objet à tracer et le nombre d'objets représentés sur le graphique. Vous pouvez également sélectionner un intervalle pour les graphiques de série temporelle et activer une capture de données de série temporelle

A propos de cette tâche

QRadar SIEM peut accumuler des données de sorte que lorsque vous effectuez une recherche de série temporelle, un cache de données soit disponible à l'affichage des données pour la période précédente. Après avoir activé le paramètre de capture de données de séries temporelles, un astérisque (*) est affiché à côté du paramètre dans la zone de liste **Value to Graph**.

Avant de commencer

Les graphiques ne sont pas affichés lorsque vous affichez des événements ou des flux en temps réel (streaming). Pour afficher des graphiques, vous devez accéder à l'onglet **Log Activity** ou **Network Activity** et choisir l'une des options suivantes :

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

Si vous envisagez de configurer un graphique de série temporelle, assurez-vous que le critère de la recherche enregistrée est groupé et indique un intervalle.

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 suivants :.

Paramètres	Description
Value to Graph	Dans la zone de liste, sélectionnez l'objet que vous souhaitez tracer sur l'axe Y du graphique. Les options comprennent tous les paramètres d'événements normalisés et personnalisés ou de flux inclus dans vos paramètres de recherche.
Display Top	Dans la zone de liste, sélectionnez le nombre d'objets que vous voulez afficher dans le graphique. La valeur par défaut est 10.. Si plus de 10 éléments sont tracés, vos données risquent d'être illisibles.

Paramètres	Description
Chart Type	Dans la zone de liste, sélectionnez le type de graphique que vous souhaitez afficher. Si votre graphique à barre, circulaire ou tableau repose sur des critères de recherche enregistrés avec un intervalle de plus d'une heure, vous devez cliquer sur Update Details **pour mettre à jour le graphique et remplir les détails d'événement**.
Capture Time Series Data	Sélectionnez cette case pour activer la capture des données de séries temporelles. Lorsque vous cochez cette case, la fonction de graphique commence à accumuler des données pour les graphiques de série temporelle. Cette option est désactivée par défaut. Cette option est uniquement disponible sur les graphiques de série temporelle.
Time Range	Dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez afficher. Cette option est uniquement disponible sur les graphiques de série temporelle.

Etape 4 Si vous avez sélectionné l'option de graphique **Time Series** et 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 flux dans le cas où votre intervalle est supérieur à une 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.

Recherche 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, QRadar SIEM recherche l'ensemble de la base de données pour les événements ou les flux qui correspondent aux critères de recherche. Ce processus peut prendre une longue période selon 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 Quick Filte** (événements) ou **Syntaxe Quick Filte** (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
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** list.
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** options. Vous pouvez sélectionner une recherche enregistrée sur la liste àafficher ou modifier.
Recherche	L'icône **Search** est disponible dans plusieurs volets sur la page de recherche. Vous pouvez cliquer sur **Search** lorsque vous avez fini de configurer la recherche et que vous souhaitez afficher les résultats.
Inclure dans mes recherches rapides	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 **Demande de l'activité du journal** ou **Demande de l'activité du réseau**.
Inclure dans mon tableau de bord	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 de tableau de bord.** ***Remarque :*** *Ce paramètre ne s'affiche que si la recherche est regroupée.*
Définir par défaut	Cette case vous permet de définir cette recherche comme votre recherche par défaut lorsque vous accédez à l'onglet **Log Activity** ou **Network Activity**.
Partager avec tout le monde	Cette case vous permet de partager cette recherche avec tous les autres utilisateurs.
Diffusion temps réel (diffusion)	Cette option vous permet d'afficher des résultats d'evénement ou de flux en mode de diffusion. Pour plus d'informations sur le mode de diffusion, voir **Affichage de répétitions d'événements**. ***Remarque :*** *Quand une diffusion en temps réel (diffusion) est activée, il est impossible de 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.*
Dernier intervalle (actualisation automatique)	Cete 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 prédéfinie 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. Activation de comptages uniques sur des données accumulées qui sont partagées avec beaucoup d'autres recherches et rapports sauvegardés peuvent 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 rapports sauvegardés qui partage 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 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 comprend Device dans le nom de la colonne.
Colonnes disponibles	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
Ajouter et supprimer des icônes de colonne (premier ensemble)	Les premiers ensembles d'icônes vous permettent de personnaliser la liste **Group By**. • **Ajouter colonne** - Sélectionnez une ou plusieurs colonnes dans la liste **Available Columns** et cliquez sur l'icône **Add Column**. • **Suppression de colonne** - Sélectionnez une ou plusieurs colonnes dans la liste **Group By** et cliquez sur l'icône **Remove Column**.
Ajouter et supprimer des icônes de colonne (dernier ensemble)	Les derniers ensembles d'icône vous permettent de personnaliser la liste **Columns**. • **Ajouter colonne** - Sélectionnez une ou plusieurs colonnes dans la liste **Available Columns** et cliquez sur l'icône **Add Column**. • **Suppression de colonne** - Sélectionnez une ou plusieurs colonnes dans la liste **Columns** et cliquez sur l'icône **Remove Column**.
Group By	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-le vers la liste prioritaire en utilisant l'icône **Move Up**. • **Move Down** - Sélectionnez une colonne et déplacez-le vers le bas de la 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 davantage personnaliser 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 de la liste prioritaire en utilisant l'icône **Move Down**. Si le type de colonne est numérique ou est basé sur le 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	Dasn la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez 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, allez à **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 le **Tableau 7-1**.

Etape 5 Dans le volet Time Range, sélectionnez les options pour l'intervalle que vous voulez capturer pour cette recherche. Voir le **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 le **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 voulez pour utiliser 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 sauvegarder les résultats de la recherche lorsqu'elle 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 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)** s'affiche dans le coin supérieur droit.

Lors de l'affichage des résultats de recherche partiels, le moteur de recherche fonctionne en arrière-plan pour effectuer la recherche et actualise les résultats partiels afin de mettre à jour l'affichage.

Lorsque la recherche est terminée, le statut **Completed** s'affiche dans le coin supérieur droit.

Sauvegarder 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 QRadar SIEM, comme les rapports. Les critères de recherche enregistrée n'expirent pas.

A propos de cette tâche

Si vous indiquez un intervalle pour votre recherche, QRadar SIEM ajoute le nom de votre recherche avec l'intervalle spécifié. Par exemple, une recherche enregistrée dénommée Exploits by Source avec un intervalle de temps de 5 minutes -les 5 dernières minutes- devient Exploits by Source - 5 dernières minutes.

Si vous modifiez un ensemble de colonnes dans une recherche précédemment enregistrée et que vous sauvegardez les critères de recherche à l'aide du même nom, les accumulations précédentes pour vous perdez les tableaux de série temporelle.

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 s'affichent.

Etape 3 Cliquez sur **Save Criteria**.

Etape 4 Saisissez les valeurs pour ces paramètres :

Paramètre	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 en savoir plus, voir **Gestion des groupes de recherche**.
Gérer les groupes	Cliquez sur **Manage Groups** pour gérer des groupes de recherche. Pour en savoir plus, voir **Gestion des groupes de recherche**.
Options Timespan :	Sélectionnez l'une des options suivantes : • **Real Time (streaming)** - Sélectionnez cette option pour filtrer vos résultats de recherche en mode de diffusion. Pour plus d'informations sur le mode de diffusion, voir **Affichage des événements** ou **des flux en streaming** • **Last Interval (auto refresh)** - Sélectionnez cette option pour filtrer vous résultats de 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 et, dans cette zone de liste, sélectionnez l'intervalle que souhaiter filtrer. • **Intervalle caractéristique** - Sélectionnez cette option et, à partir de l'agenda, sélectionnez la date et l'intervalle que vous souhaitez filtrer.
Inclure dans mes recherches rapides	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 de tableau de bord**. ***Remarque :*** *Ce paramètre ne s'affiche que si la recherche est regroupée.*

Paramètre	Description
Définir par défaut	Cochez cette case pour définir cette recherche comme votre recherche par défaut lorsque vous accédez à l'onglet **Log Activity** ou **Network Activity**.
Partager avec tout le monde	Cochez cette case pour partager ces critères de recherche avec tous les autres utilisateursQRadar SIEM.

Etape 5 Cliquez sur **OK**.

Recherche 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 dans les pages My Offenses et 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 Les options de recherche de page My Offenses and All Offenses

Options	Description
Group	Cette zone de liste vous permet de sélectionner un groupe de recherche de violation pour afficher 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** list.
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** options. Vous pouvez sélectionner une recherche enregistrée sur la liste à afficher ou 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 pour durant laquelle 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 Les options de recherche de page My Offenses and 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 volet 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.
Offense Id	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
Source IP	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 entre 0 et 10.
Gravité	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 entre 0 et 10.

Tableau 7-2 Les options de recherche de page My Offenses and All Offenses

Options	Description
Crédibilité	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 entre 0 et 10.
Pertinence	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 est entre 0 et 10.
Contient des noms d'utilisateurs	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.
Réseau de la source	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 SIEM - Guide d'administration.*
Low Level Category	Dans la zone de liste, vous pouvez sélectionner la catégorie faible niveau que vous souhaitez rechercher. Pour plus d'informations sur les catégories, voir *IBM Security QRadar SIEM - 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
Close by User	Ce paramètre ne s'affiche que lorsque la case **Closed Offenses** n'est pas cochée dans le volet 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 Les options de recherche de page My Offenses and All Offenses

Options	Description
Reason For Closing	Ce paramètre ne s'affiche que lorsque la case **Closed Offenses** n'est pas cochée dans le volet 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 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

Offense types	Description
Any	Cette option recherche toutes les sources de violation.

Tableau 7-3 Options Offense type (suite)

Offense types	Description
Source IP	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 de haut ou de bas niveau dans les zones de 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. A partir de la zone de liste **Log Source**, sélectionnez la source de journal que vous souhaitez rechercher.
Nom d'hôte	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)

Offense types	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 enregistrée, allez à **Etape 4**.
- Pour créer une nouvelle recherche, allez à **Etape 7**.

Etape 4 Sélectionner une recherche préalablement enregistrée à l'aide de l'une des options suivantes :

- Dans la liste **Available Saved Searches**, sélectionnez la recherche enregistrée que vous voulez charger.
- Dans le champ **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 enregistrée, le volet 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 caractéristique. 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 s'affichent.

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 Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez 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

Sauvegarde des critères de recherche dans l'onglet Offense

Recherche de violations dans 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
Toutes les violations	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 les 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.
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.
Source IP	Dans ce champ, vous pouvez enter 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.
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 entre 0 et 10.
Evénement / Flux	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 incluent : • 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 caractéristique. Voir **Tableau 7-4**.

Etape 6 Dans le volet Column Definition, définissez l'ordre dans lequel vous souhaitez trier les résultats :

a Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez 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

Sauvegarde des critères de recherche dans l'onglet Offense

Recherche de violations dans 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 spécifier 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 comment 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.
Recherche	L'icône **Search** est disponible dans plusieurs volets sur la page de recherche. Vous pouvez cliquer sur **Search** lorsque vous avez fini de configurer 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 Dans 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 Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez trier les résultats de la recherche.

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

Etape 7 Cliquez sur **Search**.

Etape suivante

Sauvegarde des critères de recherche dans l'onglet Offense

Recherche de violations dans 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 caractéristique. Voir **Tableau 7-6**.

Etape 5 Dans le volet Column Definition, définissez l'ordre dans lequel vous souhaitez trier les résultats :

a Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez trier les résultats de la recherche.

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

Etape 6 Cliquez sur **Search**.

Etape suivante

Sauvegarde des critères de recherche dans l'onglet Offense

Sauvegarde 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 d'autres recherches. Les critères de recherche enregistrée n'expirent pas.

Procédure

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

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

Les résultats de la recherche s'affichent.

Etape 3 Cliquez sur **Save Criteria**.

Etape 4 Entrez les valeurs pour les paramètres suivants :

Paramètre	Description
Search Name	Tapez un nom que vous souhaitez attribuer à ces critères de recherche.
Attribuer une recherche au Groupe (s)	Cochez la case pour les groupes auxquels vous souhaitez affecter cette recherche enregistrée. Si vous ne sélectionnez pas un groupe, cette recherche enregistrée est attribuée à l'autre groupe par défaut.
Gérer les groupes	Cliquez sur **Manage Groups** pour gérer des groupes de recherche. Voir **Gestion des groupes de recherche**.

Paramètre	Description
Options Timespan :	Sélectionnez l'une des options suivantes : • **Toutes les violations** - 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.
Définir par défaut	Cochez cette case pour définir cette recherche comme votre recherche par défaut.

Etape 5 Cliquez sur **OK**.

Suppression des critères de recherche

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

A propos de cette tâche

Lorsque vous supprimez une recherche enregistrée, les objets QRadar SIEM associés à la rechercher enregistrée pourraient ne plus fonctionner. Les règles de détection d'anomalies et de rapports sont des objets QRadar SIEM qui utilisent des critères de recherche enregistrés. 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 volet Saved Searches, sélectionnez la recherche dans la zone de liste **Available Saved Searches**.

Etape 4 Cliquez sur **Delete**.

Si les critères de recherche ne sont pas associés à d'autres objetsQRadar SIEM, une fenêtre de confirmation s'affiche. Voir **Etape 5**.

Si les critères de recherche enregistrée sont associés à d'autres QRadar SIEM objets, la fenêtre Delete Saved Search s'affiche. La fenêtre répertorie tous les objets QRadar SIEM qui sont associés à la recherche 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** afin de poursuivre. 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 objetsQRadar SIEM, 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. La recherche de base est relancée lorsque vous désactivez un filtre dans le volet Original Filter.

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

Sauvegarder 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** or **Network Activity** pour afficher des résultats partiels ou complètes.

Sauvegarde 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 recherche, les résultats de la recherche sont disponible 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 basée 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
Indicateurs	Indique qu'une notification par courrier électronique est en attente et s'affiche dès la fin de la recherche.
Utilisateur	Indique le nom de l'utilisateur ayant lancé la recherche.
Nom	Spécifie le nom de la recherche, si la recherche a été enregistrée. Pour plus d'informations sur la sauvegarde d'une recherche, voir **Sauvegarde 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 SIEM - Guide d'administration.*
Statut	Indique l'état 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. 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** - Indique 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 **Contrôle des activités de journal** ou **de réseau**
Taille	Indique la taille du fichier de l'ensemble des résultats de recherche.

La barre d'outils 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** pour lancer une nouvelle 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 recherche sélectionnés. Consultez **Sauvegarde 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 (suite)Manage Search Results

Fonction	Description
View	Dans cette zone de liste, vous pouvez sélectionner les résultats de 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 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 des 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 des groupes de recherche

QRadar SIEM 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 affectées 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 sauvegardée vers 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 sauvegardée 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 sauvegardée vers un autre groupe

Suppression d'un groupe ou d'une recherche sauvegardée 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 le champ **Name**, entrez un seul nom pour le 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 sauvegardée vers 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 sauvegardée dans un groupe

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

A propos de cette tâche

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

Il est impossible de supprimer les groupes suivants de ce 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'ÉVÉNEMENT ET DE FLUX PERSONNALISÉES

Les propriétés d'événements et de flux personnalisées vous permettent de rechercher, d'afficher et de rapporter des informations dans des journaux que QRadar SIEM ne normalise pas ou n'affiche pas en général.

Présentation de la propriété personnalisée

Vous pouvez créer des propriétés d'événement et de flux personnalisées à partir de plusieurs endroits sur les onglets Log Activity ou **Network Activity :**

- **Event details** - Vous pouvez sélectionner un événement depuis l'onglet **Log Activity** pour créer une propriété d'événement personnalisée dérivée de son contenu.
- **Flow details** - Vous pouvez sélectionner un flux à partir de l'onglet **Network Activity** pour créer une propriété de flux dérivée de son contenu.
- **Search page** - Vous pouvez créer et modifier un événement personnalisé ou une propriété dans la page de recherche. Lorsque vous créez une nouvelle propriété personnalisée dans la page de recherche, la propriété n'est pas dérivée d'un événement ou d'un flux particulier ; par conséquent, la fenêtre Custom Property Definition n'est pas préremplie. Vous pouvez copier et coller les informations du contenu depuis une autre source.

Autorisations obligatoires

Pour créer des propriétés, vous devez avoir l'autorisation de **User Defined Event Properties** ou de **User Defined Flow Properties**. Si vous possédez des droits d'administration, vous pouvez également créer et modifier les propriétés personnalisées à partir de l'onglet **Admin.** Cliquez sur **Admin > Data Sources > Custom Event Properties** ou sur **Admin > Data Sources > Custom Flow Properties**. Vérifiez avec votre administrateur pour vous assurer que vous possédez les droits requis. Pour plus d'informations sur les autorisations, consultez le guide d'administration*IBM Security QRadar SIEM*.

Types de propriétés personnalisées

Lorsque vous créez une propriété personnalisée, vous pouvez choisir de créer l'un des types de propriété personnalisée suivants :

- **Regex** - 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 SIEM produit des rapports sur tous les utilisateurs qui modifient les autorisations d'utilisateur sur un serveur Oracle. QRadar SIEM fournit une liste d'utilisateurs et le nombre de fois où ils ont apporté une modification à l'autorisation d'un autre compte. Cependant, en règle générale QRadar SIEM ne peut pas afficher le compte utilisateur courant ou l'autorisation qui a été modifiée. Vous pouvez créer une propriété personnalisée pour extraire ces informations dans les journaux et utiliser ensuite la propriété pour les recherches et les rapports.

L'utilisation de cette fonctionnalité requiert une connaissance avancée des expressions régulières (regex). Regex définit la zone que vous souhaitez définir en tant que 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 personnalisés, conformez-vous aux règles d'expressions régulières tel que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez faire référence aux tutoriels d'expressions régulières 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 sur le flux jusqu'à ce qu'un modèle d'expression régulière corresponde au contenu. Le premier modèle d'expression régulière à correspondre au contenu de l'événement ou du flux détermine les données à extraire.

- **Calculated** - A l'aide des propriétés personnalisées fondées 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 de la propriété personnalisée

Vous pouvez créer, modifier, copier et supprimer des propriétés personnalisées.

Création d'une propriété personnalisée basée sur une expression régulière

Vous pouvez créer une propriété client basée sur une expression régulière afin que les contenus d' événements ou de flux correspondent à une expression régulière.

A propos de cette tâche

Lorsque vous configurez une propriété personnalisée basée sur une expression régulière, les fenêtres Custom Event Property ou Custom Flow Property fournissent les paramètres suivants :

Tableau 8-1 Paramètres de la fenêtre Custom property definition (expression régulière)

Paramètre	Description
Test Field	Indique le contenu qui a été extrait de l'événement ou du flux non normalisé.
Définition de propriété	
Existing Property	Pour sélectionner une propriété existante, sélectionnez cette option et puis sélectionnez un nom de propriété enregistré précédemment dans la zone de liste.
New Property	Pour créer une nouvelle propriété, sélectionnez cette option et entrez un nom unique pour cette propriété personnalisée. Le nouveau nom de propriété ne peut être le nom d'une propriété normalisée, comme Username, *Source IP* ou *Destination IP.*
Optimisez l'analyse syntaxique des règles, des rapports et des recherches	Pour analyser et stocker la propriété lorsque QRadar SIEM reçoit pour la première fois l'événement ou le flux, sélectionnez la case à cocher. Lorsque vous sélectionnez la case à cocher, la propriété ne nécessite pas d'analyse supplémentaire pour les tests de rapports, de recherche ou de règle. Si vous désactivez cette case à cocher, la propriété est analysée à chaque fois qu'un test de rapport, de recherche ou de règle est effectué. Cette option est désactivée par défaut.
Field Type	Dans cette zone de liste, sélectionnez le type de zone. Le type de zone détermine comment la propriété personnalisée s'affiche dans QRadar SIEM et 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 personnalisée.
Définition de l'expression de propriété	
Log Source Type	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 dans la fenêtre Custom Event Property Definition.

Tableau 8-1 Paramètres de la fenêtre Custom property definition (expression régulière) (suite)

Paramètre	Description
Log Source	Dans la zone de liste, sélectionnez la source du journal à laquelle s'applique cette propriété d'événement personnalisé. S'il existe plusieurs sources de journal associées à cet événement, cette zone définit le terme multiples et le nombre de sources du journal. Ce paramètre ne s'affiche que dans la fenêtre Custom Event Property Definition.
Event Name	Pour indiquer un nom d'événement pour lequel vous souhaitez appliquer une propriété personnalisée, sélectionnez cette option. Cliquez sur **Browse** pour accéder au navigateur d'événement et sélectionnez l'identificateur QRadar SIEM (QID) du nom d'événement que vous souhaitez appliquer à cette propriété personnalisée. Cette option est activée par défaut
Category	Pour spécifier une catégorie de de bas niveau pour laquelle s'applique cette propriété personnalisée, sélectionnez cette option. Pour sélectionner une catégorie de bas niveau : **1** Dans la zone de liste **High Level Category** sélectionnez la catégorie de niveau supérieur. La liste **Low Level Category** se met à jour pour inclure uniquement les catégories associées à la catégorie de niveau supérieur sélectionnée. **2** Dans la zone de liste **Low Level Category**, sélectionnez la catégorie de bas niveau à laquelle s'applique cette propriété personnalisée.

Tableau 8-1 Paramètres de la fenêtre Custom property definition (expression régulière) (suite)

Paramètre	Description
RegEx	Entrez l'expression régulière à utiliser pour extraire les données du contenu. Les expressions régulières sont sensibles à la casse. Echantillon 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*$)`** • Entier : **`([-+]?\d*$)`** • Adresse IP : **`(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)`** Par exemple : pour faire correspondre un journal qui ressemble au suivant : **`SEVERITY=43`** Rédigez les expressions régulières comme suit : **`SEVERITY=([-+]?\d*$)`** ***Remarque :*** *Les groupes de capture doivent être mis entre parenthèses.*
Capture Group	Entrez le groupe de capture à utiliser si l'expression régulière contient plusieurs groupes de capture. Les groupes de capture traitent les caractères multiples en tant qu'unité unique. Dans un groupe de capture, les caractères sont regroupés entre parenthèses.
Test	Cliquez sur **Test** pour tester l'expression régulière contre le contenu.
Enabled	Cochez cette case pour activer cette propriété personnalisée. Si vous décochez la case, cette propriété personnalisée ne s'affiche pas dans les filtres de recherche ou les listes de colonnes et la ppropriété n'est pas analysée à partir du contenu. La valeur par défaut est Enabled.

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 affichez des événements ou des flux en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause ce mode.

Etape 3 Cliquez deux fois sur l'événement ou le flux sur lequel vous souhaitez baser la propriété personnalisée.

Etape 4 CCliquez sur **Extract Property**.

Etape 5 IDans le panneau Property Type Selection, sélectionnez l'option **Regex Based** option.

Etape 6 Configurez les paramètres de propriété personnaliséeVoir **Tableau 8-1**.

Etape 7 Cliquez sur **Test** pour tester les expressions régulières par rapport au contenu.

Etape 8 Cliquez sur **Save**.

Résultats

La propriété personnalisée s'affiche en tant qu'option dans la liste des colonnes sur la page de recherche. Pour inclure une propriété personnalisée dans une liste d'événements ou de flux, vous devez sélectionner la propriété personnalisée dans la liste des colonnes disponibles lors de la création d'une recherche.

Création d'une propriété personnalisée basée sur un calcul

Vous pouvez créer une propriété personnalisée basée sur le calcul afin que les contenus d'événements ou de flux correspondent à une expression régulière.

A propos de cette tâche

Lorsque vous configurez une propriété personnalisée basée sur un calcul, les fenêtres Custom Event Property ou Custom Flow Property fournissent les paramètres suivants :

Tableau 8-2 Paramètres de la fenêtre Custom property definition (calcul)

Paramètre	Description
Property Definition	
Property Name	Entrez un nom unique pour cette propriété personnalisée. Le nouveau nom de propriété ne peut être le nom d'une propriété normalisée, comme *Username*, Source IP ou *Destination IP.*
Description	Entrez une description pour cette propriété personnalisée.
Définition de calcul de propriété	
Property 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 personnalisés et normalisés numériques. Vous pouvez également indiquer les valeurs numériques spécifiques. 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 Paramètres de la fenêtre Custom property definition (calcul) (suite)

Paramètre	Description
Operator	Dans la zone de liste, sélectionnez l'opérateur que vous souhaitez appliquer aux propriétés sélectionnées dans le calcul. Les options comprennent : • 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 personnalisés et normalisés numériques. Vous pouvez également indiquer les valeurs numériques spécifiques. Dans la zone de liste **Property 1**, sélectionnez l'option **User Defined**. Le paramètre **Numeric Property** s'affiche. Entrez une valeur numérique spécifique.
Enabled	Cochez cette case pour activer cette propriété personnalisée. Si vous décochez la case, cette propriété personnalisée ne s'affiche pas dans les filtres de recherche d'événement ou de flux ou les listes de colonnes et la propriété d'événement ou de flux n'est pas analysée à partir du contenu. La valeur par défaut est Enabled.

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 affichez des événements ou des flux en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause ce mode.

Etape 3 Cliquez deux fois sur l'événement ou le flux sur lequel vous souhaitez baser la propriété personnalisée.

Etape 4 CCliquez sur **Extract Property**.

Etape 5 Dans le panneau In the Property Type Selection, sélectionnez l'option**Calculation Based**.

Etape 6 Configurez les paramètres de propriété personnaliséeVoir **Tableau 8-2**.

Etape 7 Cliquez sur **Save**.

Résultats

La propriété personnalisée s'affiche en tant qu'option dans la liste des colonnes sur la page de recherche.Pour inclure une propriété personnalisée dans une liste d'événements ou de flux, vous devez sélectionner la propriété de personnalisée dans la liste des colonnes disponibles lors de la création d'une recherche.

Modification d'une propriété personnalisée

Les fenêtres Custom Event Properties ou Custom Flow Properties permettent de modifier une propriété personnalisée.

A propos de cette tâche

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

Tableau 8-3 Colonnes de la fenêtre Custom properties

Colonne	Description
Property Name	Indique un seul nom pour cette propriété personnalisée
Type	Indique le type de cette propriété personnalisée Les options comprennent : • **Regex** - Une propriété personnalisée basée sur une expression régulière correspond à des contenus d'événements ou de flux d'une expression régulière. Voir **Création d'une propriété personnalisée basée sur une expression régulière** • **Calculated** - Une propriété personnalisée basée sur le calcul effectue un calcul sur les propriétés de l'événement ou du flux. Voir **Création d'une propriété personnalisée basée sur un calcul**.
Property Description	Indique une description de cette propriété personnalisée
Log Source Type	Indique le nom du type de source de journal auquel s'applique cette propriété personnalisée. Cette colonne ne s'affiche que dans la fenêtre Custom Event Properties.
Log Source	Indique la source de journal à laquelle s'applique cette propriété personnalisée. S'il existe plusieurs sources de journal associées à cet événement ou à ce flux, cette zone spécifie le terme Multiple et le nombre de sources du journal. Cette colonne ne s'affiche que dans la fenêtre Custom Event Properties.
Expression	Indique l'expression de cette propriété personnalisée L'expression dépend du type de propriété personnalisée : • Pour une propriété personnalisée basée sur les expressions régulières, ce paramètre définit l'expression régulière à utiliser pour extraire les données du contenu. • Pour une propriété personnalisée basée sur le calcul, ce paramètre spécifie le calcul que vous souhaitez utiliser pour créer une valeur de propriété personnalisée.
Username	Indique le nom de l'utilisateur qui a créé cette propriété personnalisée.
Enabled	Indique si cette propriété personnalisée est activée. Cette zone indique True ou False.
Creation Date	Indique la date de cette propriété personnalisée

Tableau 8-3 Colonnes de la fenêtre Custom properties (suite)

Colonne	Description
Modification Date	Indique la date de la dernière modification de la propriété personnalisée.

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

Tableau 8-4 Options de la barre d'outils Custom property

Option	Description
Add	Cliquez sur **Add** pour ajouter une nouvelle propriété personnalisée. Voir **Création d'une propriété personnalisée basée sur une expression régulière** ou **Création d'une propriété personnalisée basée sur un calcul**.
Edit	Cliquez sur **Edit** pour éditer la propriété personnalisée sélectionnée. Voir **Modification d'une propriété personnalisée**.
Copy	Cliquez sur **Copy** pour copier les propriétés personnalisées sélectionnées.
Delete	Cliquez sur **Delete** pour supprimer les propriétés personnalisées sélectionnées.
Enable/Disable	Cliquez sur **Enable/Disable** pour activer ou désactiver les propriétés personnalisées sélectionnées pour l'analyse syntaxique et l'affichage des filtres de recherche ou des listes de colonne.

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 personnalisée que vous souhaitez modifier, puis cliquez sur **Edit**.

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

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

Etape 7 Cliquez sur **Save**.

Copie d'une propriété personnalisée

Pour créer une nouvelle propriété personnalisée basée une propriété personnalisée existante, vous pouvez copier la ppropriété personnalisée existante et 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 personnalisée que vous souhaitez copier, puis cliquez sur **Copy**.

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

Etape 6 Modifiez les paramètres nécessaires. Voir **Tableau 8-1**.

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

Etape 8 Cliquez sur **Save**.

Suppression d'une propriété personnalisée

Vous pouvez supprimer n'importe quelle propriété personnalisée pourvu qu'elle ne soit pas associée à une autre propriété personnalisée.

A propos de cette tâche

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

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 personnalisée que vous souhaitez supprimer, puis cliquez sur **Delete**.

Etape 5 Cliquez sur **Yes**.

9 GESTION DES RÈGLES

Dans les onglets **Log Activity**, **Network Activity**, and **Offenses**, vous pouvez afficher et conserver les règles. Cette rubrique s'applique aux utilisateurs qui disposent de droits utilisateur **View Custom Rules** ou **Maintain Custom Rules.**

Pris en compte des droits de règle

Vous pouvez afficher et gérer des règles pour des zones de réseau auquelles vous pouvez accéder si vous avez les autorisations de rôle suivantes :

- Afficher des règles personnalisées
- Conserver des règles personnalisées

Pour créer des règles de détection d'anomalies, vous devez disposer d'une autorisation de **Conservation de règles personnalisées** pour l'onglet sur lequel vous souhaitez créer la règle. Par exemple, pour pouvoir créer une règle de détection d'anomalies sur l'onglet Log Activity, vous devez disposer de **Log Activity > Maintain Custom Rule**.

Pour plus d'informations sur les autorisations de rôle de l'utilisateur, voir *IBM Security QRadar SIEM -Guide d'administration.*

Présentation des règles

Les règles effectuent des tests sur les événements,les flux, ou les violations, et si les conditions d'un test sont satisfaits, la règle génère une réponse. Pour obtenir une liste complète des règles par défaut, voir*IBM Security QRadar SIEM - Guide 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 une nouvelle règle est ajoutée, modifiée ou supprimée. Si une règle qui est référencé par une autre règle est supprimée ou désactivée, un message d'avertissement est affiché et aucune mesure n'est prise.

Catégories de règles

Les deux catégories de règles sont les suivantes :

- **Custom Rules** - Les règles personnalisées effectuent des tests sur les événements, les flux et 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 dans votre réseau.

Types de règles

Les règles personnalisées incluent les types de règles suivants :

- **Event Rule** -Une règle d'événement effectue des tests sur les événements au fur et à mesure qu'ils sont traités en temps réel par le processeur d'événements. Vous pouvez créer une règle d'événement pour détecter un événement unique (au sein de certaines propriétés) ou des séquences d'événements. Par exemple, si vous souhaitez surveiller votre réseau contre les tentatives de connexion infructueuses, accéder à des hôtes multiples, ou une reconnaissance d'événement suivi par un exploit, vous pouvez créer une règle d'événement. C'est commun pour les règles d'événement de créer des violations comme une réponse.
- **Flow Rule** - Les règles de flux Rule - Une règle de flux effectue des tests sur les flux comme s'ils sont traités en temps réel par leCollecteur QFlow. Vous pouvez créer une règle de flux pour détecter un événement unique (au sein de certaines propriétés) ou des séquences de flux. C'est commun pour les règles de flux de créer des violations comme une réponse.
- **Common Rule** - Une règle commune effectuent des tests sur les zones qui sont communes aux deux enregistrements de flux et d'événements. Par exemple vous pouvez créer une règle commune qui détecte les événements et les flux qui ont une adresse IP source spécifique. C'est commun pour les règles communes de créer des violations comme une réponse.
- **Offense Rule** - Une règle de violation traite les violations uniquement lorsque des modifications sont apportées à la violation, comme, lorsque les nouveaux événements sont ajoutés ou le système planifie la violation pour une réévaluation. Il est fréquent que les règles de la violation envoient 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 dans votre réseau. Cette catégorie de règle inclut les types de règles suivantes :

- **Anomaly** - Une règle d'anomalie teste le trafic des flux pour une activité anormale,telle qu'un trafic existant ou inconnu, qui cesse brusquement ou une variation en pourcentage dans le temps est un objet actif. Par exemple, vous pouvez créer une règle d'anomalie pour comparer le volume moyen du trafic des cinq dernières minutes avec le volume moyen du trafic sur la dernière heure. S'il existe plus d'un changement de 40%, la règle génère une réponse.
- **Threshold** - Une règle du seuil teste les événements et le flux de l'activité qui est inférieure, égale ou supérieure à un seuil défini, à l'intérieur ou une plage spécifiée. Un seuil peut être basé sur n'importe quelles données collectées par QRadar SIEM. 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 client entre 08h00 et 17h00, les règles génèrent une alerte lorsque 221 clients tentent de se connecter. La règle du seuil génère un alerte lorsque le 221ème client tente de se connecter.

- **Behavioral** - 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. 410Par exemple, si un serveur de message communique +-typiquement avec 100 hôtes par seconde à minuit et qu'ensuite il commence à communiquer avec 1000 hôtes par seconde, une règle comportementale génère une alerte.

Conditions des règles

Chaque règle peut contenir les composants suivants :

- **Functions -** Avec des fonctions, 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 la fonction **Lorsqu'un événement correspond à l'une des 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 les serveurs de messagerie d'une autre règle. Les blocs de construction par défaut sont fournis à titre indicatif, qui devraient être revus et modifiés en fonction des besoins de votre réseau. Pour obtenir une liste complète des éléments structurants, voir*IBM Security QRadar SIEM - 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, consulter **Tests de règle.**

Réponses des règles

Lorsque vous répondez aux besoins des conditions de règle, une règle peut générer une ou plusieurs des réponses suivantes :

- Création d'une violation.
- Envoi d'un e-mail.
- Génération de notifications de système à l'aide de la fonction Dashboard.
- Ajout de données aux ensembles de références. Pour plus d'informations sur les ensembles de références, voir *IBM Security QRadar SIEM - Guide d'administration.*

- Ajout de données aux collections de données de référence pouvant être utilisées dans les tests de règle. Avant de pouvoir configurer pour envoyer des données vers une collection de données de référence, vous devez créer la collection de données de référence à l'aide de la commande CLI. Pour d'informations sur la création et l'utilisation des collections de données de référence, voir*IBM Security QRadar - Reference Data Collections* technical note.

  Grâce à cette option, vous pouvez ajouter des données aux types de collection suivants :

  - **Reference Map** - Dans une carte de référence, les données sont stockées dans des enregistrements qui mappent une clé à une valeur. Par exemple, pour corréler 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 de l'utilisateur en tant que valeur.
  - **Reference Map of Sets** - Dans une carte de référence d'ensembles, les données sont stockées dans les enregistrements qui mappent une clé à des valeurs multiples. Par exemple tester l'accès autorisé à un brevet, vous pouvez créer une cartes d'ensembles qui utilise une propriété d'événements personnalisés pour l'ID de Brevet en tant que clé et le paramètre **Username** en tant que valeur permettant de remplir une liste d'utilisateurs autorisés.
  - **Reference Map of Maps** - Dans un Map de référence des Maps, les données des enregistrées qui mappent une clé vers une autre,qui est à son tour mappé vers une valeur unique. Par exemple, pour tester des violations de bande passante du réseau, vous pouvez créer un Map des Maps qui utilisent la paramètre **Source IP** en tant que première clé, le paramètre **Application** en tant que seconde clé et le paramètre **Total Bytes** en tant que valeur.
- Génération d'une réponse sur 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'utilisation de l'Assistant des Règles, vous pouvez configurer des règles pour générer un fichier syslog.
  - **Forwarding Destinations** - Une règle peut transmettre les données brutes provenant de sources de journal et de données d'événement normalisées à un ou plusieurs systèmes de fournisseur, tels que des systèmes de billetterie ou d'alerte.
  - **Simple Network Management Protocol (SNMP)** - Le protocole SNMP permet QRadar SIEM d'envoyer des notifications d'événements, de flux, et de violation à un autre hôte pour être stockés. Grâce à l'Assistant des Règles, vous pouvez configurer des règles pour génèrer une réponse qui envoie des messages d'alerte SNMP à l'hôte configuré.
  - **Interface For Metadata Access Points (IF-MAP)** - La règle de réponse Interface For Metadata Access Points (IF-MAP) active la règle pour publier

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

Affichage des règles

Vous pouvez afficher les détails d'une règle, notamment les tests, les éléments structurants et les réponses.

Avant de commencer

Selon votre autorisation de rôle utilisateur, vous pouvez accéder à la page des règles à partir des onglets **Offenses**, **Log Activity** ou **Network Activity**. Pour plus d'informations sur les autorisations de rôle, consultez le Manuel d'administration *IBM Security QRadar SIEM.*

A propos de cette tâche

La page Règles affiche une liste de règles avec les paramètres auxquels elle estassociée. Pour plus d'informations sur les paramètres affichés pour chaque règle listée sur la pageRègles, voir **Tableau 9-1**.

Pour rechercher la règle dont vous souhaitez ouvrir et afficher les détails, vous pouvez utiliser la zone de liste **Group** ou le champ**Search Rules** dans la barre d'outils. Pour plus d'informations sur la barre d'outils de la page Règles, voir **Tableau 9-2**.

Procédure

Etape 1 Sélectionnez l'une des options suivantes :

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

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 disposez de l'autorisation **View Custom Rules** et que vous ne disposez pas de l'autorisation **Maintain Custom Rules**, la page de synthèse Règle s'affiche et la règle ne peut pas être éditée.

Si vous disposez de l'autorisation **Maintain Custom Rules**, la page Rule Test Stack Editor s'affiche. Vous pouvez revoir et éditer les détails de la règle. Voir **Edition d'une règle**.

Création d'une règle personnalisée

QRadar SIEM fournit des règles par défaut, cependant, vous pouvez créer de nouvelles règles pour répondre aux besoins de déploiement.

A propos de cette tâche

Pour créer une nouvelle règle, vous devez disposer de l'autorisation**Offenses > Maintain Custom Rules**.

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 **Actions**, sélectionnez l'une des options suivantes :

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

Etape 4 Lisez le texte introductif sur l'Assistant Règle. Cliquez sur **Next**.

Vous êtes invité à choisir la source à partir de laquelle vous voulez que cette règle s'applique. Le type règle par défaut est celui que vous avez sélectionné dans **Etape 3**. Vous n'avez qu'à choisir une source sur cette page si vous avez besoin de modifier votre sélection.

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

Etape 6 Dans le champ **enter rule name here** du panneau Règle, entrez un nom unique vous souhaitez affecter à cette règle.

Etape 7 Dans la zone de liste, cochez la case pour soit tester la règle localement ou globalement :

- **Local** - Cette règle est tester sur le processeur d'événement local et non partagé avec le système. La valeur configurée par défaut est le Local.
- **Global** - La règle est partagée et testée par n'importe quel processeur d'événement sur le système. Les règles globales envoient des événements et des flux au processeur central de l'événement, ce qui peut réduire les performances sur le processeur de l'événement central.

Etape 8 Ajout d'un ou de plusieurs tests à une règle :

a Facultatif. Pour filtrer les options dans la zone de liste **Test Group**, entrez le texte que vous souhaitez filtrer dans le champ **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 auquel vous souhaitez ajouter la règle, sélectionnez le signe**+** qui se trouve à côté du test.

d Facultatif. Pour identifier un test comme test exclus, cliquez sur**et** au début du test dans le panneau Règle. Le **et** est displayed as **et non.**

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

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

Etape 9 Pour exporter la règle configurée en tant qu'éléments structurants à utiliser avec d'autres règles :

a Cliquez sur **Export as Building Block**.

b Tapez un nom unique pour ce bloc de construction.

c Cliquez sur **Save**.

Etape 10 Dans le volet Groupes, 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 dont vous souhaitez que cette règle génère. Sélectionnez l'une des options suivantes :

- Pour configurer des réponses à une règle d'événement, une règle de flux ou une Règle commune, voir **Tableau 9-3**.
- Pour configurer des réponses à une règle de violation, voir **Tableau 9-4**.

Etape 13 Cliquez sur **Next**.

Etape 14 Revoir la page Rule Summary pour s'assurer que les paramètres sont corrects. Marquez les changements si nécessaire puis cliquez sur **Finish**.

Création d'une règle de détection d'anomalies

L'assistant de règle de détection d'anomalie permet de créer des règles qui appliquent des critères en utilisant des tests de Données et de Temps.

Avant de commencer

Pour créer une nouvelle règle de détection d'anomalie, vous devez répondre aux besoins suivants :

- Obtenir le droit Maintain Custom Rules.
- Effectuez une recherche groupée.

Les options de détection d'anomalies sont affiché une fois que vous effectuez une recherche groupée et que vous sauvegardez les critères de recherche.

A propos de cette tâche

Vous devez disposez de l'autorisation de rôle appropriée pour être en mesure de créer une règle de détection d'anomalies :

- Pour créer des règles de détection d'anomalies dans l'onglet **Log Activity**, vous devez disposer de l'autorisation de rôle **Log Activity > Maintain Custom Rules**

- Pour créer des règles de détection d'anomalies dans l'onglet **Log Activity**, vous devez disposer de l'autorisation de rôle **Network > Maintain Custom Rules**

Les règles de détection d'anomalies utilisent tous les critères de regroupement et de filtrage dans les critères de recherche sauvegardés sur lesquels la règle est basée mais n'utilisent pas n'importe quelle plage d'horaire dans les critères de recherche.

Lorsque vous créez une règle de détection d'anomalies, la règle est remplie par 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 des tests de la propriété Cumulés doit être inclus dans l'empilement 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. Ceci cause une détection d'anomalies permettant de tester la propriété accumulée sélectionnée séparément pour chaque événement ou groupe de flux. Par exemple, si la valeur accumulée sélectionnée est **UniqueCount(sourceIP)**, la règle teste chaque adresse IP source pour chaque groupe d'événements ou de 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 avez sélectionnée pour la zone 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. Placez le pointeur de votre souris sur le texte pour afficher tous les groupes.

Procédure

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

Etape 2 Effectuez une recherche.

Etape 3 Dans le 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. Le type de règle par défaut est celui que vous avez sélectionné dans **Etape 3**. Vous n'avez qu'à choisir une source sur cette page si vous avez besoin de modifier 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 souhaitez filtrer dans le champ **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 auquel vous souhaitez ajouter la règle, sélectionnez le signe**+** qui se trouve à côté du test.

d Facultatif. Pour identifier un test comme test exclus, cliquez sur **et** au début du test dans le panneau Rule. Le **et** s'affiche comme **et non**.

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

f Dans 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 **[Selected Accumulated Property] de chaque [groupe] séparément**.

Etape 9 Dans le panneau Groupes, sélectionnez les cases des groupes auxquels vous souhaitez affecter cette règle. Pour plus d'informations sur le groupement de règles, consultez **Gestion d'un groupe de règles**.

Etape 10 Dans le champ **Notes**, entrez les notes que vous souhaitez inclure à cette règle. Cliquez sur **Next**.

Etape 11 Sur la page Rule Responses, configurez les réponses dont vous souhaitez que cette règle génère. Voir **Tableau 9-5**.

Etape 12 Cliquez sur **Next**.

Etape 13 Revoir la règle configurée. Cliquez sur **Finish**.

Tâches de gestion des règles

Vous pouvez gérer des règles d'anomalies et des règles personnalisées. Vous pouvez activer ou désactiver les règles comme requis. Vous pouvez également éditer, copier ou supprimer une règle.

Remarque : La fonction anomaly detection figurant dans les onglets **Le journal Activité** et **Network Activity** permet de créer des règles de détection d'anomalies. Pour gèrer des règles de détection d'anomalies par défaut ou précédemment créées, vous devez utiliser la page Rules dans l'onglet **Offenses**.

Activation/ désactivation des règles

Lors du réglage de votre système, vous pouvez activer ou désactiver les règles appropriées pour vous assurer que votre système génères des violations importantes pour votre environnement.

A propos de cette tâche

Pour pouvoir activer ou désactivier une règle, vous devez disposer d'une autorisation de rôle **Offenses > Maintain Custom Rules**.

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** de la page Rules, sélectionnez **Rules**.

Etape 4 Sélectionnez la règle que vous souhaiter activer ou désactiver.

Etape 5 Dans la zone de liste **Actions**, sélectionnez **Enable/Disable**.

Modification 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

Pour pouvoir éditer une règle, vous devez disposer de l'autorisation de rôle **Offenses > Maintain Custom Rules**.

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** de la page Rules, sélectionnez **Rules**.

Etape 4 Cliquez deux fois sur la règle que vous souhaitez éditer.

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

Etape 6 Facultatif. Si vous voulez modifier 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 **Tableau 9-1**.

Etape 8 Cliquez sur **Next**.

Etape 9 Sur la page Rule Response, éditez les paramètres :

- Voir **Tableau 9-3** pour obtenir l'événement, le flux ou les réponses de règles communes.
- Voir **Tableau 9-4** pour les réponses à la règle de la violation.
- Voir **Tableau 9-5** pour les réponses à la règle de détection d'anomalies responses.

Etape 10 Cliquez sur **Next**.

Etape 11 Revoir la règle configurée. Cliquez sur **Finish**.

Copie d'une règle

Pour créer une nouvelle règle, vous pouvez copier une règle existante, entrez un nouveau nom pour la règle, puis personnaliser les paramètres de la nouvelle règle selon les besoins..

A propos de cette tâche

Pour pouvoir copier une règle, vous devez disposer de l'autorisation de rôle **Offenses > Maintain Custom Rules**.

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 le champ **Enter name for the copied rule**, entrez un nom pour la nouvelle règle. Cliquez sur **OK**.

Suppression d'une règle

QRadar SIEM vous permet de supprimer la a règle de votre système.

A propos de cette tâche

Pour pouvoir supprimer une règle, vous devez disposer de l'autorisation de rôle **Offenses > Maintain Custom Rules**.

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 d'un 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 les éléments structurants de vos groupes vous permet d'afficher avec et de surveiller efficacementvos règles. Par exemple, vous pouvez afficher toutes les règles relatives au respect des règles.

Les règles une fois créées peuvent être affectées à un groupe existant. Pour plus d'informations sur l'affectation d'une règle à un groupe à l'aide de l'assistant de règles, voir **Création d'une règle personnalisée** ou **Création d'une règle de détection d'anomalies**.

Affichage d'un groupe de règles

Sur la page Rules, vous pouvez filtrer les règles et blocs de construction pour n'afficher uniquement que les règles et blocs de construction appartenant à un groupe spécifique.

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**, choisissez si vous souhaitez afficher les règles ou les éléments structurants.

Etape 4 Dans la zone de liste **Filter**, sélectionnez la catégorie que vous souhaitez afficher.

Résultat

La liste des éléments affectés à ce groupe s'affiche.

Création d'un groupe

La page Rules prévoit un groupe de règles par défauts. 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 pour les paramètres suivants :

- **Nom** - 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 navigation.

Etape 9 Fermez la fenêtre des Groupes.

Affectation d'un élément à un groupe

Vous pouvez affecter à un groupe une règle sélectionnée ou deséléments structurants.

Procédure

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

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

Etape 3 Sélectionnez la règle ou le bloc de construction que vous voulez affecter à un groupe.

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

Etape 5 Cochez la case du groupe auquel vous souhaitez affecter la règle ou le bloc de construction.

Etape 6 Cliquez sur **Assign Groups**.

Etape 7 Fermer la fenêtre Choisir groupes.

Modification d'un groupe

Vous pouvez éditer un nom de groupe pour modifier un nom ou une 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 éditer.

Etape 5 Cliquez sur **Edit**.

Etape 6 Mettez à jour les valeurs pour les paramètres suivants :

- **Nom** - 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 modifier l'emplacement d'un groupe, cliquez sur le nouveau groupe et glissez le dossier vers le nouvel emplacement dans votre arborescence de navigation.

Etape 9 Fermer la fenêtre des Groupes.

Copie d'un élément vers un autre groupe

En utilisant la fonctionnalité des groupes, vous pouvez copier une règle ou des éléments structurants d'un groupe vers d'autres roupes.

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 sur lequel vous souhaitez copier la règle ou le bloc de construction.

Etape 7 Cliquez sur **Copy**.

Etape 8 Fermez la fenêtre des Groupes.

Suppression d'un élément d'un groupe

Vous pouvez supprimer un élément d'un groupe. Lorsque supprimez un élément d'un groupe, seule la règle ou les éléments structurants sont supprimés du groupe. Ils restent disponible 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 des Groupes.

Suppression d'un groupe

Vous pouvez supprimer un groupe. Lorsque vous supprimez un groupe, les règles ou les éléments structurants de ce groupe demeurentdisponibles sur la page Règles.

Procédure

Etape 1 Cliquez sur l'ongletOffense.

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.

Modification d'éléments structurants

QRadar SIEM inclut un ensemble d'éléments structurants que vous pouvez éditer pour correspondre aux besoins de votre déploiement.

A propos de cette tâche

Un élément structurant est une pile de test de rôle réutilisable que vous pouvez inclure en tant que composant dans d'autres règles.

PFar exemple, vous pouvez éditer l'élément structurant BB:HostDefinition: Mail Servers pour identifier tous les serveurs de messagerie dans votre déploiement. Ensuite, vous pouvez configurer toute règle permettant d'exclure vos serveurs de messagerie des tests de règles.

Pour plus d'informations concernant les blocs de construction par défaut, consultez *IBM Security QRadar SIEM - Guide d'administration.*

Procédure

Etape 1 Cliquez sur l'ongletOffenses.

Etape 2 Dans le menu de 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 Continuer 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 s'affiche fournissant pour chaque règle les informations suivantes :

Tableau 9-1 Rules page paramètres

Paramètre	Description
Rule Name	Affiche le nom de la règle.
Group	Affiche le groupe auquel cette règle est affectée. Pour plus d'informations sur groupes,consultez **Gestion d'un groupe de règles**.
Rule Category	Affiche la catégorie de règle pour 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, consultez **Types de règles**.
Enabled	Indique si la règle est activée ou pas. Pour plus d'informations sur activer ou désactiver les règles, consultez **Activation/ désactivation des règles**.
Response	Affiche la response de règle, s'il en existe une. réponse à la règle inclut : • Dispatch New Event • Email • Log • Notification • SNMP • Reference Set • Reference Data • IF-MAP Response Pour plus d'informations sur les réponses de règles, consultez **Réponses des règles**.
Event/Flow Count	Affiche le nombre d'événements ou de flux associés à cette règle lorsque cette dernière contribue à une violation.
Nombre de violations	Affiche le nombre de violations générées par cette règle.

Tableau 9-1 Rules page paramètres (suite)

Paramètre	Description
Origine	Indique si cette règle est une règle par défaut (Système) ou une règle personnalisée (Utilisateur).
Date de création	Indiquez la date et l'heure de la création de cette règle.
Date de modification	Indiquez 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 Rules page

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, consultez **Gestion d'un groupe de règles**.
Actions	Cliquez sur **Actions** et sélectionnez l'une des options suivantes : • **New Event Rule** - Sélectionnez cette option pour créer une nouvelle règle d'événement. Consultez **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 des 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**.

Tableau 9-2 Fonction de la barre d'outils Rules page (suite)

Fonction	Description
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.*
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) • Remarques • 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

Le **Tableau 9-3** fournit des paramètres de la page 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 de plus amples informations sur la gravité, consultez 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, consultez 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, consultez le **Glossaire**.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Assurez-vous que l'événement détecté est partie de la «violation»	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 listes, cochez le paramètre sur lequel vous souhaitez indexer la violation. La valeur par défaut est Source IPv6. Pour les règles d'événements, les options incluent l'adresse IP cible, l'adresse IPv6 cible, l'adresse MAC cible, port cible, nom de l'événement, nom d'hôte, journal source, règle, l'adresse IP source, l'adresse IPv6 source, MAC adresse source, port source, ou nom d'utilisateur. Pour les règles de flux,les options incluent l'App ID, l'ASN cible, l'IP adresse cible, l'IP identité cible, port cible nom de l'événement, règle, l'ASN source, l'IP adresse source, l'IP identité source, ou port source. Pour les règles communes, les options incluent l'adresse IP cible, l'identité IP cible, port cible, règle, l'IP adresse source, l'identité IP source et port source. • **Annotate this offense** - Cochez cette case pour ajouter une annotation à cette violation et entrez 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 entrez l'annotation que vous souhaitez ajouter à l'événement.
Supprimez l'événement détecté	Cochez cette case pour forcer l'envoi d'un événement, qui est normalement envoyé au composant Magistrate, à envoyer à la base de données Ariel pour une 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 d' origine ou flux, 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**.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Event Description	Entrez une description de l'événement. La description s'affiche sur le panneau des annotations des détails de l'événement.
Severity	Dans la zone de liste, sélectionnez la gravité de l'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est 0. La gravité s'affiche dans l'Annotation pane des détails de l'événement. Pour de plus amples informations sur la gravité, consultez 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 des annotations des détails de l'événement. Pour plus d'informations sur la crédibilité, consultez 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 des annotations des détails de l'événement. Pour plus d'informations sur la pertinence, consultez le **Glossaire**.
High-Level Category	Dans la zone des liste, sélectionnez la catégorie d'événement de haut niveau que vous avez besoin lors du traitement des événements. Pour plus d'informations sur les categories d'événements, voir *IBM Security QRadar SIEM - Guide d'administration.*
Low-Level Category	Dans la zone de liste, sélectionnez les catégories d'événement de bas niveau dont vous avez besoin lors du traitement des événements. Pour plus d'informations sur les categories d'événements, voir *IBM Security QRadar SIEM - Guide d'administration.*
Annotate this offense	Cochez cette case pour ajouter une annotation à cette violation et entrez l'annotation.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Assurez-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'a été créée l'onglet created on the **Offenses**, créez-en une. 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 listes, cochez le paramètre sur lequel vous souhaitez indexer la violation. La valeur par défaut est source IP. Pour les règles d'événements, les options incluent l'adresse IP cible, l'adresse IPv6 cible, l'adresse MAC cible, port cible, nom de l'événement, nom d'hôte, journal source, règle, l'adresse IP source, l'adresse IPv6 source, MAC adresse source, port source, ou nom d'utilisateur. Pour les règles de flux,les options incluent l'App ID, l'ASN cible, l'IP adresse cible, l'IP identité cible, port cible nom de l'événement, règle, l'ASN source, l'IP adresse source, l'IP identité source, ou port source. Pour les règles communes, les options incluent l'adresse IP cible, l'identité IP cible, port cible, règle, l'IP adresse source, l'identité IP source et port source. • **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 d'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 ne souhaitez pas que les informations sur the Event Name (nom d'événement) contribuent au nom de la violation. Il s'agit de la valeur par défaut.
Email	Cochez cette case pour afficher les options des courriers électroniques. Par défaut, la case est vide.

Tableau 9-3 Paramètres de la page Event/Flow/Common Rule Response (suite)

Paramètre	Description
Saisissez les adresses e-mails à notifier	Entrez l'adresse électronique pour envoyer une notification si cette règle en génère une. Utilisez une virgule pour séparer les adresses électroniques.
Alerte SNMP	Ce paramètre ne s'affiche que lorsque les paramètres SNMP paramètres sont configurés dans les paramètres du système. Pour plus d'informations sur la configuration des paramètres du système, voir *IBM Security QRadar SIEM - Guide d'administration.* ▶ Cochez cette case pour activer cette règle pour envoyer une notification SNMP (trap). La Sortie d'Alerte SNMP incluent l'heure du système,l'OID de l'interruption, et la notification des données, telle que définie par MIB. Q1 Labs Pour plus d'informations sur Q1 Labs MIB, voir *IBM Security QRadar SIEM - 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	Cocher cette case si vous souhaitez enregistrer localement l'événement ou le flux. Par défaut, cette case est désélectionnée. 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 enregistrer un événement ou le transférer à une destination de transfert. Une destination de transfert est un système de fournisseur, tel que SIEM, ticketing, ou les systèmes d'alerte. Lorsque vous cochez cette case, une liste des destinations de renvoi est affichée. Cochez la case du destination de renvoi ou vous souhaiter envoyer ou fluxer 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 du transfert, voir *IBM Security QRadar SIEM - 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 du tableau de bord. Pour plus d'informations sur tableau de bord, consultez l'onglet **Gestion des tableaux 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 les données à l'ensemble de référence : **1** A partir de la zone de liste, sélectionnez les données que vous voulez ajouter. Les options incluent toutes les données normalisées ou personnalisées. **2** A partir de la zone de liste, sélectionnez l'ensemble des références que vous voulez ajouter aux données spécifiées. Les **Add to Reference Set** réponses de règles offrent les fonctions suivantes : • **Refresh** - cliquez sur **Refresh** pour actualiser la première zone de liste afin de s'assurer que la liste est en cours. • **Configure Reference Sets** - Cliquez sur **Configure Reference Sets** pour configurer l'ensemble de la référence. Cette option n'est disponible que lorsque vous disposez d'une autorisation administrative. Pour plus d'informations sur la gestion des ensembles de référence, voir *IBM Security QRadar SIEM- 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 de créer la collection de données de référence à l'aide de la commande CLI. Pour plus d'informations sur la création et l'utilisation de collectes de données de référence, voir *IBM Security QRadar- Reference Data Collections Technical Note*. Cochez cette case si vous souhaitez, à la suite de cette règle, que les événements soient générées pour ajouter une collection de données de référence. Une fois que vous cochez cette case, sélectionnez l'une des options suivantes : • **Add to a Reference Map** - Sélectionnez cette option pour envoyer la collection de données de clé unique/paires de valeurs multiples. Vous devez sélectionner la clé et la valeur pour l'enregistrement de données puis sélectionner la mappe de référence pour ajouter l'enregistrement des données. • **Add to a Reference Map of Sets** - Sélectionnez cette option pour envoyer des données vers collection de clé/paires de valeurs uniques. Vous devez sélectionner la clé et la valeur pour l'enregistrement des données et sélectionner la mappe de référence des ensembles sur lesquels vous souhaitez ajouter l'enregistrement des données. • **Add to a Reference Map of Maps** - Sélectionnez cette option pour envoyer des données vers une collection de clé/paires de valeurs multiples. Vous devez sélectionner une clé pour la première carte, une clé pour la seconde carte puis la valeur pour l'enregistrement des données. Vous devez également sélectionner la carte de référence sur lequel vous souhaitez ajouter l'enregistrement des 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 du l'événement sur le serveur IF-MAP. Pour plus d'informations sur la configuration des paramètres IF-MAP, voir *IBM Security QRadar SIEM- Guide d'administration.*
Response Limiter	Cochez la case et utilisez la zone de liste pour configurer la fréquence pendant laquelle vous voulez que cette règle répond.
Enable Rule	Cochez cette case pour activer cette règle. Par défaut, la case est cochée.

Tableau 9-4 fournit des 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	
Name/Annotate the detected offense	Cochez cette case pour afficher les noms des options.

Tableau 9-4 Paramètres de la page Offense Rule Response (suite)

Paramètre	Description
New Offense Name	Entrez le nom que vous voulez affecter à la violation.
Offense Annotation	Entrez l'annotation du 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 des courriers électroniques. Par défaut, la case est vide.
Saisissez l'adresse e-mail à notifier	Entrez l'adresse électronique pour envoyer une notification si cette règle est générée. Séparez par virgule plusieurs adresses électroniques.
Alerte SNMP	Ce paramètre ne s'affiche que lorsque les paramètres SNMP sont configurés dans les paramètres du système. Pour plus d'informations sur la configuration des paramètres du système, voir *IBM Security QRadar SIEM - Guide d'administration.* ▶ Cochez cette case pour activer cette règle pour envoyer une notification SNMP (trap). La Sortie d'Alerte SNMP incluent l'heure du système,l'OID de l'interruption, et la notification des données, telle que définie par MIB. Q1 Labs Pour plus d'informations sur Q1 Labs MIB, voir *IBM Security QRadar SIEM - 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	Cocher cette case si vous souhaitez enregistrer localement l'événement ou le flux. Par défaut, cette case est désélectionnée. 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**

Tableau 9-4 Paramètres de la page Offense Rule Response (suite)

Paramètre	Description
Send to Forwarding Destinations	Cochez cette case si vous voulez enregistrer un événement ou le transférer à une destination de transfert. Une destination de transfert est un système de fournisseur, tel que SIEM, ticketing, ou les systèmes d'alerte. Lorsque vous cochez cette case, une liste des destinations de renvoi est affichée. Cochez la case du destination de renvoi ou vous souhaiter envoyer ou fluxer 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 du transfert, voir *IBM Security QRadar SIEM - 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 du l'événement sur le serveur IF-MAP. Pour plus d'informations sur la configuration des paramètres IF-MAP, voir *IBM Security QRadar SIEM- Guide d'administration.*
Response Limiter	Sélectionnez cette case et utilisez la liste de zone pour configurer la fréquence avec laquelle vous voulez que cette règle réponde.
Enable Rule	Cochez cette case pour activer cette règle. Par défaut, la case est cochée.

Le **Tableau 9-5** 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	Indiquez que cette règle envoie un nouvel événement en plus d'origine ou de flux, qui est traité comme tous les autres événements dans le système. Par défaut cette case est sélectionnée et ne peut pas être effacée.
Event Name	Entrez un nom unique pour l'événement que vous souhaitez afficher sur l'onglet **Offenses**.
Event Description	Entrez une description de l'événement. La description est affichée dans le Panneau des Annotations des détails de l'événement.

Tableau 9-5 Paramètres de la page Anomaly Detection Rule Response (suite)

Paramètre	Description
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 d'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 ne souhaitez pas que les informations sur the Event Name (nom d'événement) contribuent 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 de 5. La gravité est affichée sur le panneau des annotations des détails d'événement. Pour de plus amples informations sur la gravité, consultez **Glossaire**.
Credibility	Dans la zone de liste, sélectionnez crédibilité d'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 des détails d'événements. Pour plus d'informations sur la crédibilité, consultez le **Glossaire**.
Relevance	Dans la zone de liste, sélectionnez la pertinence d'événement. L'intervalle est compris entre 0 (le plus faible) et 10 (le plus élevé) et la valeur par défaut est de 5. La pertinence s'affiche sur le panneau d'annotations des détails d'événements. Pour plus d'informations sur la pertinence, consultez **Glossaire**.
High Level Category	Dans la zone des liste, sélectionnez la catégorie d'événement de haut niveau que vous avez besoin lors du traitement des événements. Pour plus d'informations sur les categories d'événements, voir *IBM Security QRadar SIEM - Guide d'administration.*
Low Level Category	Dans la zone de liste, sélectionnez les catégories d'événement de bas niveau dont vous avez besoin lors du traitement des événements. Pour plus d'informations sur les categories d'événements, voir *IBM Security QRadar SIEM - Guide d'administration.*
Annotate this offense	Cochez cette case pour ajouter une annotation à cette violation et entrez l'annotation.

Tableau 9-5 Paramètres de la page Anomaly Detection Rule Response (suite)

Paramètre	Description
Assurez-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** - Indiquez 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 tapez le nombre des secondes que vous voulez inclure pour les événements ou les flux détectés de la source sur l'onglet.**Offenses**
Email	Cochez cette case pour afficher les options des courriers électroniques. Par défaut, la case est vide.
Saisissez l'adresse e-mail à notifier	Entrez l'adresse électronique pour envoyer une notification si cette règle en génère une. Utilisez une virgule pour séparer les adresses électroniques.
Alerte SNMP	Ce paramètre ne s'affiche que lorsque les paramètres SNMP sont configurés dans les paramètres du système. Pour plus d'informations sur la configuration des paramètres du système, voir *IBM Security QRadar SIEM - Guide d'administration.* ▶ Cochez cette case pour activer cette règle pour envoyer une notification SNMP (trap). La Sortie d'Alerte SNMP incluent l'heure du système,l'OID de l'interruption, et la notification des données, telle que définie par MIB. Q1 Labs Pour plus d'informations sur Q1 Labs MIB, voir *IBM Security QRadar SIEM - 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 du tableau de bord. Pour plus d'informations sur tableau de bord, consultez l'onglet **Gestion des tableaux 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	Cocher cette case si vous souhaitez enregistrer localement l'événement ou le flux. Par défaut, la case est décochée. 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 les données à l'ensemble de référence : **1** A partir de la zone de liste, sélectionnez les données que vous voulez ajouter. Les options incluent toutes les données normalisées ou personnalisées. **2** A partir de la zone de liste, sélectionnez l'ensemble des références que vous voulez ajouter aux données spécifiées. Les **Add to Reference Set** réponses de règles offrent les fonctions suivantes : • **Refresh** - cliquez sur **Refresh** pour actualiser la première zone de liste afin de s'assurer que la liste est en cours. • **Configure Reference Sets** - Cliquez sur **Configure Reference Sets** pour configurer l'ensemble de la référence. Cette option n'est disponible que lorsque vous disposez d'une autorisation administrative. Pour plus d'informations sur la gestion des ensembles de référence, voir *IBM Security QRadar SIEM- 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 de créer la collection de données de référence à l'aide de la commande CLI. Pour plus d'informations sur la création et l'utilisation de collectes de données de référence, voir *IBM Security QRadar- Reference Data Collections Technical Note*. Cochez cette case si vous souhaitez, à la suite de cette règle, que les événements soient générées pour ajouter une collection de données de référence. Une fois que vous cochez cette case, sélectionnez l'une des options suivantes : • **Add to a Reference Map** - Sélectionnez cette option pour envoyer la collection de données de clé unique/paires de valeurs multiples. Vous devez sélectionner la clé et la valeur pour l'enregistrement de données puis sélectionner la mappe de référence pour ajouter l'enregistrement des données. • **Add to a Reference Map of Sets** - Sélectionnez cette option pour envoyer des données vers collection de clé/paires de valeurs uniques. Vous devez sélectionner la clé et la valeur pour l'enregistrement des données et sélectionner la mappe de référence des ensembles sur lesquels vous souhaitez ajouter l'enregistrement des données. • **Add to a Reference Map of Maps** - Sélectionnez cette option pour envoyer des données vers une collection de clé/paires de valeurs multiples. Vous devez sélectionner une clé pour la première carte, une clé pour la seconde carte puis la valeur pour l'enregistrement des données. Vous devez également sélectionner la carte de référence sur lequel vous souhaitez ajouter l'enregistrement des 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 du l'événement sur le serveur IF-MAP. Pour plus d'informations sur la configuration des paramètres IF-MAP, voir *IBM Security QRadar SIEM- Guide d'administration.*
Response Limiter	Sélectionnez cette case et utilisez la liste de zone pour configurer la fréquence aveclaquelle vous souhaitez que cette règle réponde.
Enable Rule	Cochez cette case pour activer cette règle. Par défaut, la case est cochée.

10 GESTION DES ACTIFS

QRadar SIEM 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. L'onglet **Assets** vous permet de gérer les actifs sur votre réseau.

Présentation de l'onglet Assets

Les profils d'actif fournissent des informations sur chaque actif connu sur votre réseau, y compris les services qui s'exécutent sur chaque actif. Les informations de profil d'actif sont utilisées à des fins de corrélation afin de réduire les faux positifs. Par exemple, si une source tente d'exploiter un service spécifique en cours d'exécution sur un actif, QRadar SIEM peut déterminer si l'actif est vulnérable aux attaques en mettant en corrélation l'attaque avec le profil d'actif.

L'onglet **Assets** vous permet de :

- Rechercher des actifs spécifiques.
- Voir tous les actifs étudiés.
- Afficher les informations d'identité des actifs étudiés.
- Ajouter manuellement les profils d'actif.
- Modifier les profils d'actif pour les actifs ajoutés ou découverts manuellement.
- Ajuster les vulnérabilités de faux positifs.
- Imprimer ou exporter des profils d'actif.

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 de flux, voir *IBM Security QRadar SIEM Administration Guide*.

Détails de vulnérabilité

Les scanners tiers identifient et signalent les vulnérabilités découvertes à QRadar SIEM 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 identificateur 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, consultez le guide d'évaluation de la vulnérabilité *IBM Security QRadar SIEM*.

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.

A l'aide de la fonction de recherche d'actif, vous pouvez rechercher des actifs par références de données externes afin de déterminer si des vulnérabilités connues existent dans votre déploiement.

Par exemple :

Vous recevez une notification indiquant que l'ID CVE : CVE-2010-000 est exploité activement dans la zone. Pour vérifier si des hôtes de votre déploiement sont vulnérables à cette exploitation, vous pouvez entrer `CVE-2010-000` dans le paramètre de recherche **CVE ID** afin d'afficher une liste de tous les hôtes qui sont vulnérables à cet ID CVE spécifique.

Remarque : Pour plus d'informations sur la base de données OSVDB, voir *http://osvdb.org/*. Pour plus d'informations sur la base de données NVDB, voir *http://nvd.nist.gov/*.

Etude des profils d'actifs

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 dans les 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 des actifs à répertorier. Sélectionnez l'une des options suivantes :

- Pour répertorier tous les profils d'actif de votre déploiement, cliquez sur **Show All**.
- Pour répertorier un ensemble défini d'actifs, définissez vos critères de recherche. Voir **Tableau 10-2**.

Etape 3 Facultatif. Pour afficher des informations supplémentaires sur un actif, déplacez votre souris sur l'adresse IP de l'actif à étudier.

Etape 4 Pour afficher la page Asset Profile de l'actif, cliquez deux fois dessus. Voir **Tableau 10-4**.

Etape 5 Facultatif. Pour étudier davantage de données associées, cliquez sur une fonction de barre d'outils dans le panneau Asset Profile. Pour obtenir des descriptions sur les fonctions de la barre d'outils, voir **Tableau 10-8**.

Etape 6 Facultatif. Pour modifier des paramètres 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, cliquez deux fois sur la ligne de la vulnérabilité que vous souhaitez afficher.
- Dans le panneau Ports and Vulnerabilities, cliquez sur le lien dans le paramètre **Name** de la vulnérabilité que vous souhaitez afficher.

  Voir **Paramètres de la fenêtre Review Vulnerability Details**.

Tâches de gestion des profils d'actifs

L'onglet **Assets** vous permet d'ajouter, de modifier, d'importer et d'exporter des profils d'actif.

Ajout d'un profil d'actif

QRadar SIEM détecte et ajoute automatiquement les profils d'actif ; c'est pourquoi il n'est généralement pas nécessaire d'ajouter un profil d'actif. Cependant, vous devez peut-être ajouter manuellement un profil.

A propos de cette tâche

Après avoir ajouté un profil d'actif, vous devez configurer les paramètres suivants :

Table 10-1 Paramètres de la page Add Asset Profile

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	Dans la zone de liste, entrez la pondération à affecter à cet actif. L'intervalle est compris entre 0 et 10. La valeur par défaut est 0.
Business Owner	Entrez le nom du propriétaire fonctionnel de l'actif. Un directeur de service est un exemple de propriétaire fonctionnel. La longueur maximale est de 255 caractères.
Business Owner Contact Info	Entrez les informations de contact du propriétaire fonctionnel. La longueur maximale est de 255 caractères.

Table 10-1 Paramètres de la page Add Asset Profile (suite)

Paramètre	Description
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 des valeurs pour les paramètres. Voir **Table 10-1**.

Etape 5 Cliquez sur **Save**.

Etape suivante

Après avoir ajouté un profil d'actif, vous pouvez modifier le profil pour configurer des paramètres de profil d'actif supplémentaires, tels que les informations sur le propriétaire fonctionnel et sur le système d'exploitation. Voir **Modification d'un actif**.

Modification d'un actif

Vous pouvez modifier un profil d'actif détecté automatiquement 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 des actifs à répertorier. Sélectionnez l'une des options suivantes :

- Pour répertorier tous les profils d'actif de votre déploiement, cliquez sur **Show All**.
- Pour répertorier un ensemble défini d'actifs, définissez vos critères de recherche. Voir **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 Modifiez les paramètres. Voir **Tableau 10-6**.

Etape 7 Cliquez sur **Save Changes**.

Suppression des actifs

Vous pouvez supprimer des actifs spécifiques ou l'ensemble des profils d'actifs.

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 à répertorier. Sélectionnez l'une des options suivantes :

- Pour répertorier tous les profils d'actif de votre déploiement, cliquez sur **Show All**.
- Pour répertorier 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 dans la zone de liste **Actions**.
- Dans la zone de liste **Actions**, sélectionnez **Delete Listed**.

Etape 5 Cliquez sur **OK**.

Importation de profils d'actifs

Vous pouvez importer des informations de profil d'actif dans QRadar SIEM.

Avant de commencer

Le fichier importé doit être un fichier CSV respectant le format suivant :

```
ip,name,weight,description
```

Où :

- **IP** - Indique une adresse IP valide selon la notation décimale à points. Par exemple : 192.168.5.34.
- **Name** - Indique le nom de cet actif pouvant contenir jusqu'à 255 caractères. Les virgules ne sont pas acceptées dans cette zone et invalident le processus d'importation. Par exemple : WebServer01 est correct.
- **Weight** - Indique un nombre compris entre 0 et 10, qui correspond à l'importance de cet actif sur votre réseau. Une valeur égale à 0 représente une importance faible et une valeur égale à 10 une importance très élevée.
- **Description** - Indique une description textuelle de cet actif pouvant contenir jusqu'à 255 caractères. Cette valeur est facultative.

Par exemple, les entrées suivantes peuvent être incluses dans un fichier CSV :

```
192.168.5.34,WebServer01,5,Main Production Web Server
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.

Résultat

Si une erreur se produit pendant le processus d'importation, aucun actif n'est importé.

Exportation des actifs

Vous pouvez exporter des profils d'actif vers un fichier au format Extended Markup Language (XML) ou Comma-Separated Value (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 à répertorier. Sélectionnez l'une des options suivantes :

- Pour répertorier tous les profils d'actif de votre déploiement, cliquez sur **Show All**.
- Pour répertorier un ensemble défini d'actifs, définissez vos critères de recherche. Voir **Tableau 10-2**.

Etape 4 Dans la zone de liste **Actions**, sélectionnez l'une des options suivantes :

- Export to XML
- Export to CSV

Une fenêtre d'état fournit l'état du processus d'exportation.

Etape 5 Facultatif. Si vous souhaitez utiliser d'autres onglets et d'autres pages dans QRadar SIEM lors de l'exportation, cliquez sur le lien **Notify When Done**.

Une fois l'exportation terminée, la fenêtre File Download s'affiche.

Etape 6 Dans la fenêtre File Download, sélectionnez 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 et barre d'outils de l'onglet Assets

Cette rubrique contient des tableaux qui décrivent les paramètres et les barres d'outils affichés sur chaque page de l'onglet **Assets**.

Fonctions de la barre d'outils et des paramètres de la page Asset Profile Search

Le tableau suivant décrit les paramètres de la page Asset Profile Search :

Tableau 10-2 Paramètres Asset Profile Search

Paramètre	Description
Propriétés d'actif	
IP	Entrez l'adresse IP ou la plage CIDR des actifs que vous souhaitez rechercher.
MAC	Entrez l'adresse MAC de l'actif que vous souhaitez rechercher.
Host Name	Entrez le nom d'hôte de l'actif que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Machine Name	Entrez le nom de la machine de l'actif que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Username	Entrez l'utilisateur des actifs que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
User Group	Entrez le groupe d'utilisateurs des actifs que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Extra Data	Entrez le texte que vous souhaitez rechercher. Le contenu de cette zone représente du texte défini par l'utilisateur et dépend des périphériques de votre réseau qui sont disponibles pour fournir des données d'identité. On peut citer : l'emplacement physique des périphériques, les politiques pertinentes ou les noms des ports et commutateurs réseau.
Asset Name	Entrez le nom des actifs que vous souhaitez rechercher. Cette zone de recherche est insensible à la casse et accepte tous les caractères de symbole.
Description	Entrez la description des actifs que vous souhaitez rechercher.
Port	Entrez les ports (TCP ou UDP) ou plages de ports des actifs que vous souhaitez rechercher. Vous pouvez entrer plusieurs ports, séparés par des virgules. Par exemple, 80, 8080 ou 6000 à 7000.
Risk Level	Dans 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	Dans la zone de liste, sélectionnez le réseau des actifs que vous souhaitez rechercher.
Asset Weight	Entrez la pondération des actifs que vous souhaitez rechercher. Dans 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 SIEM 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
Show only hosts with vulnerabilities	Sélectionnez cette case à cocher si vous souhaitez afficher uniquement les actifs avec des vulnérabilités dans les résultats de la recherche.
Operating System	Entrez le système d'exploitation des actifs que vous souhaitez rechercher. Par exemple, Red Hat Linux®.
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.
Propriétés étendues des actifs	
Business Owner	Entrez le propriétaire fonctionnel des actifs que vous souhaitez rechercher. Un directeur de rayon est un exemple de propriétaire fonctionnel.
Business Owner Contact Info	Entrez les informations de contact du propriétaire fonctionnel des actifs que vous souhaitez rechercher.
Technical Owner	Entrez le propriétaire technique des actifs que vous souhaitez rechercher. Un responsable informatique ou un directeur 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.
Attributs de vulnérabilité	
OSVDB ID	Entrez l'identifiant de vulnérabilité, tel que défini sur le 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 URL d'exploitation générique dirigent vers un script/code d'exploitation ou fichier texte détaillé qui explique comment exploiter une vulnérabilité particulière.*
Generic Informational URL	Entrez l'URL d'informations génériques que vous souhaitez rechercher. ***Remarque :*** *L'adresse URL d'information générique dirige vers des informations sur un type ou une classe de vulnérabilité. Par exemple, cet attribut peut contenir un lien vers un livre blanc sur les attaques DDoS.*
IBM APPSCAN	Entrez l'identificateur IBM AppScan que vous souhaitez rechercher. Par exemple, security-check-applicationtestscriptdetected.
ISS X-Force ID	Entrez l'ID Internet Security System (ISS) X-Force que vous souhaitez rechercher. Par exemple, 1234.
Keyword	Entrez le mot-clé que vous souhaitez rechercher dans toutes les zones dans la OSVDB.
Mail List Post	Entrez l'URL de l'ID de publication de la liste d'adresses que vous souhaitez rechercher.
Metasploit ID	Entrez l'ID Metasploit que vous souhaitez rechercher.
Microsoft Knowledge Base Article	Entrez l'ID de l'article de la base de connaissances Microsoft® que vous souhaitez rechercher. Par exemple, KB958644.
Microsoft Security Bulletin	Entrez l'ID de sécurité Microsoft que vous souhaitez rechercher. Par exemple, MS04-004.
Milw0rm	Entrez l'ID Milw0rm que vous souhaitez rechercher. Par exemple, 6824.
Nessus Script ID	Entrez l'URL de l'ID du script Nessus que vous souhaitez rechercher. Par exemple, 10123.
News Article	Tapez l'URL de l'ID de l'article d'actualité que vous souhaitez rechercher. ***Remarque :*** *L'ID d'article d'actualité fait référence à des articles d'actualité sur des vulnérabilités spécifiques.*
Niko Item ID	Entrez l'ID de l'élément Niko que vous souhaitez rechercher.
OVAL ID	Entrez l'ID OVAL (Open Vulnerability and Assessment Language) que vous souhaitez rechercher. Par exemple, 5863.

Tableau 10-2 Paramètres Asset Profile Search (suite)

Paramètre	Description
Other Advisory URL	Entrez d'autres URL de recommandation que vous souhaitez rechercher.
Other Solution URL	Entrez d'autres URL de solution que vous souhaitez rechercher.
Packet Storm	Entrez la référence Packet Storm que vous souhaitez rechercher.
RedHat RHSA	Entrez l'ID RHSA (RedHat Security Alert) que vous souhaitez rechercher. Par exemple, RHSA-2004:065-05.
Related OSVDB ID	Entrez l'ID OSVDB lié que vous souhaitez rechercher. Les ID sont reliés par des références croisées dans la OSVDB. En règle générale, les ID OSVDB sont reliés par des références croisées, si la source de l'information est la même.
SCIP VulDB ID	Entrez l'ID VulDB (Vulnerability Database) du SCIP (Secure Communications Interoperability Protocol) que vous souhaitez rechercher.
Secunia Advisory ID	Entrez l'ID de recommandation Secunia que vous souhaitez rechercher. Par exemple : 10123.
Security Tracker	Entrez l'ID Security Tracker que vous souhaitez rechercher. Par exemple, 1009695.
Snort Signature ID	Entrez l'ID Signature Snort que vous souhaitez rechercher. Par exemple, 1324.
Tenable PVS	Entrez l'ID Tenable Passive Vulnerability Scanner (PVS) que vous souhaitez rechercher.
US-CERT Cyber Security Alert	Entrez l'ID de l'alerte de cybersécurité US-CERT que vous souhaitez rechercher. Par exemple, TA06-333A.
VUPEN Advisory	Entrez l'ID de sécurité VUPEN que vous souhaitez rechercher.
Vender Specific Advisory URL	Entrez l'URL de la recommandation spécifique du fournisseur que vous souhaitez rechercher.
Vendor Specific News/Changelog Entry	Entrez l'URL de l'entrée du journal des changements/nouveautés spécifiques du fournisseur que vous souhaitez rechercher.
Vendor Specific Solution URL	Entrez l'URL de la solution spécifique du fournisseur que vous souhaitez rechercher.
Vendor URL	Entrez l'URL du fournisseur que vous souhaitez rechercher.

La barre d'outils Asset Profile Search fournit les options suivantes :

Tableau 10-3 Barre d'outils de l'onglet Assets

Options	Description
Add Asset	Cliquez sur **Add Asset** pour ajouter un profil d'actif. Voir **Ajout d'un profil d'actif**.

Tableau 10-3 Barre d'outils de l'onglet Assets (suite)

Options	Description
Actions	Cliquez sur **Actions** pour importer des actifs. Voir **Importation de profils d'actifs**. ***Remarque :*** *Le menu Actions est uniquement disponible si vous disposez des privilèges d'administrateur. Pour plus d'informations, consultez le guide d'administration IBM Security QRadar SIEM.*

Fonctions de la barre d'outils et des paramètres de la page Asset Profiles

La page Asset Profile fournit les informations suivantes :

Tableau 10-4 Paramètres de la page Asset Profile

Paramètre	Description
IP Address	Indique l'adresse IP de l'actif.
MAC	Indique la dernière adresse MAC connue des actifs.
Name	Indique le nom, le nom d'hôte ou le nom de l'ordinateur des actifs. Si ces informations ne sont pas connues, cette zone est vide.
User	Indique le dernier utilisateur connu des actifs. Si cette information n'est pas connue, cette zone est vide.
Group	Indique le dernier groupe d'utilisateur connu des actifs. Si cette information n'est pas connue, cette zone est vide.
Network	Indique le réseau auquel l'actif appartient.
Weight	Indique la pondération de l'actif.
Risk Level	Indique le niveau de risque des actifs.
Vulnerabilities	Indique le nombre des vulnérabilités identifiées associés à cet actif. Cette valeur inclut également le nombre de vulnérabilités actives et passives.
Last Seen	Indique la date et l'heure auxquelles l'actif a été observé pour la dernière fois. Si l'actif a été saisi manuellement, mais qu'il n'a jamais été observé de façon active ou passive, la colonne indique Never.

La barre d'outils de la page Asset Profiles fournit les fonctions suivantes :

Tableau 10-5 Fonctions de la barre d'outils de la page Asset Profiles

Fonction	Description
Modify Search	Cliquez sur **Modify Search** pour retourner à la page de recherche d'actifs afin de modifier vos critères de recherche. Voir **Etude des profils d'actifs**.
Add Asset	Cliquez sur **Add Asset** pour ajouter un profil d'actif. Voir **Ajout d'un profil d'actif**.
Edit Asset	Cliquez sur **Edit Asset** pour modifier un profil d'actif. Cette option est uniquement activée si vous avez sélectionné un profil d'actif dans la liste des résultats. Voir **Modification d'un actif**.

Tableau 10-5 Fonctions de la barre d'outils de la page Asset Profiles (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 **Suppression des actifs**. • **Delete Listed** - Sélectionnez cette option pour supprimer tous les profils d'actif énumérés dans la liste des résultats. Voir **Suppression des actifs**. • **Import Assets** - Sélectionnez cette option pour importer des actifs. Voir **Importation de profils d'actifs**. • **Export to XML** - Sélectionnez cette option pour exporter des profils d'actif au format XML. Voir **Exportation des actifs**. • **Export to CSV** - Sélectionnez cette option pour exporter des profils d'actif au format CSV. Voir **Exportation des actifs**. ***Remarque :*** *Le menu **Actions** n'est disponible que si vous disposez des privilèges d'administration. Pour plus d'informations, consultez le guide d'administration IBM Security QRadar SIEM.*
Print	Cliquez sur **Print** pour imprimer les profils d'actif affichés sur la page.

Fonctions de la barre d'outils et des paramètres de la page Asset Profile

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.
IP Address	Indique l'adresse IP de l'actif.
Network	Indique le réseau auquel l'actif appartient.
Host Name (DNS Name)	Indique le nom DNS ou l'adresse IP de l'actif, si cette information est connue.
Risk Level	Indique le niveau de risque (0 à 10) pour l'actif, où 0 est le niveau le plus bas et 10 le plus élevé. Il s'agit d'une valeur pondérée par rapport à l'ensemble des autres hôtes présents dans votre déploiement.
Operating System	Indique le système d'exploitation exécuté sur l'actif. ***Remarque :*** *Vous pouvez directement éditer ce paramètre si le paramètre **Override** est défini en tant que **Override Until the Next Scan** ou **Override Forever**. Dans 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 qu'entré manuellement. ***Remarque :*** *Vous pouvez directement éditer ce paramètre si le paramètre* ***Override*** *est défini en tant que* ***Override Until the Next Scan*** *ou* ***Override Forever****. Dans la zone de liste, sélectionnez le nom du fournisseur du système d'exploitation.*
Version	Indique la version du système d'exploitation. ***Remarque :*** *Vous pouvez éditer ce paramètre si le paramètre* ***Override*** *est défini en tant que* ***Override Until the Next Scan*** *ou* ***Override Forever****. Dans 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). Dans 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 des actifs.
Machine Name	Indique le dernier nom connu de la machine de l'actif.
Username	Indique le dernier utilisateur connu des actifs.
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'utilisateur connu des actifs.
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 informatique ou un directeur est un exemple de propriétaire technique.
Technical Owner Contact Info	Indique les informations de contact du propriétaire technique.
Location	Indique l'emplacement physique de l'actif.

La barre d'outils de la page Asset Profile fournit les fonctions suivantes :

Tableau 10-7 Barre d'outils de la page Asset Profile

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 retourner à la page de recherche d'actifs afin de modifier vos critères de recherche. Voir **Etude des profils d'actifs**.
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 Fonctions de la barre d'outils du panneau Asset Profile

Options	Description
View by Network	Si cet actif est associé à une violation, 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 **Contrôle des violations regroupées 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 **Contrôle des violations regroupées 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 **Contrôle des violations regroupées par IP cible.**

Tableau 10-8 Fonctions de la barre d'outils du panneau Asset Profile (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 : • **Time Range** - Recent (Last 24 Hours) • **Search Parameters** - Indique d'appliquer les filtres suivants aux résultats de la recherche : - Identity is true - Identity IP is the IP address of the asset • **Column Definition** - Indique d'afficher les colonnes suivantes 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 la recherche d'événements, 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 : • **Time Range** - Recent (Last 24 Hours) • **Search Parameters** - Indique le filtre suivant à appliquer aux résultats de la recherche : L'adresse IP source ou cible est l'adresse IP de l'actif. • **Column Definition** - Indique la colonne **Application Group** à afficher dans les résultats de la recherche. 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**.

Tableau 10-8 Fonctions de la barre d'outils du panneau Asset Profile (suite)

Options	Description
Search Connections	Cliquez sur **Search Connections** pour rechercher des connexions. La fenêtre Connection Search s'affiche. ***Remarque :*** *Cette option apparaît uniquement lorsque vous avez acheté IBM Security QRadar Risk Manager et obtenu une licence. Pour plus d'informations, consultez le guide d'utilisation IBM Security QRadar Risk Manager.*
View Topology	Cliquez sur **View Topology** pour étudier davantage l'actif. La fenêtre Current Topology s'affiche. ***Remarque :*** *Cette option est uniquement disponible lorsque vous avez acheté IBM Security QRadar Risk Manager et obtenu une licence. Pour plus d'informations, consultez le guide d'utilisation IBM Security QRadar Risk Manager.*

Le panneau Ports and Vulnerabilities de la page Asset Profile affiche les informations suivantes :

Tableau 10-9 Paramètres du panneau Ports and Vulnerabilities

Paramètre	Description
Vuln ID	Indique l'ID de la vulnérabilité. Le paramètre Vuln ID est un identifiant unique qui est généré par Vulnerability Information System (VIS).
Port	Indique le numéro de port pour les services reconnus sur l'actif.
Service	Indique les services reconnus sur 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 est uniquement disponible si votre système s'intègre aux 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 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 de façon passive ou active.

Tableau 10-9 Paramètres du panneau Ports and Vulnerabilities (suite)

Paramètre	Description
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, consultez le guide d'administration IBM Security QRadar SIEM.*

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 identifiant unique qui est 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.
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 d'une vulnérabilité. Vous pouvez utiliser les scores CVSS pour mesurer les inquiétudes justifiées par une vulnérabilité par rapport à d'autres vulnérabilités. Pour plus d'informations sur CVSS, voir *http://www.first.org/cvss/*.
Description	Indique une description de la vulnérabilité détectée. Cette valeur est uniquement disponible si votre système s'intègre aux outils VA.
Concern	Indique les effets que la vulnérabilité peut avoir sur votre réseau.

Tableau 10-10 Détails de la fenêtre Research Vulnerabilities Details

Paramètre	Description
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.
Products	Affiche la liste des produits qui sont associés avec 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'onglet **Reports** pour créer, éditer, distribuer et gérer les rapports.

L'onglet **Reports** vous fournit :

- Des options de rapports détaillées nécessaires pour satisfaire les diverses normes de réglementation, telles que la conformité PCI.
- La flexibilité dans la présentation et le contenu.

Présentation de l'onglet Reports

Vous pouvez créer vos propres rapports personnalisés dans QRadar SIEM ou utiliser un rapport par défaut. Vous pouvez personnaliser et renommer chacun des rapports par défaut et les distribuer à d'autres utilisateurs QRadar SIEM.

L'onglet **Reports** peut exiger une longue période de temps pour s'actualiser si votre système inclut un nombre important de rapports.

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 Support technique Microsoft.

Prise en compte du fuseau horaire

Pour garantir que la fonction Reports utilise la date et l'heure correctes de présentation des données, votre session QRadar SIEM doit être synchronisée avec votre fuseau horaire. Lors de l'installation et de la configuration de QRadar SIEM, le fuseau horaire est configuré. Vérifiez auprès de votre administrateur pour s'assurer que votre session QRadar SIEM est synchronisée avec votre fuseau horaire.

Autorisations de l'onglet Reports

Les administratifs peuvent afficher tous les rapports créés par les autres utilisateurs QRadar SIEM. Les utilisateurs non administrateurs peuvent uniquement visualiser 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 visualiser des informations statistiques sur le

modèle rapports, effectuer des actions sur les modèles de rapport, afficher les rapports générés et supprimer le contenu généré.

L'onglet **Reports** fournit les informations suivantes :

Table 11-1 Paramètres de l'onglet Reports

Paramètres	Description
Flag Column	Si une erreur se produit, provoquant l'échec de la génération du rapport, l'icône **Error** s'affiche dans cette colonne.
Report Name	Indique le nom du rapport.
Group	Indique le groupe auquel appartient ce rapport.
Schedule	Indique la fréquence à laquelle le rapport est généré. Les rapports qui indiquent une planification par intervalle, lorsqu'elle est activée, sont automatiquement générés conformément à l'intervalle spécifié. Si un rapport n'indique pas une planification par intervalle, vous devez générer manuellement le rapport. Voir **Génération manuelle d'un rapport**.
Next Run Time	Indique la durée, en heures et en minutes, jusqu'à la génération du prochain rapport.
Last Modification	Indique la date de la dernière modification de ce rapport.
Owner	Indique l'utilisateur QRadar SIEM qui possède le rapport.
Author	Indique l'utilisateur QRadar SIEM qui a créé le rapport.
Generated Reports	Dans cette zone de liste, sélectionnez la date d'émission du rapport généré que vous souhaitez afficher. Lorsque vous sélectionnez la date d'émission, le paramètre **Format** affiche les formats disponibles pour les rapports générés. Voir **Affichage des rapports générés**. Si aucun rapport n'est généré, **None** s'affiche.
Formats	Indique les formats de rapport du rapport sélectionné actuellement dans la colonne **Generated Reports**. Cliquez sur l'icône du format que vous souhaitez afficher. Les formats de rapport incluent : • **PDF** - Portable Document Format • **HTML** - Format Hyper Text Markup Language • **RTF** - Rich Text Format • **XML** - Extensible Markup Language (uniquement disponible pour les tableaux) • **XLS** - Format Microsoft® Excel (uniquement disponible pour les tableaux)

Vous pouvez pointer votre souris sur un rapport pour prévisualiser résumé dans une infobulle. Le résumé indique la configuration du rapport et le type de contenu que génère le rapport.

ordre de tri de l'onglet Report

Par défaut, les rapports sont triés par colonne de **Last Modification.** Dans le menu de navigation Reports, les rapports sont triés par intervalle horaire. Afin de filtrer le rapport pour n'afficher que les rapports d'une fréquence spécifique, cliquez sur la flèche à côté de l'élément de menu **Report** dans le menu de navigation et sélectionnez le groupe (frequency) du dossier.

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 barre d'outils de l'onglet Reports

Option	Description
Group	A partir la zone de liste, sélectionnez le groupe que vous souhaitez afficher. le groupe est affiché avec les rapports affectés. Pour plus d'informations, voir **Groupes de rapports**.
Manage Groups	Cliquez sur **Manage Groups** afin de gérer le groupe de rapports. En utilisant la fonction Manage Groups, vous pouvez organiser vos rapports en groupes fonctionnels. Pour plus d'informations, voir **Groupes de rapports**.

Tableau 11-2 Options de barre d'outils de l'onglet Reports (suite)

Option	Description
Actions	Cliquez sur **Actions** pour effectuez les options 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 d'éditer le rapport sélectionné. Vous pouvez également cliquer deux fois sur un rapport afin d'éditer le contenu. • **Duplicate** - Sélectionnez cette option afin de dupliquer ou de renommer le rapport sélectionné. Pour plus d'informations, voir **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 option afin de générer le rapport sélectionné. Cette option est utile lorsque vous souhaitez générer un rapport avant que les données accumulées nécessaires ne soient disponibles. Par exemple, si vous voulez exécuter un rapport hebdomadaire avant qu'une semaine entière ne se soit écoulée puisque vous avez créé le rapport, vous pouvez générer le rapport en utilisant 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.
Hide Inactive Reports	Sélectionnez cette case afin de masquer les modèles de rapport inactifs. L'onglet **Reports** s'actualise automatiquement et affiche uniquement les rapports actifs. Décochez la case afin d'afficher les rapports inactifs masqués.

Tableau 11-2 Options de barre d'outils de l'onglet Reports (suite)

Option	Description
Search Reports	Entrez vos critères de recherche dans la zone **Search Reports** puis cliquez sur l'icône **Search Reports**. Une recherche est effectuée en fonction des paramètres suivants pour déterminer lequel correspond à vos critères spécifiés : • Report Title • Report Description • Report Groups • Report Author User Name

Barre d'état

La barre d'état affiche le nombre de résultats de recherche (**Displaying 1 of 10 items**) qui s'affiche actuellement et le volume de temps (**Elapsed time:**) nécessaire pour traiter les résultats de la recherche.

Présentation des rapports

Un rapport peut être constitué de plusieurs éléments de données et peut représenter un réseau et des données de sécurité dans une variété de styles, tels que des tableaux, des graphiques linéaires, des graphiques circulaires et des histogrammes.

Lorsque vous sélectionnez l'agencement d'un rapport, considérez le type de rapport que vous souhaitez créer. Par exemple, ne choisissez pas un petit conteneur de tableau pour un contenu graphique qui affiche un grand nombre d'objets. chaque graphique comprend une légende et une liste de réseaux dont le contenu est dérivé, choisissez un conteneur assez grand pour contenir les données. Pour prévisualiser comment chaque graphique affiche un ensemble de données, voir **Types de graphiques**.

Types de graphiques

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 données et des objets de réseau. Vous pouvez tracer des données avec plusieurs caractéristiques et créer les graphiques dans un seul rapport généré.

QRadar SIEM inclut les types de graphiques 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.
- **Asset Vulnerabilities** - Vous pouvez utiliser le graphique Asset Vulnerabilities afficher les données de vulnérabilité pour chaque actif défini dans votre déploiement. Vous pouvez générer des graphiques de vulnérabilité de l'actif lorsque les vulnérabilités ont été détectées par une analyse VA. Pour plus d'informations, voir le *IBM Security QRadarGuide de gestion de l'évaluation de la vulnérabilité*

- **Connections** -L'option The Connections s'affiche uniquement lorsque IBM Security QRadar Risk Manager a été acheté et mis sous licence. Pour plus d'informations, voir le *IBM Security QRadar Risk ManagerGuide d'utilisation*.
- **Device Rules** - L'option Device Rules s'affiche uniquement lorsque IBM Security QRadar Risk Manager a été acheté et mis sous licence. Pour plus d'informations, voir le *IBM Security QRadar Risk Manager Guide d'utilisation*.
- **Device Unused Objects** -L'option The Device Unused Objects s'affiche uniquement lorsque IBM Security QRadar Risk Manager a été acheté et mis sous licence. Pour plus d'informations, voir le *IBM Security QRadar Risk Manager Guide d'utilisation*.
- **Events/Logs** - Vous pouvez utiliser le graphique Event/Logs afin d'afficher des informations sur l'événement. Vous pouvez baser vos graphiques sur des données provenant des recherches enregistrées dans 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 Flows afin d'afficher des informations sur l'événement. Vous pouvez baser vos graphiques sur des données provenant des recherches enregistrées dans 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 la principale destination des espaces de présentation de l'image dans les emplacements réseau que vous sélectionnez.
- **Top Offenses** - Le graphique Top Offenses affiche les violations TopN qui se produisent à l'heure actuelle pour les emplacements réseau que vous sélectionnez.
- **Top Source IPs** -Le graphique Top Source IPs affiche et tri les sources de violations principales (adresses IP) qui attaquent votre réseau ou les actifs de l'entreprise.

Pour plus d'informations sur les types de graphique, voir **Paramètres des conteneurs de graphique**.

Types de graphiques

Chaque type de graphique prend en charge une variété de types de graphiques que vous pouvez utiliser pour afficher les données. Les fichiers de configuration de réseau déterminent les couleurs que les tableaux utilisent pour représenter le trafic réseau. Chaque adresse IP est représentée à l'aide d'une couleur unique.

Le tableau suivant donne des exemples sur la manière dont QRadar SIEM trace les données réseau et de sécurité :

Tableau 11-3 Types de graphiques

Types de graphiques	Disponibilité
Line Graph	Disponible avec les types de graphiques suivants : • Events/Logs • Flows • Connections
Stacked Line Graph	Disponible avec les types de graphiques suivants : • Events/Logs • Flows • Connections
Bar Graph	Disponible avec les types de graphiques suivants : • Events/Logs • Flows • Asset Vulnerabilities • Connections
Horizontal Bar Graph	Disponible avec les types de graphiques suivants : • Top Source IPs • Top Offenses • Top Destination IPs
Stacked Bar Graph	Disponible avec les types de graphiques suivants : • Events/Logs • Flows • Connections
Pie Graph	Disponible avec les types de graphiques suivants : • Events/Logs • Flows • Asset Vulnerabilities • Connections

Tableau 11-3 Types (suite) de graphiques

Types (suite) de graphiques	Disponibilité
Table Graph	Disponible avec les types de graphiques suivants : • Event/Logs • Flows • Top Source IPs • Top Offenses • Top Destination IPs • Connections Pour afficher le contenu d'un tableau, vous devez concevoir le rapport avec un conteneur de largeur pleine page.
Aggregate Table	Disponible avec le graphique Asset Vulnerabilities. Pour afficher le contenu d'un tableau, vous devez concevoir le rapport avec un conteneur de largeur pleine page.

Création de rapports personnalisés

Dans l'onglet **Reports** vous pouvez accéder au Report Wizard pour créer un nouveau rapport.

A propos de cette tâche

L'assistant Report Wizard fournit un guide étape par étape sur la conception, la planification et la génération des rapports. L'assistant utilise les éléments clés suivants pour vous aider à créer un rapport :

- **Layout** - Position et taille de chaque conteneur
- **Container** - Marque de réservation pour le contenu offert
- **Content** - Définition du graphique placé dans le conteneur

Après avoir créé un rapport qui génère hebdomadairement ou mensuellement, la date prévue doit être écoulée avant que le rapport généré renvoie des résultats. Pour un rapport planifié, vous devez attendre l'heure planifiée pour la construction des résultats. Par exemple, une recherche hebdomadaire nécessite 7 jours pour construire les données. Cette recherche ne renvoie pas de résultats avant l'écoulement de 7 jours.

Lorsque vous spécifiez le format final du rapport, n'oubliez pas la taille du fichier des rapports générés peut être d'un ou de deux mégaoctets, en fonction du format de sortie sélectionné. Le format PDF est de plus petite taille et n'occupe pas une grande d'espace de stockage important sur le disque.

Procédure

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

Etape 2 Dans la zone de liste **Actions**, sélectionnez **Create**.

Etape 3 Sur la page d'acceuil de l'assistant de rapports cliquez sur **Next** pour aller à la page suivante.

Etape 4 Sélectionnez l'une des options de planifications suivantes :

Option	Description
Manually	Génère un rapport une fois. Il s'agit du réglage par défaut, mais vous pouvez générer ce rapport aussi souvent que nécessaire.
Hourly	Planifie le rapport pour générer, à la fin de chaque heure en utilisant les données de la précédente heure. Si vous sélectionnez l'option Hourly option, une configuration supplémentaire est nécessaire. Dans les zones de liste, sélectionnez un cadre temporel de début et de fin du cycle de génération. Un rapport est généré pour chaque heure dans ce cadre temporel. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00 pour les deux zones **From** et **To**.
Daily	Planifie le rapport pour générer quotidiennement en utilisant les données de la journée précédente. Pour chaque graphique sur un rapport, vous pouvez sélectionner les 24 dernières heures de la journée, ou sélectionner un cadre temporel précis de la journée précédente. Si vous choisissez l'option **Daily**, une configuration supplémentaire est nécessaire. Cochez la case à côté de chaque jour où vous souhaitez générer un rapport. En outre, vous pouvez utiliser la zone de liste pour sélectionner une heure de début du cycle de génération de rapports. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.
Weekly	Planifie le rapport pour générer hebdomadairement en utilisant les données de la semaine précédente. Si vous sélectionnez l'option **Weekly**, une configuration supplémentaire est nécessaire. Sélectionnez le jour où vous souhaitez générer le rapport. La valeur configurée par défaut est le lundi. Dans la zone de liste, sélectionnez l'heure de début du cycle de génération de rapports. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.
Monthly	Planifie le rapport pour générer mensuellement en utilisant les données du mois précédent. Si vous choisissez l'option **Monthly**, une configuration supplémentaire est nécessaire. Dans la zone de liste, sélectionnez la date où vous souhaitez générer le rapport. La valeur configurée par défaut est le premier jour du mois. Vous pouvez également utiliser la zone de liste pour sélectionner un temps de commencement pour le cycle de génération de rapports. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00.

Etape 5 Dans le volet Allow this report to generate manually, 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 Configurez la présentation de votre rapport :

a Dans la zone de liste **Orientation**, sélectionnez la page d'orientation: portrait ou paysage. La valeur configurée par défaut est paysage.

b Sélectionnez une des six options d'agencement affichées dans le Report Wizard.

c Cliquez sur **Next** afin de se déplacer à la page suivante du Report Wizard.

Etape 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 le marquage de votre rapport, voir **Marquage d'un rapport**.

Etape 8 Configurez chaque conteneur dans le rapport :

a Dans la zone de liste **Chart Type** sélectionnez un type de graphique. Voir **Types de graphiques**.

b Sur la fenêtre Container Details - <chart_type>, configurez les paramètres de graphique. Pour des informations détaillées sur la configuration de votre graphique, voir **Paramètres des conteneurs de graphique**.

c Cliquez sur **Save Container Details**.

L'assistant Wizard renvoie à la page Specify Report Contents, ce qui vous permet de configurer les autres conteneurs dans votre rapport.

d Si nécessaire, répétez les étapes **a** à **c** pour tous les conteneurs.

e Cliquez sur **Next** afin de vous déplacer à la page suivante de l'assistante Report Wizard.

Etape 9 Prévisualisez la page Preview the Layout Preview, puis cliquez sur **Next** pour passer à l'étape suivante de l'assistant Report Wizard.

Etape 10 Sélectionnez les cases à cocher les formats de rapports que vous voulez générer puis cliquez sur **Next**.

Les options incluent les formats de rapports suivants :

- **PDF** - Portable Document Format
- **HTML** - Format Hyper Text Markup Language
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (uniquement disponible pour les tableaux)
- Format **XLS** - Microsoft® Excel

Etape 11 Sélectionnez les canaux de distribution pour votre rapport, puis cliquez sur **Next**. Les options incluent les canaux de distribution suivants :

Option	Description
Report Console	Cochez cette case pour envoyer le rapport généré à l'onglet **Reports**. Il s'agit du canal de distribution par défaut.
Sélectionnez les utilisateurs qui devraient être en mesure d'afficher le rapport généré.	Cette option s'affiche uniquement une fois que vous avez coché la case **Report Console**. Dans la liste des utilisateurs, sélectionnez les utilisateurs QRadar SIEM 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 sur les autorisations, voir le IBM Security QRadar SIEM Guide d'administration.*
Select all users	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 QRadar SIEM 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 sur les autorisations, voir le IBM Security QRadar SIEM Guide d'administration.*
Email	Cochez cette case si vous voulez distribuer les rapports générés par e-mail.
Entrez le(s) adresse(s) e-mail de distribution de rapport	Cette option s'affiche uniquement une fois que vous avez coché la case **Email**. Entrez l'adresse e-mail de chaque destinataire des rapports générés; séparez la liste des adresses e-mail avec des virgules. Le nombre maximum de caractères pour ce paramètre est 255. ***Remarque :*** *Les destinataires reçoivent cet e-mail de no_reply_reports@qradar.*
Include Report as attachment (non-HTML only)	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.
Include link to Report Console	Cette option s'affiche uniquement une fois que vous avez coché la case **Email**. Cochez cette case pour inclure un lien vers Report Console dans l'e-mail.

Etape 12 Sur la page Finishing Up, entrez les valeurs des paramètres suivants :

Paramètre	Description
Report Description	Entrez une description pour ce rapport. La description est affichée dans la page Report Summary et dans l'e-mail de distribution des rapports générés.
Groups	Sélectionnez les groupes auxquels vous voulez affecter ce rapport. Pour plus d'informations à propos des groupes, voir **Groupes de rapports**.
Would you like to run the report now?	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 afin de prévisualiser la configuration de votre rapport.

Etape 15 Cliquez sur **Finish**.

Result

Le rapport est immédiatement généré.Si vous décochez la case **Would you like to run the report now?** sur la page finale de l'assistant, le rapport est sauvegardé et généré à l'heure planifiée.

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 un nouveau rapport avec le même nom ; cependant, le rapport original reste le même.

Tâches de gestion des rapports

A l'aide de l'onglet Reports et de l'assistant, vous pouvez gérer les rapports. Vous pouvez éditer, dupliquer, partager et marquer des rapports. Vous pouvez également supprimer les rapports générés.

Modification d'un rapport

A l'aide de l'assistant Report Wizard, vous pouvez éditer n'importe quel rapport par défaut ou personnalisé à modifier.

A propos de cette tâche

QRadar SIEM 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 Report Wizard, modifier les paramètres pour personnaliser le rapport afin de générer le contenu dont vous avez besoin. Pour plus d'informations sur la manière d'utiliser l'assistant Report Wizard, voir **Création de rapports personnalisés**.

Etape 4 Cliquez sur **Finish**.

Result

Si vous reconfigurez un rapport afin d'entrer un nouveau titre de rapport, le rapport est enregistré comme nouveau rapport avec le nouveau nom, mais l'original rapport reste le même.

Affichage des rapports générés

Sur l'onglet **Reports**, une icône s'affiche sur la colonne **Formats** si un rapport a généré un 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 génère pas de contenu, la valeur **None** est affichée dans la colonne **Generated Reports**.

Les icônes représentant le format du rapport généré sont affichées dans la colonne **Formats**. Les rapports peuvent être générés aux formats suivants :

- **PDF** - Portable Document Format
- **HTML** - Format Hyper Text Markup Language
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (uniquement disponible pour les tableaux)
- Format **XLS** - Microsoft® Excel

Les formats XML et XLS sont disponibles uniquement pour les rapports qui utilisent un format tableau de graphique unique (portrait ou paysage).

Vous pouvez uniquement afficher les rapports auxquels l'administrateur QRadar SIEM vous autorise à accéder. Les administrateurs peuvent accéder à tous les rapports.

Si vous utilisez Mozilla Firefox comme navigateur et que vous sélectionnez le format de rapport RTF, le navigateur Web Mozilla Firefox lance une nouvelle fenêtre de navigateur. Le lancement de cette nouvelle fenêtre est le résultat de la configuration du navigateur Mozilla Firefox et n'affecte pas QRadar SIEM. Vous pouvez fermer la fenêtre et continuer votre session QRadar SIEM.

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.

Result

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 dont vous souhaitez supprimer le contenu généré.

Etape 3 Dans la zone de liste **Actions**, cliquez sur **Delete Generated Content**.

Result

Tout le contenu généré pour le rapport sélectionné est supprimé.

Génération manuelle d'un rapport

Un rapport peut être configuré pour être généré automatiquement, cependant, vous pouvez générer un rapport manuellement, à n'importe quel moment.

A propos de cette tâche

Pendant que le rapport est généré, la colonne **Next Run Time** affiche l'un des trois messages suivants :

- **Generating** - Le rapport est en cours de génération.
- **Queued (*position in the queue*)** - Le rapport est mis en attente pour la génération. Le message indique la position du rapport en file d'attente. Par exemple, 1 de 3.
- **(*x* hour(s) *x* min(s) *y* sec(s))** - Le rapport est planifié pour s'exécuter. Le message est un compte à rebours qui indique quand le rapport suivant sera exécuté.

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 des rapports générés**.

Duplication d'un rapport

Pour créer un rapport qui présente une forte ressemblance avec un rapport existant, vous pouvez dupliquer le rapport que vous souhaitez modéliser puis le personnaliser.

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 de 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'affectent 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**.

Marquage d'un rapport

Pour marquer les rapports, vous pouvez importer des logos et des images spécifiques. To Pour des rapports de marque avec des logos personnalisés, vous devez télécharger et configurer les logos avant de commencer à utiliser le Report Wizard.

Avant de commencer

Nous vous recommandons l'utilisation des graphiques 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 vers QRadar SIEM, l'image est automatiquement enregistrée au format Portable Network Graphic (PNG).

Lorsque vous téléchargez une nouvelle image et que vous la définissez comme votre image par défaut, la nouvelle image par défaut n'est pas appliquée aux rapports qui ont été précédemment générés. La mise à jour du logo sur les rapports précédemment générés nécessite la génération manuelle d'un nouveau contenu dans le rapport.

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** pour 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** pour télécharger l'image vers QRadar SIEM.

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 efficacement organiser et trouver des rapports. Par exemple, vous pouvez afficher tous les rapports relatifs à la conformité de la Payment Card Industry Data Security Standard (PCIDSS).

Par défaut, l'onglet **Reports** affiche la liste de tous les rapports, Cependant, vous pouvez classer les rapports dans des groupes tels que :

- Compliance
- Executive

- Log Sources
- Network Management
- Security
- VoIP
- Other

Lorsque vous créez un nouveau rapport, vous pouvez affecter le rapport à un groupe existant ou créer un nouveau groupe. Vous devez disposer d'un accès administratif afin de créer, modifier ou supprimer des groupes. Pour plus d'informations sur les rôles, voir le *IBM Security QRadar SIEM Guide d'administration*.

Création d'un groupe

QRadar SIEM inclut des groupes de rapport par défaut, cependant, vous pouvez également ajouter des groupes.

Procédure

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

Etape 2 Click **Manage Groups**.

Etape 3 En utilisant l'arborescence de navigation, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.

Etape 4 Cliquez sur **New Group**.

Etape 5 Entrez les valeurs pour les paramètres suivants :

- **Name** - Entrez le nom pour le nouveau groupe. Le nom peut contenir jusqu' à 225 caractères.
- **Description** - Entrez une description pour ce groupe. La description peut contenir 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 éditer un groupe de rapport pour modifier 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 éditer.

Etape 4 Cliquez sur **Edit**.

Etape 5 Mettez les valeurs des paramètres à jour, si nécessaire :

- **Name** - Entrez le nom pour le nouveau groupe. Le nom peut contenir jusqu' à 225 caractères.
- **Description** - Entrez une description pour ce groupe. La description peut contenir 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 A partir de la zone de liste **Actions**, sélectionnez **Assign Groups**.

Etape 4 Dans la liste **Item Groups**, sélectionnez la case du groupe auquel vous souhaitez attribuer 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 d'un rapport d'un groupe

Utilisation d'une icône **Remove**, vous pouvez supprimer un rapport d'un groupe.

A propos de cette tâche

Lorsque vous supprimez un rapport à partir d'un groupe, le rapport 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 des conteneurs de graphique

Le type de graphique détermine la façon dont le rapport généré présente des données et des objets de réseau. Vous pouvez tracer des données avec plusieurs caractéristiques et créer les graphiques dans un seul rapport généré.

Paramètres du conteneur de graphiques Asset Vulnerabilities

Le tableau suivant décrit les paramètres de conteneur du graphique Asset Vulnerabilities :

Tableau 11-4 Paramètres du conteneur Asset Vulnerabilities

Paramètre	Description
Container Details - Assets	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Assets to Top	Dans la zone de liste, sélectionnez le nombre des actifs que vous souhaitez inclure dans ce rapport.

Tableau 11-4 Paramètres du conteneur Asset Vulnerabilities (suite)

Paramètre	Description
Graph Type	Dans la zone de liste, sélectionnez le type de graphiqueà 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 des sous-rapports. Il s'agit de la configuration par défaut. Ce type de graphiquenécessite 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 des sous-rapports. Ce type de graphiquenécessite que la recherche enregistrée corresponde à une recherche groupée. Pour afficher des exemples de chaque type de données des graphiques, voir **Types de graphiques**.
Order Assets By	Sélectionnez le type de données en fonction duquel vous souhaitez trier le graphique. 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 à propos de CVSS, voir *http://www.first.org/cvss/*. • **Vulnerability Count** - Trie les données en fonction du nombre de vulnérabilités des actifs.
Sub-Report Details	
Sub-report	Indique le type d'information affichée dans le sous-rapport.
Order Sub-report By	Sélectionnez le paramètre en fonction duquel vous souhaitez organiser le sous-rapport. Les options incluent : • Risk (Base Score) • OSVDB ID • OSVDB Title • Last Modified Date • Disclosure Date • Discovery Date Pour plus d'informations sur la base de données Open Source Vulnerability (OSVDB), voir *http://osvdb.org/*.

Tableau 11-4 Paramètres du conteneur Asset Vulnerabilities (suite)

Paramètre	Description
Limit Sub-report to Top	Dans la zone de liste, sélectionnez le nombre de vulnérabilités que vous souhaitez inclure dans ce sous-rapport.
Graph Content	
Vulnerabilities	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 vulnérabilité, voir **Gestion de l'actif.** **3** Dans la liste **Search Results**, sélectionnez les vulnérabilités que vous souhaitez signaler. Cliquez sur **Add**. **4** Cliquez sur **Submit**.
IP Address	Tapez l'adresse IP, le CIDR ou une liste des adresses IP séparées par des virgules que vous souhaitez signaler Les CIDR partiels sont autorisés.
Networks	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels recueillir des données de graphiques.

Paramètres du conteneur de graphiques Event/Logs

Le tableau suivant décrit les paramètres de conteneur du graphique Events/Logs Vulnerabilities :

Tableau 11-5 Paramètres de conteneur du graphique Event/Logs

Paramètre	Description
Container Details - Events/Logs	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Events/Logs to Top	Dans la zone de liste, sélectionnez le nombre des événements/journaux à afficher dans le rapport généré.

Tableau 11-5 Paramètres de conteneur du graphique Event/Logs (suite)

Paramètre	Description
Graph Type	Dans la zone de liste, sélectionnez le type de graphiqueà afficher dans le rapport généré. Les options incluent : • **Bar** - Affiche les données dans un graphique à barres. Il s'agit du type de graphiquepar défaut. Ce type de graphiquenécessite 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 graphiquenécessite que la recherche enregistrée corresponde à une recherche groupée. • **Stacked Bar** - Affiche les données dans un graphique à barres empilées. • **Stacked Line** - Affiche les données dans un graphique à courbes empilées. • **Table** - Affiche les données sous la forme d'un tableau. L'option **Table** est uniquement disponible pour le conteneur de largeur pleine page seulement. Pour afficher des exemples de chaque graphique, voir **Types de graphiques**.

Tableau 11-5 Paramètres de conteneur du graphique Event/Logs (suite)

Paramètre	Description
Manual Scheduling	Le panneau Manual Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Manually** dans le Report Wizard. En utilisant les options Manual Scheduling, vous pouvez créer une planification manuelle qui peut exécuter un rapport sur une période de temps personnalisée définie, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez. Par exemple, vous pouvez programmer un rapport pour qu'il soit exécuté du 1er au 31 Octobre, incluant uniquement les données générées pendant vos heures de travail, telles que du lundi au vendredi, de 8h00 à 21h00. 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 les 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 du graphique Event/Logs (suite)

Paramètre	Description
Hourly Scheduling	Afin d'affiner davantage 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 sélectionnez uniquement les heures de 8h00 à 17h00. Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport. Le panneau Hourly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Hourly** dans le Report Wizard. ▶ 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 les 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 du graphique Event/Logs (suite)

Paramètre	Description
Daily Scheduling	Le panneau Daily Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Daily** dans le Report Wizard. **1** Sélectionnez une des options suivantes : • **All data from previous day (24 hours)** • **Data of previous day from** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. **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 les 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 du graphique Event/Logs (suite)

Paramètre	Description
Weekly Scheduling	Le panneau Weekly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Weekly** dans le Report Wizard. **1** Sélectionnez une des options suivantes : • **All data from previous week** • **All Data from previous week from** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut est le dimanche. **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 les 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 davantage 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 sélectionnez 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 du graphique Event/Logs (suite)

Paramètre	Description
Monthly Scheduling	Le panneau Monthly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Monthly** dans le Report Wizard. **1** Sélectionnez une des options suivantes : • **All data from previous month** • **Data from previous month from the** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut s'étend du 1er au 31. **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 les 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 davantage 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 sélectionnez uniquement les heures de 8h00 à 17h00. **3** Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.
Graph Content	
Group	Dans la zone de liste, sélectionnez une 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 du graphique Event/Logs (suite)

Paramètre	Description
Type Saved Search or Select from List	Pour affiner la liste **Available Saved Searches**, entrez le nom de la recherche que vous souhaitez localiser dans la zone **Type Saved Search or Select from List**. Vous pouvez également entrer un mot-clé pour afficher la liste des recherches incluant ce mot clé. Par exemple, entrez **`Firewall`** afin d'afficher une liste de toutes les recherches qui incluent Firewall dans le nom de la recherche.
Available Saved Searches	Fournit une liste des recherches enregistrées disponibles. Toutes les recherches enregistrées disponibles s'affichent par défaut, Cependant, vous pouvez filtrer la liste en sélectionnant un groupe dans la zone de liste **Group** ou en entrant le nom d'une recherche enregistrée connue dans la zone **Type Saved Search or Select from List**.
Create New Event Search	Cliquez sur **Create New Event Search** pour créer une nouvelle recherche. Pour plus d'informations sur la création d'une recherche d'événements, voir **Etude des activités de journal.**

Paramètres du conteneur de graphiques Flows

Le tableau suivant décrit les paramètres de conteneur du graphique Flows Vulnerabilities :

Tableau 11-6 Détails du conteneur de flux

Paramètre	Description
Container Details - Flows	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Flows to Top	Dans la zone de liste, sélectionnez le nombre de flux qui doivent être affichés dans le rapport généré.

Tableau 11-6 Détails du conteneur de flux (suite)

Paramètre	Description
Graph Type	Dans la zone de liste, sélectionnez le type de graphiqueà afficher dans le rapport généré. Les options incluent : • **Bar** - Affiche les données dans un graphique à barres. Il s'agit du type de graphiquepar 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 graphiques**.

Tableau 11-6 Détails du conteneur de flux (suite)

Paramètre	Description
Manual Scheduling	Le panneau Manual Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Manually** dans le Report Wizard. En utilisant les options Manual Scheduling, vous pouvez créer une planification manuelle qui peut exécuter un rapport sur une période de temps personnalisée définie, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez. Par exemple, vous pouvez programmer un rapport pour qu'il soit exécuté du 1er au 31 Octobre, incluant uniquement les données générées pendant vos heures de travail, telles que du lundi au vendredi, de 8h00 à 21h00. 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****, l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise les 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.* **6**

Tableau 11-6 Détails du conteneur de flux (suite)

Paramètre	Description
	Afin d'affiner davantage 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 sélectionnez uniquement les heures de 8h00 à 17h00. **3** Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport. Le panneau Hourly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Hourly** dans le Report Wizard.
Hourly Scheduling	▶ 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****, l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise les 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 du conteneur de flux (suite)

Paramètre	Description
Daily Scheduling	Le panneau Daily Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Daily** dans le Report Wizard. **1** Sélectionnez une des options suivantes : • **All data from previous day (24 hours)** • **Data of previous day from** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1h00. **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****, l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise les 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 du conteneur de flux (suite)

Paramètre	Description
Weekly Scheduling	Le panneau Weekly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Weekly** dans le Report Wizard. **1** Sélectionnez une des options suivantes : • All data from previous week • **All Data from previous week from** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut est le dimanche. **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****, l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise les 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 davantage 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 sélectionnez 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 du conteneur de flux (suite)

Paramètre	Description
Monthly Scheduling	Le panneau Monthly Scheduling s'affiche uniquement si vous sélectionnez l'option de planification **Monthly** dans le Report Wizard. **1** Sélectionnez une des options suivantes : • **All data from previous month** • **Data from previous month from the** - Dans les zones de liste, sélectionnez la période de temps que vous souhaitez pour le rapport généré. La valeur configurée par défaut s'étend du 1er au 31. **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****, l'emplacement des processeurs d'événements associés à la recherche d'événements utilisée pour regrouper certaines des données rapportées. Si le rapport utilise les 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 davantage 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 sélectionnez uniquement les heures de 8h00 à 17h00. **3** Cochez la case pour chaque jour de la semaine pour lequel vous souhaitez programmer votre rapport.
Graph Content	
Group	Dans la zone de liste, sélectionnez une recherche enregistrée pour afficher les recherches enregistrées appartenant à ce groupe dans la zone de liste **Available Saved Searches**.
Type Saved Search or Select from List	Pour affiner la liste **Available Saved Searches**, entrez le nom de la recherche que vous souhaitez localiser dans la zone **Type Saved Search or Select from List**. Vous pouvez également entrer un mot-clé pour afficher la liste des recherches incluant ce mot clé. Par exemple, entrez **`Firewall`** afin d'afficher une liste de toutes les recherches qui incluent Firewall dans le nom de la recherche.

Tableau 11-6 Détails du conteneur de flux (suite)

Paramètre	Description
Available Saved Searches	Fournit une liste des recherches enregistrées disponibles. Toutes les recherches enregistrées disponibles s'affichent par défaut, Cependant, vous pouvez filtrer la liste en sélectionnant un groupe dans la zone de liste **Group** ou en entrant le nom d'une recherche enregistrée connue dans la zone **Type Saved Search or Select from List**.
Create New Flow Search	Cliquez sur **Create New Flow Search** afin de créer une nouvelle recherche. Pour plus d'informations sur la création d'un flux de recherche, voir **Demande de l'activité du réseau.**

Paramètres du conteneur de graphiques Top Source IPs

Le tableau suivant décrit les paramètres de conteneur du graphique Top Source IPs :

Tableau 11-7 Paramètres de conteneur de graphique des IP source principales

Paramètre	Description
Container Details - Top Source IPs	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Top Source IPs to	Dans la zone de liste, sélectionnez le nombre des sources de l'espace de présentation de l'image qui doivent être affichés dans le rapport généré.
Graph Type	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 diagramme à barres.
Order Results By	Dans la zone de liste, sélectionnez le tri des données dans le graphique. Les options incluent : • Asset Weight • Risk • Magnitude
Graph Content	
Networks	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels recueillir des données graphiques.

Paramètres du conteneur de graphiques Top Offenses

Le tableau suivant décrit les paramètres de conteneur du graphique Top Offenses :

Tableau 11-8 Paramètres de conteneur de graphique de violations principales

Paramètre	Description
Container Details - Top Offenses	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Top Offenses To	Dans la zone de liste, sélectionnez le nombre des violations à inclure dans les graphiques. La valeur configurée par défaut est 10.
Graph Type	Dans la zone de liste, sélectionnez le type de graphique à afficher dans le rapport généré. Les options incluent : • **Table** - Affiche les données sous la forme d'un tableau (uniquement avec conteneur de largeur pleine page). • **Horizontal Bar** - Affiche les données dans un diagramme à barres.
Order Results By:	Dans la zone de liste, sélectionnez le tri des données dans le graphique. Les options incluent : • Severity • Magnitude • Relevance • Credibility
Graph Content - Parameter Based	
Parameter Based	Sélectionnez cette option si vous souhaitez inclure un paramètre basé sur le graphique des principales violations dans votre rapport. Lorsque cette option est sélectionnée, les paramètres **Include**, **Offenses Category** et **Networks** sont affichés.
Include	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 : • Active Offenses • Inactive Offenses • Hidden Offenses • Closed Offenses 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.

Tableau 11-8 Paramètres de conteneur de graphique de violations principales (suite)

Paramètre	Description
Offenses Category	Cette option s'affiche uniquement si l'option **Parameter Based** est sélectionnée. Dans la zone de liste **High Level Category**, sélectionnez la catégorie de haut niveau que vous souhaitez inclure dans le rapport généré. Dans la zone de liste **Low Level Category**, sélectionnez la catégorie de bas niveau que vous souhaitez inclure dans le rapport généré. Pour plus d'informations sur les catégories de haut et de bas niveau, voir le *IBM Security QRadar SIEM Guide d'administration*.
Networks	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 recueillir des données graphiques.
Graph Content - Saved Search Based	
Saved Search Based	Sélectionnez cette option si vous souhaitez inclure une recherche enregistrée basée sur le graphique des principales violations dans votre rapport. Lorsque cette option est sélectionnée, les paramètres **Group, Type Saved Search or Select from List et Available Saved Searches** s'affichent.
Group	Dans la zone de liste, sélectionnez une recherche enregistrée pour afficher les recherches enregistrées appartenant à ce groupe dans la zone de liste **Available Saved Searches**.
Type Saved Search or Select from List	Pour affiner la liste **Available Saved Searches**, entrez le nom de la recherche que vous souhaitez localiser dans la zone **Type Saved Search or Select from List**. Vous pouvez également entrer un mot-clé pour afficher la liste des recherches incluant ce mot clé. Par exemple, entrez **`Firewall`** afin d'afficher une liste de toutes les recherches qui incluent Firewall dans le nom de la recherche.
Available Saved Searches	Fournit une liste des recherches enregistrées disponibles. Toutes les recherches enregistrées disponibles s'affichent par défaut, Cependant, vous pouvez filtrer la liste en sélectionnant un groupe dans la zone de liste **Group** ou en entrant le nom d'une recherche enregistrée connue dans la zone **Type Saved Search or Select from List**.

Paramètres du conteneur de graphiques Top Destination IPs

Le tableau suivant décrit les paramètres de conteneur du graphique Top Destination IPs :

Tableau 11-9 Paramètres de conteneur de graphique des IP cible principales

Paramètre	Description
Container Details - Top Destination IPs	
Chart Title	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Chart Sub-Title	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Limit Top Destination IPs to	Dans la zone de liste, sélectionnez le nombre des cibles des espaces de présentation de l'image à afficher dans le rapport généré.
Graph Type	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 diagramme à barres.
Order Results By	Dans la zone de liste, sélectionnez l'affichage des données dans le graphique. Les options incluent : • Asset Weight • Risk Level • Magnitude

Tableau 11-9 Paramètres de conteneur de graphique des IP cible principales (suite)

Paramètre	Description
Graph content	
Networks	Dans l'arborescence de navigation, sélectionnez un ou plusieurs réseaux à partir desquels recueillir des données graphiques.

A TESTS DE RÈGLES

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 de taux.

Tests de règle d'événement

Cette section fournit des informations sur les tests de règles d'événement que vous pouvez appliquer à la règle notamment :

- **Tests de profil d'hôte**
- **Tests IP/Port**
- **Tests de propriété d'événement**
- **Tests de propriétés communs**
- **Tests de source de journal**
- **Fonction - tests de séquence**
- **Fonction - tests de compteur**
- **Fonction - tests simples**
- **Tests Date/Heure**
- **Tests de propriété du réseau**
- **Fonction - tests négatifs**

Tests de profil d'hôte Les tests de profil d'hôte comprennent :

Tableau A-1 Règles d'événements : Tests de profil d'hôte

Test	Description	Nom du test par défaut	Paramètres
Host Profile Port	Validez lorsque le port est ouvert sur une source ou une destination locale configurée. Vous pouvez également spécifier si le statut du port est détecté en utilisant l'une des méthodes suivantes : • **Active** - QRadar SIEM recherche activement des ports configurés via l'évaluation de la vulnérabilité et de l'analyse. • **Passive** - QRadar SIEM surveille passivement le réseau en enregistrant les hôtes déjà détectés.	lorsque le port de destination de l'hôte **source** est ouvert **either actively or passively**	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 considère l'analyse active ou passive ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.
Host Existence	Validez lorsque l'hôte source ou de destination est connu pour sa présence via l'analyse active ou passive. Vous pouvez également spécifier si l'état de l'hôte est détecté en utilisant l'une des méthodes suivantes : • **Active** - QRadar SIEM recherche activement des hôtes configurés via l'évaluation de la vulnérabilité et de l'analyse. • **Passive** - QRadar SIEM surveille passivement le réseau en enregistrant 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 à l'hôte source ou de destination. La valeur par défaut est **source**. • **actively seen | passively seen | either actively or passively seen** - Indiquez si vous souhaitez que ce test considère l'analyse active ou passive ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.

Tableau A-1 Règles d'événements : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Host Profile Age	Validez lorsque la source locale ou de destination est supérieure à la valeur configurée dans les intervalles configurés.	lorsque l'âge du profil d'hôte de la **source** locale est **greater than this number of time intervals**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test s'applique à l'hôte source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge d'hôte du profil. • **this number of** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **time intervals** - Indiquez si vous souhaitez que le test considère les minutes ou les heures.
Host Port Age	Validez lorsque l'âge du profil du port source ou de destination est supérieur ou inférieur au temps configuré.	lorsque l'âge du port du profil de l'hôte de la **source** locale est **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 considère les valeurs supérieures ou inférieures à l'âge du port du profil. La valeur par défaut est **greater than**. • **this number of** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **time intervals** - Indiquez si vous souhaitez que le test considère les minutes ou les heures.

Tableau A-1 Règles d'événements : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Asset Weight	Validez lorsque l'actif spécifié possède une pondération assignée supérieure ou inférieure à la valeur configurée.	lorsque l'actif de **destination** a une pondération **greater than this weight**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test considère l'actif source et de destination. La valeur par défaut est **destination**. • **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 la pondération que ce test doive prendre en considération.
Host Vulnerable to Event	Validez lorsque le port de l'hôte spécifié est vulnérable à l'événement en cours.	lorsque la **destination** est vulnérable à un exploit **current** sur **any** port	Configurez les paramètres suivants : • **destination | source | local host | remote host** - Indiquez si vous souhaitez que ce test considère une destination, une source, un hôte local ou un hôte distant. La valeur par défaut est **destination**. • **current | any** - Indiquez si vous souhaitez que ce test considère l'exploit en cours ou n'importe quel autre exploit. La valeur par défaut est **current**. • **any | current** - Indiquez si vous souhaitez que ce test considère n'importe quel port en cours. La valeur par défaut est **any**.
OSVDB IDs	Validez lorsqu'une adresse IP (source ou de destination) est vulnérable aux ID Open Source Vulnerability Database (OSVDB) configurés.	lorsque **source IP** est vulnérable à l'un des **OSVDB IDs suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est **source IP**. • **OSVDB IDs** - Indiquez n'importe quel ID OSVDB que vous souhaitez que le test considère. Pour plus d'informations sur les ID OSVDB, consultez *http://osvdb.org/*.

Tests IP/Port Les tests IP/Port comprennent :

Tableau A-2 Règles d'événements : Groupe de tests IP/Port

Test	Description	Nom du test par défaut	Paramètres
Source Port	Validez lorsque le port de la source de l'événement fait partie des ports source configurés.	lorsque le port source est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Destination Port	Validez lorsque le port de la destination de l'événement fait partie des ports de destination configurés.	lorsque le port de destination est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Local Port	Validez lorsque le port local de l'événement fait partie des ports locaux configurés.	lorsque le port local est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Remote Port	Validez 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 ce test doive prendre en considération.
Source IP Address	Validez lorsque l'adresse IP source de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP source est l'une des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Destination IP Address	Validez lorsque l'adresse IP de destination de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP de destination fait partie des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Local IP Address	Validez lorsque l'adresse IP locale de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP locale est l'une des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Remote IP Address	Validez lorsque l'adresse IP distante de l'événement est l'une des adresses IP configurées.	lorsque l'adresse IP distante est l'une des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
IP Address	Validez 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 **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Source or Destination Port	lorsque le port source ou de destination est l'un des ports configurés	lorsque le port source ou de destination est l'un de **these ports**	**these ports** - Indiquez les ports que ce test doive prendre en considération.

Tests de propriété d'événement Le groupe de tests de propriétés d'événement comprend :

Tableau A-3 Règles d'événements : Tests de propriétés d'événement

Test	Description	Nom du test par défaut	Paramètres
Local Network Object	Validez lorsque l'événement se produit dans le réseau spécifié.	lorsque le réseau de **destination** est **one of the following networks**	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 appliquer ce test.
IP Protocol	Validez lorsque le protocole IP de l'événement est l'un des protocoles configurés.	lorsque le protocole d'adresse IP est l'un des **protocols 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 inclue dans n'importe quel emplacement du contenu de l'événement.	lorsqu'Event Payload contient **this string**	**this string** - Indiquez la chaîne de texte que vous souhaitez inclure pour ce test.
QID of Event	Un QID est un identificateur unique pour les événements. Ce test est valide lorsque l'identificateur d'événements est un QID configuré.	lorsque le QID d'événements est 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 de niveau faible et élevée que vous souhaitez localiser. • Sélectionnez l'option QID Search et entrez le QID ou le nom que vous souhaitez localiser. Cliquez sur **Search**.

Tableau A-3 Règles d'événements : Tests de propriétés d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Context	Event Context est la relation entre l'adresse IP source et l'adresse IP de destination de l'événement. Par exemple, une adresse IP source locale vers une adresse IP de destination distante. Validez si le contexte d'événements est l'une des options suivantes : • Local to Local • Local to Remote • Remote to Local • Remote to Remote	lorsque le contexte d'événements est **this context**	**this context** - Indiquez le contexte que ce test doive prendre en considération. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Event Category	Validez lorsque la catégorie d'événements est la même que la catégorie configurée, par exemple, l'attaque Denial of Service (DoS).	lorsque la catégorie d'événements pour l'événement est l'une des **categories suivantes**	**categories** - Indiquez la catégorie d'événements que ce test doive prendre en considération. Pour plus d'informations sur les catégories d'événements, voir *IBM Security QRadar SIEM le guide d'administration*.
Severity	Validez lorsque la gravité de l'événement est supérieure, inférieure ou égale à la valeur configurée.	lorsque la gravité de l'événement est **greater than 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**.
Credibility	Validez lorsque la crédibilité est supérieure, inférieure ou égale à la valeur configurée.	lorsque la crédibilité de la valeur est **greater than 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**.

Tableau A-3 Règles d'événements : Tests de propriétés d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Relevance	Validez lorsque la pertinence est supérieure, inférieure ou égale à la valeur configurée.	lorsque la pertinence est **greater than 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	Validez lorsque l'adresse IP source de l'événement est locale ou distante.	lorsque la source est **local or remote {par défaut : remote}**	**local | remote** - Indiquez un trafic local ou distant.
Destination Location	Validez lorsque l'adresse IP de destination de l'événement est locale ou distante.	lorsque la destination est **local or remote {par défaut : remote}**	**local | remote** - Indiquez un trafic local ou distant.
Rate Analysis	QRadar SIEM contrôle les taux d'événements de tous les QID et adresses IP source et de destination et marque les événements qui montrent un comportement de taux anormal. Validez lorsque l'événement est marqué pour l'analyse de taux.	lorsque l'événement est marqué pour l'analyse de taux.	N/A
Geographic Location	Validez lorsque l'adresse IP source correspond à l'emplacement géographique configuré.	lorsque la source est localisée dans cette **geographic region**	**geographic location** - Sélectionnez un emplacement géographique.

Tableau A-3 Règles d'événements : Tests de propriétés d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
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 annuler un réglage du 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 ce test doive prendre en considération. Entrez la signature dans le format suivant : <CAT|QID|ANY>:<value>:<source IP>:<dest IP> Emplacement : <CAT|QID|ANY> - Indiquez si vous souhaitez que cette signature faux positif considère une catégorie (CAT), Q1 Labs un identificateur (QID), ou une autre valeur. <value> - Indiquez la valeur du paramètre <CAT|QID|ANY> Par exemple, si vous avez spécifié QID, vous devez indiquer la valeur QID. <source IP> - Indiquez l'adresse IP source que cette signature de faux positif doive prendre en considération. <dest IP> - Indiquez l'adresse IP de destination que vous souhaitez que la signature du faux positif prenne en considération.

Tableau A-3 Règles d'événements : Tests de propriétés d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	Validez lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé à une chaîne d'expressions régulières particulières ***Remarque :*** *Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez les modèles d'expressions régulières personnalisés, acceptez les règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.*	lorsque l'**username** correspond au **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 chaîne d'expression régulière que vous souhaitez considérer pour ce test.
IPv6	Validez lorsque l'adresse IPv6 de destination ou source correspond à l'adresse IP configurée.	lorsque **source IP (v6)** est l'une des **IPv6 addresses suivantes**	Configurez les paramètres suivants : • **source IP (v6) | destination IP (v6)** - Indiquez si vous souhaitez que ce test considère l'adresse IPv6 source ou de destination. • **IP (v6) addresses** - Indiquez les adresses IPv6 que ce test doive prendre en considération.
Reference Set	Validez lorsque l'une ou toutes les propriétés d'événements sont comprises dans l'un ou tous les ensembles de référence configurés.	Lorsqu'**any** de **these event properties** est comprise dans **any** de **these reference set(s)**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération.

Tableau A-3 Règles d'événements : Tests de propriétés d'événement (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Map	Validez lorsque l'une ou toutes les propriétés d'événements dans une paire clé ou de valeur configurée sont comprises dans l'une ou toutes les cartes de référence configurées.	lorsqu'**any** de **these event properties** est la clé et **any** de **these event properties** est la valeur dans **any** de **these reference maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération • **these reference maps** - Indiquez les cartes de référence que ce test doive prendre en considération.
Reference Map of Sets	Validez lorsque l'une ou toutes les propriétés d'événements dans une paire clé ou de valeur configurée sont comprises dans l'un ou tous les ensembles de cartes de référence configurés.	lorsqu'**any** de **these event properties** est la clé et **any** de **these event properties** est la valeur dans **any** de **these reference maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération • **these reference map of sets** - Indiquez les ensembles de cartes de référence que ce test doive prendre en considération.
Reference Map of Maps	Validez lorsque l'une ou toutes les propriétés d'événements dans une paire ou de valeur configurée dans une paire clé ou de valeur primaire et secondaire sont comprises dans l'un ou tous les ensembles de cartes de cartes de référence configurés.	lorsqu'**any** de **these event properties** est la clé de la première carte et **any** de **these event properties** est la clé de la deuxième carte et **any** de **these properties** est la valeur dans any de **these reference map of maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération • **these reference map of maps** - Indiquez la carte de référence des cartes que ce test doive prendre en considération.
Search Filter	Validez lorsque l'événement correspond au filtre de recherche spécifié.	lorsque l'événement correspond à ce **filtre de recherche**	**this search filter** - Indiquez le filtre de recherche que ce test doive prendre en considération.

Tests de propriétés communs Le groupe de tests de propriétés communs comprend :

Tableau A-4 Règles d'événements : Tests de propriétés communs

Test	Description	Nom du test par défaut	Paramètres
CVSS Risk (Host)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque l'hôte de **destination** possède une valeur de risque CVSS **greater than this amount**	Configurez les paramètres suivants : • **source | destination | autre** - 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 de risque CVSS soit supérieure, inférieure ou égale à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.
CVSS Risk (Port)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque le port de **destination** possède une valeur de risque CVSS **greater than this amount**	• **source | destination | either** - Indiquez si le test prend en considération le port source ou de destination de l'événement. • **greater than | less than | equal to** - Indiquez si vous souhaitez que le niveau de menace soit supérieur, inférieur ou égal à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.
Custom Rule Engines	Validez lorsque l'événement est traité par des moteurs de règles personnalisées spécifiés.	lorsque l'événement est traité par l'un de **these** moteurs de règles personnalisées	**these** - Indiquez le moteur de règles personnalisées que ce test doive prendre en considération.

Tableau A-4 Règles d'événements : Tests de propriétés communs (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	Validez lorsque la propriété configurée est associée à une chaîne d'expressions régulières particulières (regex). ***Remarque :*** *Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez les modèles d'expressions régulières personnalisés, acceptez les règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.*	lorsque **these propriétés** correspondent au **regex suivant**	Configurez les paramètres suivants : • **these properties** - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événements et de flux personnalisées normalisés. • **regex** - Indiquez la chaîne d'expression régulière que vous souhaitez considérer pour ce test.
Hexadecimal	Validez lorsque la propriété configurée est associée à une valeur hexadécimale.	Si aucune de **these properties** ne contient de **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'événements et de flux personnalisées normalisés. • **these hexadecimal values** - Indiquez les valeurs hexadécimales que vous ce test doive prendre en considération.

Tests de source de journal Les tests de source de journal comprennent :

Tableau A-5 Règles d'événements : Tests de source de journal

Test	Description	Nom du test par défaut	Paramètres
Source Log Sources	Validez lorsque l'une des sources du journal configurées est la source de l'événement.	lorsque le ou les événements sont détectés par une ou plusieurs **these log source**	**these log sources** - Indiquez les sources du journal que ce test doit détecter.

Tableau A-5 Règles d'événements : Tests de source de journal (suite)

Test	Description	Nom du test par défaut	Paramètres
Log Source Type	Validez lorsque l'un des types de la source du journal configurée est la source de l'événement.	lorsque le ou les événements sont détectés par un ou plusieurs de **these log source**	**these log source** - Indiquez les sources du journal que ce test doive considérer.
Inactive Log Sources	Validez lorsque l'une des sources du journal configurées n'a pas généré un événement à l'heure configurée.	lorsque le ou les événements sont détectés par une ou plusieurs de **these log sources** pendant **this many** secondes	Configurez les paramètres suivants : **these log sources** - Indiquez les sources du journal que ce test doive considérer. **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération.
Log Source Groups	Validez lorsqu'un événement est détecté par les groupes de sources du journal configurés.	lorsque le ou les événements sont détectés par un ou plusieurs de **these log source groups**	**these log source groups** - Indiquez les groupes que cette règle doive prendre en considération.

Fonction - tests de séquence La fonction - les tests de séquence comprennent :

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Event Function	Vous pouvez utiliser les blocs de construction ou d'autres règles pour remplir aux conditions du 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 **rules, in|in any,** à partir de **the same|any source IP** vers **the same|any destination IP,** dans **this many seconds**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **in | in any** - Indiquez si ce test doive prendre en considération **in** ou **in any**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** sources configurées. • **username | source IP | source port | destination IP | destination port | QID | event ID | log source | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test doive prendre en considération **same** ou **any** destinations configurées. • **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 ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **seconds**.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (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 remplir aux conditions du test. Vous pouvez utiliser cette fonction pour détecter un nombre de règles spécifiées, en séquence, relatives à une source ou une destination dans un intervalle configuré.	lorsqu'au moins **this number** de ces **rules, in|in any,** à partir de **the same|any source IP** vers **the same|any destination IP**, dans **this many seconds**	Configurez les paramètres suivants : • **this number** - Indiquez le nombre de règles que vous souhaitez que cette fonction considère. • **rules** - Indiquez les règles que ce test doive prendre en considération. • **in | in any** - Indiquez si vous souhaitez que le test considère **in** ou **in any**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** sources configurées. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** destinations configurées. • **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 ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération.
Multi-Event Sequence Function Between Hosts	Vous permet de détecter une séquence des règles sélectionnées relatives aux mêmes hôtes source et de destination dans l'intervalle configuré. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour remplir aux conditions du test.	lorsque cette séquence de **rules**, relative au même hôte source et de destination dans **ce many seconds**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **seconds**.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (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 remplir aux conditions du test.	lorsqu'au moins **this many** de **rules, en in|in any,** avec le même **username** suivi par au moins **this many** de **rules en in| in any** de **to/from** la même **destination IP** que la séquence précédente, dans **this many minutes**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de règles que ce test doive prendre en considération. • **rules** - Indiquez les règles que ce test doive prendre 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'adresse IP source, le port source, l'adresse IP de destination, ou le port de destination. La valeur par défaut est **username**. • **this many** - Indiquez le nombre de règles que ce test doive prendre en considération. • **rules** - Indiquez les règles que ce test doive prendre 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 ce test doive prendre 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'adresse IP source, le port source, l'adresse 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 doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que cette règle doive prendre en considération. La valeur par défaut est **minutes**.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes et différentes propriétés d'événements dans un intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** dans **this many minutes** une fois que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.
Event Property Function	Vous permet de détecter un nombre de règles spécifiques configurées avec les mêmes propriétés d'événements dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **event properties this many minutes** une fois que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois défini avec des propriétés d'événements identiques et différentes dans un intervalle configuré après une série de règles spécifiques.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **event properties** et les **event properties** différentes dans **this many minutes** une fois que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois, configurées dans un intervalle configuré après qu'une série de règles spécifiques se produit avec des propriétés d'événements identiques.	lorsque **these rules** correspondent au moins à **this many** dans **this many minutes** une fois que **these rules** correspondent **aux propriétés d'événements**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsque les règles spécifiques se produisent un nombre de fois défini avec des propriétés d'événements identiques dans un intervalle configuré et une fois qu'une série de règles spécifiques se produit avec des propriétés d'événements identiques.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **event properties** dans **this many minutes** une fois que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **event properties** - Indiquez les propriétés d'événements que vous souhaitez affecter à ce test. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que vous souhaitez affecter à ce test. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois défini avec des propriétés d'événements identiques et différentes dans un intervalle configuré après qu'une série de règles spécifiques se produit avec les mêmes propriétés d'événements.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **event properties** dans **this many minutes** une fois que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsqu'un nombre spécifique d'événements se produit des propriétés d'événements identiques et différentes dans un intervalle après qu'une série de règles spécifiques se produit.	lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** et les **event properties** différentes dans **this many minutes** une fois que **these rules** correspondent	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **event properties** - Indiquez les propriétés d'événements que vous souhaitez affecter à ce test. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsqu'un nombre spécifique d'événements se produit avec les mêmes propriétés d'événements dans un intervalle configuré et après qu'une série de règles spécifiques se produit avec les mêmes propriétés d'événements.	lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** en **this many minutes** après que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-6 Règles d'événements : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsqu'un nombre spécifique d'événements se produit avec des propriétés d'événements identiques et différentes dans un intervalle configuré et après qu'une série de règles spécifiques se produit avec les mêmes propriétés d'événements.	lorsqu'au moins **this many** événements sont observés avec les mêmes **event properties** et les **event properties** différentes dans **this many minutes** une fois que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Fonction - tests de compteur La fonction - les tests de compteur comprennent :

Tableau A-7 Règles d'événements : Fonctions - Groupe de compteurs

Test	Description	Nom du test par défaut	Paramètres
Multi-Event Counter Function	Vous permet de tester le nombre d'événements 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 remplir aux conditions du test.	lorsqu'un(e) **source IP** correspond à **more than|exactly this many** de ces **rules** via **more than|exactly this many destination IP,** dans **this 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 ce test doive prendre en considération. La valeur par défaut est **source IP**. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère exactement le nombre de règles ou plus. • **this many** - Indiquez le nombre de règles que ce test doive prendre en considération. • **rules** - Indiquez les règles que ce test doive prendre en considération. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère le nombre exact d'adresses IP de destination, de ports de destination, de QID, d'ID d'événements source ou de sources de journal que vous avez sélectionnés dans la source précédente. • **this many** - Indiquez le nombre d'adresse IP, de ports, de QID, d'événements, de sources de journal ou des catégories que ce test doive prendre en considération. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que ce test doive prendre en considération. La valeur par défaut est **destination IP**. • **this many** - Indiquez le temps de la valeur que vous souhaitez affecter à ce test. • **seconds | minutes | hours | days** - Indiquez l'intervalle que cette règle doive prendre en considération. La valeur par défaut est **minutes**.

Tableau A-7 Règles d'événements : Fonctions - Groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Function	Vous permet de détecter une série de règles pour une adresse IP ou un port spécifique suivi par une série de règles spécifiques pour une adresse IP ou un port spécifique. Vous pouvez également utiliser les blocs de construction ou les règles existantes pour remplir aux conditions du test.	lorsque toutes ces **rules** ayant la même adresse **source IP** plus de **this many**, à travers **more than|exactly this many destination IP** dans **this many minutes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère le nombre exact d'adresses IP de destination, de ports de destination, de QID, d'ID d'événements source ou de sources du journal que vous sélectionnez dans la source précédente. • **this many** - Indiquez le nombre que ce test doive prendre en considération selon l'option configurée dans le paramètre IP source. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que ce test doive prendre en considération. La valeur par défaut est **destination IP**. • **this many** - Indiquez l'intervalle que vous souhaitez affecter à ce test. • **seconds | minutes | hours | days** - Indiquez l'intervalle que cette règle doive prendre en considération. La valeur par défaut est **minutes**.

Tableau A-7 Règles d'événements : Fonctions - Groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Username Function	Vous permet de détecter les diverses mises à jour des noms d'utilisateurs sur un hôte unique.	lorsque l'**username** change plus de **this many** dans **this many hours** sur un hôte unique.	Configurez les paramètres suivants : • **MAC | username | hostname** - Indiquez si vous souhaitez que ce test considère le nom d'utilisateur, l'adresse MAC ou le nom de l'hôte. La valeur par défaut est **username**. • **this many** - Indiquez le nombre de changements que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **hours**.
Event Property Function	Vous permet de détecter une série d'événements avec les mêmes propriétés d'événements dans l'intervalle configuré. Par exemple, si vous pouvez utiliser ce test lorsque 100 événements ayant la même adresse IP source se produisent dans les 5 minutes.	Lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** dans **this many minutes**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.

Tableau A-7 Règles d'événements : Fonctions - Groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter une série d'événements ayant des propriétés d'événements identiques et différentes dans l'intervalle configuré. Par exemple, si vous pouvez utiliser ce test pour détecter lorsque 100 événements ayant la même adresse IP source et une adresse IP de destination différente se produisent dans les 5 minutes.	Lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** et différentes **event properties** dans **this many minutes**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés propriétés d'événements normalisées et personnalisées. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes propriétés d'événements dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.

Tableau A-7 Règles d'événements : Fonctions - Groupe de compteurs (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'événements dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **event properties** dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.
Event Property Function	Vous permet de détecter un nombre de règles spécifiques avec des propriétés d'événements identiques et différentes dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes et différentes **event properties dans this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.

Fonction - tests simples La fonction - les tests simples :

Tableau A-8 Règles d'événements : Groupe Simple

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 remplir aux conditions du test. L'événement doit correspondre à l'une ou toutes les règles sélectionnées. Si vous souhaitez créer une instruction OR pour ce test de règles, spécifiez le paramètre **any**.	Lorsqu'un événement correspond à **any|all** les règles suivantes	Configurez les paramètres suivants : • **any | all** - Indiquez soit **any** ou **all** les règles configurées qui devraient s'appliquer à ce test. • **rules** - Indiquez les règles que ce test doive prendre en considération.

Tests Date/Heure Les dates et heures comprennent :

Tableau A-9 Règles d'événements : Tests Date/Heure

Test	Description	Nom du test par défaut	Paramètres
Event Day	Validez lorsque l'événement se produit à la date configurée.	lorsque les événements se produisent au **on** de la date **selected**	Configurez les paramètres suivants : • **on | after | before** - Indiquez si vous souhaitez que ce test considère avant, après ou à la date configurée. La valeur par défaut est **on**. • **selected** - Indiquez le jour du mois que ce test doive prendre en considération.
Event Week	Validez lorsque l'événement se produit pendant les jours de semaine configurés.	lorsque les événements se produisent dans l'un de **these days of the week**	**these days of the week** - Indiquez les jours de la semaine que ce test doive prendre en considération.
Event Time	Validez lorsque l'événement se produit avant, après ou à l'heure configurée.	lorsque les événements se produisent **after this time**	Configurez les paramètres suivants : • **after | before | at** - Indiquez si vous souhaitez que ce test considère avant, après ou à l'heure configurée. La valeur par défaut est **after**. • **this time** - Indiquez l'heure que ce test doive prendre en considération.

Tests de propriété du réseau Le test de la propriété du réseau comprend :

Tableau A-10 Règles d'événements : Tests de propriétés du réseau

Test	Description	Nom du test par défaut	Paramètres
Local Networks	Validez lorsque l'événement se produit dans le réseau spécifié.	lorsque le réseau local est **one of the following networks**	**one of the following networks** - Indiquez les zones du réseau dans lesquelles vous souhaitez appliquer ce test.
Remote Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux distants.	lorsque **source IP** fait partie d'un **remote network locations 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 dans lesquels vous souhaitez effectuer ce test.
Remote Services Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux des services distants configurés.	lorsque **source IP** fait partie d'un**remote services network locations suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • **remote services network locations** - Indiquez les emplacements réseau de services dans lesquels vous souhaitez effectuer ce test.
Geographic Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements des réseaux géographiques configurés.	lorsque **Source IP** fait partie d'un **geographic network locations 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 réseaux que ce test doive prendre en considération.

Fonction - tests négatifs La fonction - les tests négatifs comprennent :

Tableau A-11 Règles d'événements : Fonctions - Groupe négatif

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsqu'aucune des règles spécifiées dans un intervalle configuré après une série de règles spécifiques ne se produit avec les mêmes propriétés d'événements	Lorsqu'aucune de **these rules** ne correspond dans **this many minutes** après que**these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.
Rule Function	Vous permet d'être alerté lorsqu'aucune de ces règles spécifiées dans un intervalle configuré après qu'une série de règles ne se produit.	Lorsqu'aucune de **these rules** ne correspond dans **this many minutes** après que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tests de règle de flux

Cette section fournit des informations sur les tests de règles de flux que vous pouvez appliquer à la règle notamment :

- **Tests de profil d'hôte**
- **Tests IP/Port**

- **Tests de propriété de flux**
- **Tests de propriété communs**
- **Fonction - tests de séquence**
- **Fonction - tests de compteur**
- **Fonction - tests simples**
- **Tests Date/Heure**
- **Tests de propriété du réseau**
- **Fonction - tests négatifs**

Tests de profil d'hôte Les tests de profil d'hôte comprennent :

Tableau A-12 Règles de flux : Tests de profil d'hôte

Test	Description	Nom du test par défaut	Paramètres
Host Profile Port	Validez lorsque le port est ouvert sur une source ou une destination locale configurée. Vous pouvez également spécifier si le statut du port est détecté en utilisant l'une des méthodes suivantes : • **Active** - QRadar SIEM recherche activement le port configuré via l'évaluation ou l'analyse de la vulnérabilité. • **Passive** - QRadar SIEM surveille passivement le réseau en enregistrant les hôtes déjà détectés.	lorsque le port de destination de l'hôte **source** est ouvert **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 considère l'analyse active ou passive ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.
Host Existence	Validez 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 de l'hôte est détecté en utilisant l'une des méthodes suivantes : • **Active** - QRadar SIEM recherche activement le port configuré via l'évaluation ou l'analyse de la vulnérabilité. • **Passive** - QRadar SIEM surveille passivement le réseau en enregistrant 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 considère l'analyse active ou passive ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.

Tableau A-12 Règles de flux : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Host Profile Age	Validez lorsque la source locale ou de destination est supérieure à la valeur configurée dans les intervalles configurés.	lorsque l'âge du profil d'hôte **source** est **greater than this number of time intervals**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test s'applique à l'hôte source ou de destination. La valeur par défaut est **source**. • **greater than | less than** - Indiquez si vous souhaitez que ce test considère les valeurs supérieures ou inférieures à l'âge de l'hôte du profil. • **this number of** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **time intervals** - Indiquez si vous souhaitez que le test considère les minutes ou les heures.
Host Port Age	Validez lorsque l'âge du profil du port source ou de destination est supérieur ou inférieur au temps configuré.	lorsque l'âge du port du profil de l'hôte **source** est **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 considère les valeurs supérieures ou inférieures à l'âge du port du profil. La valeur par défaut est **greater than**. • **this number of** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **time intervals** - Indiquez si vous souhaitez que le test considère les minutes ou les heures.

Tableau A-12 Règles de flux : Tests de profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Asset Weight	Validez lorsque l'unité (de destination) attaquée ou l'hôte attaquant (source) a une pondération assignée supérieure ou inférieure à la valeur configurée.	lorsque l'actif de **destination** a une pondération **greater than this weight**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test considère l'actif source et de destination. La valeur par défaut est **destination**. • **greater than | less than | equal to** - Indiquez si vous souhaitez que la valeur soit supérieure, inférieure ou égale à la valeur configurée. • **this weight** - Indiquez le poids que ce test doive prendre en considération.
OSVDB IDs	Validez lorsqu'une adresse IP (source, de destination ou quelconque) est vulnérable aux ID Open Source Vulnerability Database (OSVDB) configurés.	lorsque la **source IP** est vulnérable à l'un des **OSVDB ID suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est **source IP**. • **OSVDB IDs** - Indiquez n'importe quel ID OSVDB que vous souhaitez que le test considère. Pour plus d'informations sur les ID OSVDB, consultez *http://osvdb.org/*.

Tests IP/Port Les tests IP/Port comprennent :

Tableau A-13 Règles de flux : Groupe de tests IP/Port

Test	Description	Nom du test par défaut	Paramètres
Source Port	Validez lorsque le port de la source du flux est l'un des ports source configurés.	lorsque le port source est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Destination Port	Validez lorsque le port de destination du flux est l'un des ports de destination configurés.	lorsque le port de destination est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Local Port	Validez lorsque le port local du flux est l'un des ports locaux configurés.	lorsque le port local est l'un des ports suivants	**ports** - Indiquez les ports que ce test doive prendre en considération.

Tableau A-13 Règles de flux : Groupe de tests IP/Port (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Port	Validez lorsque le port distant du flux est l'un des ports distants configurés.	lorsque le port distant est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Source IP Address	Validez lorsque l'adresse IP source du flux est l'une des adresses IP configurées.	lorsque l'adresse IP source est l'une des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Destination IP Address	Validez lorsque l'adresse IP de destination du flux est l'une des adresses IP configurées.	lorsque l'adresse IP de destination fait partie des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Local IP Address	Validez lorsque l'adresse IP local du flux est l'une des adresses IP configurées.	lorsque l'adresse IP locale est l'une des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Remote IP Address	Validez lorsque l'adresse IP distante du flux est l'une des adresses IP configurées.	lorsque l'adresse IP distante est l'une des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
IP Address	Validez lorsque l'adresse IP de destination ou source du flux est l'une des adresses IP configurées.	lorsque l'adresse IP source ou de destination est l'une des **IP addresses suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Source or Destination Port	Validez lorsque le port source ou de destination est l'un des ports configurés	lorsque le port source ou de destination est l'un de **these ports**	**these ports** - Indiquez les ports que ce test doive prendre en considération.

Tests de propriété de flux Le test de propriétés de flux comprend :

Tableau A-14 Règles de flux : Tests de propriétés de flux

Test	Description	Nom du test par défaut	Paramètres
IP Protocol	Validez lorsque le protocole IP du flux est l'un des protocoles configurés.	lorsque le protocole IP est l'un des **protocols suivants**	**protocols** - Indiquez les protocoles que vous souhaitez ajouter à ce test.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
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. Validez si le contexte du flux 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 dans lequel vous souhaitez effectuer ce test. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Validez lorsque l'adresse IP source de l'événement est locale ou distante.	lorsque la source est **local or remote {par défaut : remote}**	**local | remote** - Indiquez un trafic local ou distant. La valeur par défaut est **remote**.
Destination Location	Validez lorsque l'adresse IP de destination du flux est locale ou distante.	lorsque la destination est **local or remote {par défaut : remote}**	**local | remote** - Indiquez un trafic local ou distant. La valeur par défaut est **remote**.
Geographic Location	Validez lorsque l'adresse IP source correspond à l'emplacement géographique configuré.	lorsque la source est localisée dans cette **geographic region**	**geographic location** - Sélectionnez un emplacement géographique.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	Validez lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé à une chaîne d'expressions régulières particulières ***Remarque :*** *Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez les modèles d'expressions régulières personnalisés, acceptez les règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.*	lorsque l'**username** correspond au **regex**	Configurez les paramètres suivants : • **hostname | source hostname |destination hostname | source payload | destination payload** - Indiquez la valeur que vous souhaitez associer à ce test. La valeur par défaut est **username**. • **regex** - Indiquez la chaîne d'expression régulière que ce test doive prendre en considération.
IPv6	Validez lorsque l'adresse IPv6 de destination ou source correspond à l'adresse IP configurée.	lorsque **source IP (v6)** fait partie des **IP (v6) addresses suivantes**	Configurez les paramètres suivants : • **source IP (v6) | destination IP (v6)** - Indiquez si vous souhaitez que ce test considère l'adresse IPv6 source ou de destination. • **IP (v6) addresses** - Indiquez les adresses IPv6 que ce test doive prendre en considération.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Set	Validez lorsque l'une ou toutes les propriétés du flux sont comprises dans l'un ou tous les ensembles de référence configurés.	lorsqu'**any** de **these flow properties** est compris dans **any** of **these reference set(s)**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** ensembles de référence configurés. • **these reference set(s)** - Indiquez les ensembles de référence que ce test doive prendre en considération.
Reference Map	Validez lorsque l'une ou toutes les propriétés de flux dans une paire clé ou de valeur configurée sont comprises dans l'une ou toutes les cartes de référence configurées.	lorsqu'**any** de **these flow properties** est la clé et **any** de **these flow properties** est la valeur dans **any** de **these reference maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération • **these reference maps** - Indiquez les cartes de référence que ce test doive prendre en considération.
Reference Map of Sets	Validez lorsque l'une ou toutes les propriétés de flux dans une paire clé ou de valeur configurée sont comprises dans l'un ou tous les ensembles de référence configurés.	lorsqu'**any** de **these flow properties** est la clé et **any** de **these flow properties** est la valeur dans **any** de **these reference maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. • **these reference map of sets** - Indiquez les ensembles de cartes de référence que ce test doive prendre en considération.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Map of Maps	Validez lorsque l'une ou toutes les propriétés de flux dans une paire clé ou de valeur primaire et secondaire configurée sont comprises dans l'un ou tous les ensembles de cartes de cartes de référence configurées.	lorsqu'**any** de **these flow properties** est la clé de la première carte et **any** de **these flow properties** est la clé de la seconde carte et **any** de **these flow properties** est la valeur dans **these reference map of maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération • **these reference map of maps** - Indiquez les cartes des cartes de référence que ce test doive considérer.
Flow Bias	Validez lorsque la direction du flux correspond à la tendance du flux configuré.	lorsque la tendance du flux est l'une des **bias suivantes**	**inbound | outbound | mostly inbound | mostly outbound | balanced** - Indiquez la tendance du flux que ce test doive prendre en considération. La valeur par défaut est **inbound**.
Byte / Packet Count	Validez lorsque le nombre d'octets ou de paquets correspond à la quantité configurée.	lorsque les **source bytes** sont **greater than this amount**	Configurez les paramètres suivants : • **source | destination | local | remote** - Indiquez si vous souhaitez que le test considère les paquets ou les octets locaux ou distants de la source ou de la destination. La valeur par défaut est **source**. • **bytes | packets**- Indiquez si vous souhaitez que le test considère les paquets ou les octets. La valeur par défaut est **bytes**. • **greater than | less than | equal to** - Indiquez si le nombre d'octets ou de paquets est supérieur, inférieur ou égal à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
Host Count	Validez lorsque le nombre d'hôtes correspond à la quantité configurée.	lorsque le nombre d'hôtes **source** est **greater than this amount**.	Configurez les paramètres suivants : • **source | destination | local | remote** - Indiquez si vous souhaitez que ce test considère les hôtes distants, locaux, de destination ou source. La valeur par défaut est **source**. • **greater than | less than | equal to** - Indiquez si le nombre d'hôte est supérieur, inférieur ou égal à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.
Packet Rate	Validez lorsque le taux de paquets correspond à la quantité configurée.	lorsque le taux de paquets **source** est **greater than value** de paquets ou de secondes	Configurez les paramètres suivants : • **source | destination | local | remote** - Indiquez si vous souhaitez que ce test considère le taux de paquets locaux ou distants, source ou de destination. La valeur par défaut est **source**. • **greater than | less than | equal to** - Indiquez si le taux de paquets est supérieur, inférieur ou égal à la valeur configurée. • **0** - Indiquez la valeur que ce test doive considérer. La valeur par défaut est **0**.
Flow Duration	Validez lorsque la durée du flux correspond à l'intervalle configuré.	lorsque la durée du flux est **greater than value seconds**	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 ce test doive prendre en considération. La valeur par défaut est **0**. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**.

Tableau A-14 Règles de flux : Tests de propriétés de flux (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 chaîne de recherche entrée est inclue n'importe où dans le contenu de l'événement.	lorsque le contenu de la **source** correspond au **regex string**	Configurez les paramètres suivants : • source | destination | local | remote - Indiquez si vous souhaitez que ce critère considère le contenu local ou distant, source ou de destination. La valeur par défaut est **source**. • matches the regex | matches the hexadecimal - Indiquez si vous souhaitez faire correspondre à une expression régulière ou une chaîne hexadécimale. La valeur par défaut est **regex**. • **string** - Indiquez la chaîne de texte que vous souhaitez inclure dans ce test.
Flow Source Name	Validez lorsque le nom de la source de flux correspond aux valeurs configurées.	lorsque le nom de la source de flux est l'un de **these source**	**these sources** - Indiquez les noms de la source que ce test doive prendre en considération.
Flow Interface	Validez lorsque l'interface de flux correspond aux valeurs configurées.	lorsque l'interface du flux est l'une des **these interfaces**	**these interfaces** - Indiquez l'interface de flux que ce test doive prendre en considération.
Flow Type	Validez lorsque le type de flux correspond aux valeurs configurées.	lorsque le type du flux est l'un de **these flow types**	**these flow types** - Indiquez le type de flux que ce test doive prendre en considération.
Byte/Packet Ratio	Validez lorsque le rapport octet/paquet correspond à la valeur configurée.	lorsque le rapport octet/paquet de la **source** est **greater than value** octets/paquet	Configurez les paramètres suivants : • source | destination | local | remote - Indiquez si vous souhaitez que ce critère considère le rapport octet/paquet local ou distant, source ou de destination. La valeur par défaut est **source**. • **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 le test considère.
ICMP Type	Validez lorsque le type Internet Control Message Protocol (ICMP) correspond aux valeurs configurées.	lorsque le type ICMP est l'un des **these types**	**these types** - Indiquez les types ICMP que ce test doive prendre en considération.
ICMP Code	Validez lorsque le code ICMP correspond aux valeurs configurées.	lorsque le code ICMP est l'un de **these codes**	**these codes** - Indiquez les codes ICMP que ce test doive prendre en considération.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
DSCP	Validez lorsque le code de services différenciés (DSCP) correspond aux valeurs configurées.	lorsque le DSCP de **destination** est l'un de **these values**	Configurez les paramètres suivants : • source | destination | local | remote | either - Indiquez si vous souhaitez que ce test considère soit le DSCP source, de destination, local, ou distant. La valeur par défaut est **destination**. • **these values** - Indiquez les valeurs DSCP que ce test doive prendre en considération.
IP Precedence	Validez lorsque la priorité de l'IP correspond aux valeurs configurées	lorsque la priorité de l'IP de **destination** est l'une de **these values**	Configurez les paramètres suivants : • source | destination | local | remote | either - Indiquez si vous souhaitez que ce test considère le DSCP source, de destination, local ou distant. La valeur par défaut est **destination**. • **these values** - Indiquez les valeurs de priorité IP que ce test doive prendre en considération.
Packet Ratio	Validez lorsque le rapport 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 **greater than this value**	Configurez les paramètres suivants : • source | destination | local | remote - Spécifiez la direction que ce test doive prendre en considération en tant que valeur précédente du rapport. La valeur par défaut est **source**. • **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 le test considère.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
TCP Flags	Validez lorsque les indicateurs TCP correspondant aux valeurs configurées.	lorsque les indicateurs TCP de **destination are exactly these flags**	Configurez les paramètres suivants : • source | destination | local | remote - Indiquez si vous souhaitez que ce critère considère les indicateurs TCP source, de destination, local ou distant. La valeur par défaut est **destination**. • **are exactly | includes all of | includes any of** - Indiquez si vous souhaitez que ce test considère exactement tous ou aucun des indicateurs TCP configurés. La valeur par défaut est **are exactly**. • **these flags** - Indiquez les indicateurs TCP que ce test doive prendre en considération.
IF Index	Validez lorsque l'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 ce test doive prendre en considération. La valeur par défaut est **input**. • **all | any** - Indiquez si vous souhaitez que ce test considère toute ou n'importe quelle valeur IF Index configurée. • **these values** - Indiquez les indexes IF que ce test doive prendre en considération.
TCP Flag Combination	Validez lorsque les indicateurs TCP correspondent aux combinaisons d'indicateur configurées.	lorsque les indicateurs TCP de **destination** sont de **these flag combinations**	Configurez les paramètres suivants : • source | destination | local | remote - Indiquez si vous souhaitez que ce critère considère les indicateurs TCP source, de destination, local ou distant. La valeur par défaut est **destination**. • **these flag combinations** - Indiquez les combinaisons d'indicateurs que ce test doive prendre en considération. Indicateurs séparés par des virgules.
Search Filter	Validez lorsque le flux correspond au filtre de recherche spécifié.	lorsque le flux correspond à **this search filter**	**this search filter** - Indiquez le filtre de recherche que ce test doive prendre en considération.

Tableau A-14 Règles de flux : Tests de propriétés de flux (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Payload	Validez lorsque la partie spécifiée du flux possède ou ne possède pas un contenu.	lorsque la partie de **destination** du flux **has** des données de contenu	Configurez les paramètres suivants : • **the source | the destination | the local | the remote | either** - Indiquez si vous souhaitez que ce test le flux source, de destination, local, distant ou quelque soit le côté du flux. La valeur par défaut est **destination**. • **has | has not** - Indiquez si vous souhaitez que ce test considère les flux qui ont ou n'ont pas de contenu.

Tests de propriété communs La date et l'heure comprennent :

Tableau A-15 Règles de flux : Tests de propriété communs

Test	Description	Nom du test par défaut	Paramètres
CVSS Risk (Host)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque l'hôte de **destination** possède une valeur de risque CVSS **supérieure à cette valeur**	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 de risque CVSS est supérieure, inférieure ou égale à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.
CVSS Risk (Port)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque le port de **destination** possède une valeur de risque CVSS **greater than this amount**	• **source | destination | either** - Indiquez si le test prend en considération le port source ou de destination du flux. • **greater than | less than | equal to** - Indiquez si vous souhaitez que le niveau de menace soit supérieur, inférieur ou égal à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.

Tableau A-15 Règles de flux : Tests de propriété communs (suite)

Test	Description	Nom du test par défaut	Paramètres
Custom Rule Engine	Validez lorsque le flux est traité par des moteurs de règles personnalisées spécifiées.	lorsque le flux est traité par l'un de **These** Custom Rule Engines	**these** - Indiquez le Custom Rule Engine que vous souhaitez que le test considère.
Regex	Validez lorsque la propriété configurée est associée à une chaîne d'expressions régulières particulières (expression régulière). ***Remarque :*** *Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez les modèles d'expressions régulières personnalisés, acceptez les règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.*	lorsque **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'événements et de flux normalisées et personnalisées. • **regex** - Indiquez la chaîne d'expression régulière que ce test doive prendre en considération.
Hexadecimal	Validez lorsque la propriété configurée est associée à une valeur hexadécimale.	Si aucune de **these properties** ne contient de **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'événements et de flux normalisées et personnalisées. • **these hexadecimal values** - Indiquez les valeurs hexadécimales que vous ce test doive prendre en considération.

Fonction - tests de séquence La fonction : les tests de séquences comprennent :

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences

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 remplir aux conditions du 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 **rules, in|in any,** à partir de **the same|any source IP** vers **the same|any destination IP,** dans **this many seconds**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **in | in any** - Indiquez si ce test doive prendre en considération **in** ou **in any**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** sources configurées. • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** destinations configurées. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est **destination IP**. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **seconds**.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Flow Function	Vous permet d'utiliser les blocs de construction ou d'autres règles pour remplir aux conditions du test. Vous pouvez utiliser cette fonction pour détecter un nombre de règles spécifiées, en séquence, relatives à une source ou une destination dans un intervalle configuré.	lorsqu'au moins **this number** de ces **rules, in|in any, à partir de the same| any source IP** vers **the same|any destination IP** dans **this many seconds**	Configurez les paramètres suivants : • **this number** - Indiquez le nombre de règles que vous souhaitez que cette fonction considère. • **rules** - Indiquez les règles que ce test doive prendre en considération. • **in | in any** - Indiquez si vous souhaitez que le test considère **in** ou **in any**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** sources configurées. • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** destinations configurées. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est **destination IP**. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Flow Sequence Function Between Hosts	Vous permet de détecter une séquence des règles sélectionnées relatives aux mêmes hôtes source et de destination dans l'intervalle configuré. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour remplir aux conditions du test.	lorsque cette séquence de **rules**, relative au même hôte source et de destination dans **this many seconds**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre 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 de flux dans l'intervalle configuré.	lorsque **these rules** correspondent à au moins **this many** dans **this many minutes** après que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (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 configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **flow properties** dans **this many minutes** une fois **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois, configurées avec des propriétés de flux identiques et des propriétés de flux différentes dans un intervalle configuré après une série de règles spécifiques.	lorsque **these rules** correspondent à au moins **this many** avec les mêmes **flow properties** dans **this many minutes** après que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois défini dans un intervalle une fois qu'une série de règles spécifiques se produit avec des propriétés de flux similaires.	lorsque **these rules** correspondent à au moins **this many** dans **this many minutes** une fois **these rules** correspondent avec les mêmes **flow properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet de détecter les règles spécifiques se produisent un nombre de fois défini avec les mêmes propriétés de flux dans un intervalle configuré et une fois qu'une série de règles spécifiques se produit avec les mêmes propriétés de flux.	lorsque **these rules** correspondent à au moins **this many** avec les mêmes **flow properties** dans **this many minutes** une fois **these rules** correspondent les mêmes **flow properties**	Configurez les paramètres suivants : • **these** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these** - Indiquez les règles que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet d'être alerté lorsque les règles spécifiques se produisent un nombre de fois, configurées avec les mêmes ou différentes propriétés de flux dans un intervalle configuré et une fois qu'une série de règles spécifiques se produit avec les mêmes propriétés de flux.	lorsque **these rules** correspondent à au moins **this many** avec les mêmes **flow properties** et différentes **flow properties** dans **this many minutes** une fois **these rules** correspondent avec les mêmes **flow properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet d'être alerté lorsqu'un nombre spécifique de flux se produit avec des propriétés identiques et différentes de flux dans un intervalle configuré après qu'une série de règles spécifiques se produit.	lorsqu'au moins **this many** flux sont observés avec les mêmes **flow properties** et différentes **flow properties** dans **this many minutes** une fois que **these rules** correspondent.	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (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 configuré une fois qu'une série de règles spécifiques se produit avec les mêmes propriétés de flux.	Lorsqu'au moins **this many** flows sont observés avec les mêmes **flow properties** dans **this many minutes** une fois **these rules** correspondent avec les mêmes **flow properties**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Tableau A-16 Règles de flux : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet d'être alerté lorsqu'un nombre spécifique de flux se produit avec des propriétés identique et différentes dans un intervalle configuré une fois qu'une série de règles spécifiques se produit avec les mêmes propriétés de flux.	Lorsqu'au moins **this many** flux sont affichés avec les mêmes **flow properties** et différentes **flow properties**dans **this many minutes** après **these rules** correspondent avec les mêmes **flow properties**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.

Fonction - tests de compteur La 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'événements 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 remplir aux conditions du test.	lorsqu'une **source IP** correspond à **more than|exactly this many** de ces **rules** via **more than|exactly this many destination IP,** dans **this many minutes**	Configurez les paramètres suivants : • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère exactement le nombre de règles ou plus. • **this many** - Indiquez le nombre de règles que ce test doive prendre en considération. • **rules** - Indiquez les règles que ce test doive prendre en considération. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère le nombre exact d'adresses IP de destination, de ports de destination, de QID, d'ID d'événements source ou de sources de journal que vous sélectionnez dans la source préxédente. • **this many** - Indiquez le nombre d'adresses IP, ports ou noms d'utilisateur que vous souhaitez que le test considère. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que ce test doive prendre en considération. La valeur par défaut est **destination IP**. • **this many** - Indiquez le temps de la valeur que vous souhaitez affecter à ce test. • **seconds | minutes | hours | days** - Indiquez l'intervalle que cette règle doive prendre en considération. La valeur par défaut est **minutes**.

Tableau A-17 Règles de flux : Fonctions - Groupe de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Function	Vous permet de détecter une série de règles pour une adresse IP ou un port spécifique par une série de règles spécifiques pour une adresse IP ou un port spécifique. Vous pouvez également utiliser les blocs de construction ou les règles existantes pour remplir aux conditions du test.	lorsque toutes ces **rules** ayant la même adresse **source IP** plus de **this many**, à travers **more than|exactly this many destination IP** dans **this many minutes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère le nombre exact d'adresses IP de destination, de ports de destination, de QID, d'ID d'événements source ou de sources log que vous sélectionnez dans la source préxédente. • **this many** - Indiquez le nombre que ce test doive prendre en considération selon l'option configurée dans le paramètre **source IP**. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que ce test doive prendre en considération. La valeur par défaut est **destination IP**. • **this many** - Indiquez l'intervalle que vous souhaitez affecter à ce test. • **seconds | minutes | hours | days** - Indiquez l'intervalle que cette règle doive 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 une série d'événements avec les mêmes propriétés d'événements dans l'intervalle configuré. Par exemple, si vous pouvez utiliser ce test pour détecter lorsque 100 événements avec la même adresse IP source se produisent dans les 5 minutes.	Lorsqu'au moins **this many** flux sont affichés avec les mêmes **flow properties** dans **this many minutes**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.
Flow Property Function	Vous permet de détecter une série d'événements avec les mêmes et différentes propriétés d'événements dans l'intervalle 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 les 5 minutes.	Lorsqu'au moins **this many** flux sont affichés avec les mêmes **flow properties** et différentes **flow properties** dans **this many minutes**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre de flux que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. 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 configuré.	lorsque **these rules** correspondent au moins à **this many** dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. 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 configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **flow properties** dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. 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 différentes propriétés de flux dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **flow properties** et différentes **flow properties** dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.

Fonction - tests simples La fonction - les tests simples :

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 remplir aux conditions du test. La violation doit correspondre à une ou toutes les règles sélectionnées. Si vous souhaitez créer une instruction OR pour ce test de règles, spécifiez le paramètre **any**.	Lorsqu'un flux correspond à **any|all** des **rules suivantes**	Configurez les paramètres suivants : • **any | all** - Indiquez **any** ou **all** règles configurées qui devraient s'appliquer à ce test. • **rules** - Indiquez les règles que ce test doive prendre en considération.

Tests Date/Heure Les tests de dates et d'heures comprennent :

Tableau A-19 Règles de flux : Tests Date/Heure

Test	Description	Nom du test par défaut	Paramètres
Flow Day	Validez lorsque le flux se produit au jour du mois configuré.	lorsque le ou les flux se produisent au **on** du jour du mois **selected**	Configurez les paramètres suivants : • **on | after | before** - Indiquez si vous souhaitez que ce test considère avant, après ou à la date configurée. La valeur par défaut est **on**. • **selected** - Indiquez le jour du mois que ce test doive considérer.
Flow Week	Validez lorsque le flux se produit pendant les jours du mois configurés.	lorsque le ou les flux se produisent à l'un de **these days of the week**	**these days of the week** - Indiquez les jours de la semaine que ce test doive prendre en considération.
Flow Time	Validez lorsque le flux se produit avant, après ou à l'heure configurée.	lorsque le ou les flux se produisent **after this time**	Configurez les paramètres suivants : • **after | before | at** - Indiquez si vous souhaitez que le test considère avant, après ou à la date configurée. La valeur par défaut est **after**. • **this time** - Indiquez l'heure que ce test doive prendre en considération.

Tests de propriété du réseau Le test de la propriété du réseau comprend :

Tableau A-20 Règles de flux : Tests de propriétés du réseau

Test	Description	Nom du test par défaut	Paramètres
Local Network Object	Validez lorsque le flux se produit dans le réseau spécifié.	lorsque le réseau local est **one of the following**	**one of the following networks** - Indiquez les zones du réseau sur lesquelles vous souhaitez appliquer ce test.
Remote Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux distants.	lorsque **source IP** fait partie d'un **remote network locations suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est **source IP**. • **remote network locations** - Indiquez les emplacements réseau dans lesquels vous souhaitez effectuer ce test.

Tableau A-20 Règles de flux : Tests de propriétés du réseau (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Services Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux des services distants configurés.	lorsque **source IP** fait partie d'un **remote services network locations suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est **source IP**. • **remote services network locations** - Indiquez les emplacements réseau de services distants dans lesquels vous souhaitez effectuer ce test.
Geographic Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements des réseaux géographiques configurés.	lorsque **source IP** fait partie de l'un des emplacements géographiques de réseaux suivants	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est **source IP**. • **geographic network locations** - Indiquez les emplacements réseaux que ce test doive prendre en considération.

Fonction - tests négatifs La fonction - les tests négatifs comprennent :

Tableau A-21 Règles de flux : Fonctions : Groupe négatif

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet d'être alerté lorsque des règles spécifiées se produisent dans un intervalle configuré après qu'une série de règles spécifiques se produit avec les mêmes propriétés de flux.	Lorsqu'aucune de **these rules** ne correspond dans **this many minutes** après que **these rules** correspondent aux mêmes **flow properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.
Rule Function	Vous permet d'être alerté lorsqu'aucune de ces règles spécifiées ne se produit dans un intervalle configuré après qu'une série de règles se produit.	Lorsqu'aucune de **these rules** ne correspond dans **this many minutes** après que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tests de règle communs

Cette section fournit des informations sur les tests de règles communes que vous pouvez appliquer à l'événement et à l'enregistrement de flux à la fois notamment :

- **Tests de profil d'hôte**
- **Tests IP/Port**
- **Tests de propriété communs**

- **Fonctions - tests de séquence**
- **Fonction - tests de compteur**
- **Fonction - tests simples**
- **Tests Date/Heure**
- **Tests de propriété du réseau**
- **Fonctions - tests négatifs**

Tests de profil d'hôte Les tests de profil d'hôte comprennent :

Tableau A-22 Règles communes : Tests du profil d'hôte

Test	Description	Nom du test par défaut	Paramètres
Host Profile Port	Validez lorsque le port est ouvert sur une source ou une destination locale configurée. Vous pouvez également spécifier si le statut du port est détecté en utilisant l'une des méthodes suivantes : • **Active** - QRadar SIEM recherche activement des ports configurés via l'évaluation de la vulnérabilité et de l'analyse. • **Passive** - QRadar SIEM surveille passivement le réseau en enregistrant les hôtes déjà détectés.	lorsque le port de destination de l'hôte **source** est ouvert **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 considère l'analyse active ou passive ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.
Host Existence	Validez 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 de l'hôte est détecté en utilisant l'une des méthodes suivantes : • **Active** - QRadar SIEM recherche activement le port configuré via l'évaluation ou l'analyse de la vulnérabilité. • **Passive** - QRadar SIEM surveille passivement le réseau en enregistrant 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 considère l'analyse active ou passive ou les deux à la fois. La valeur par défaut est **either actively or passively seen**.

Tableau A-22 Règles communes : Tests du profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Host Profile Age	Validez lorsque la source locale ou de destination est supérieure à la valeur configurée dans les intervalles configurés.	lorsque l'âge du profil d'hôte **source** est **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 considère les valeurs supérieures ou inférieures à l'âge du port du profil. • **this number of** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **time intervals** - Indiquez si vous souhaitez que le test considère les minutes ou les heures.
Host Port Age	Validez 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 du profil de l'hôte **source** est **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 considère les valeurs supérieures ou inférieures à l'âge du port du profil. La valeur par défaut est **greater than**. • **this number of** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **time intervals** - Indiquez si vous souhaitez que le test considère les minutes ou les heures.

Tableau A-22 Règles communes : Tests du profil d'hôte (suite)

Test	Description	Nom du test par défaut	Paramètres
Asset Weight	Validez lorsque l'unité (de destination) attaquée ou l'hôte attaquant (source) a une pondération assignée supérieure ou inférieure à la valeur configurée.	lorsque l'actif de **destination** a une pondération **greater than this weight**	Configurez les paramètres suivants : • **source | destination** - Indiquez si vous souhaitez que ce test considère l'actif source et de destination. La valeur par défaut est **destination**. • **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 la pondération que ce test doive prendre en considération.
OSVDB IDs	Validez lorsqu'une adresse IP (source ou de destination) est vulnérable aux ID Open Source Vulnerability Database (OSVDB) configurés.	lorsque la **source IP** est vulnérable à l'un des **OSVDB ID suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. La valeur par défaut est **source IP**. • **OSVDB IDs** - Indiquez n'importe quel ID OSVDB que vous souhaitez que le test considère. Pour plus d'informations sur les ID OSVDB, consultez *http://osvdb.org/*.

Tests IP/Port Les tests IP/Port comprennent :

Tableau A-23 Règles communes : Groupe de tests IP/Port

Test	Description	Nom du test par défaut	Paramètres
Source Port	Validez lorsque le port source de l'événement ou du flux fait partie des ports source configurés.	lorsque le port source est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Destination Port	Validez lorsque le port de destination de l'événement ou du flux fait partie des ports de destinations configurés.	lorsque le port de destination est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.

Tableau A-23 Règles communes : Groupe de tests IP/Port (suite)

Test	Description	Nom du test par défaut	Paramètres
Local Port	Validez lorsque le port local de l'événement ou du flux fait partie des ports locaux configurés.	lorsque le port local est l'un des ports suivants	**ports** - Indiquez les ports que ce test doive prendre en considération.
Remote Port	Validez lorsque le port distant de l'événement ou du flux fait partie des ports distants configurés.	lorsque le port distant est l'un des **ports suivants**	**ports** - Indiquez les ports que ce test doive prendre en considération.
Source IP Address	Validez lorsque l'adresse IP source de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'adresse IP source est l'une des **adresses IP suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Destination IP Address	Validez lorsque l'adresse IP de destination de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'adresse IP de destination fait partie des **adresses IP suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Local IP Address	Validez lorsque l'adresse IP locale de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'adresse IP locale est l'une des adresses IP suivantes	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Remote IP Address	Validez lorsque l'adresse IP distante de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'adresse IP distante est l'une des **adresses IP suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
IP Address	Validez lorsque l'adresse IP source ou de destination de l'événement ou du flux fait partie des adresses IP configurées.	lorsque l'adresse IP source ou de destination est l'une des **adresses IP suivantes**	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération.
Source or Destination Port	lorsque le port source ou de destination est l'un des ports configurés	lorsque le port source ou de destination est l'un de **these ports**	**these ports** - Indiquez les ports que ce test doive prendre en considération.

Tests de propriété communs Les tests de propriété communs comprennent :

Tableau A-24 Règles communes : Tests de propriété communs

Test	Description	Nom du test par défaut	Paramètres
IP Protocol	Validez lorsque le protocole IP de l'événement ou du flux est l'un des protocoles configurés.	lorsque le protocole IP est l'un des **protocols suivants**	**protocols** - Indiquez les protocoles que vous souhaitez ajouter à ce test.

Tableau A-24 Règles communes : Tests de propriété communs (suite)

Test	Description	Nom du test par défaut	Paramètres
Payload Search	Cet 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 le flux source ou le contenu de destination contient **this string**	**this string** - Indiquez la chaîne de texte que vous souhaitez inclure pour ce test.
Context	Le contexte est la relation entre la source et la destination de l'événement ou du flux. Par exemple, une source locale vers une destination distante. Validez si le contexte est l'une des options suivantes : • Local to Local • Local to Remote • Remote to Local • Remote to Remote	lorsque le contexte est **this context**	**this context** - Indiquez le contexte dans lequel vous souhaitez effectuer ce test. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Validez lorsque la source est locale ou distante.	lorsque la source est **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**
Destination Location	Validez lorsque l'adresse IP de destination du flux ou de l'événement est locale ou distante.	lorsque la destination est **local ou remote {par défaut : remote}**	**local | remote** - Indiquez si le trafic est local ou distant.
Geographic Location	Validez lorsque l'adresse IP source correspond à l'emplacement géographique configuré.	lorsque la source est localisée dans cette **geographic region**	**geographic location** - Sélectionnez un emplacement géographique.

Tableau A-24 Règles communes : Tests de propriété communs (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	Validez lorsque l'adresse MAC configurée, le nom d'utilisateur, le nom d'hôte ou le système d'exploitation est associé à une chaîne d'expressions régulières particulières ***Remarque :*** *Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez les modèles d'expressions régulières personnalisés, acceptez les règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.*	lorsque l'**username** correspond au **regex**	Configurez les paramètres suivants : • **hostname | source hostname |destination hostname | source payload | destination payload** - Indiquez la valeur que vous souhaitez associer à ce test. La valeur par défaut est **username**. • **regex** - Indiquez la chaîne d'expression régulière que ce test doive prendre en considération.
IPv6	Validez lorsque l'adresse IPv6 de destination ou source correspond à l'adresse IP configurée.	lorsque la **source IP (v6)** est l'une des **IPv6 addresses suivantes**	Configurez les paramètres suivants : • **source IP (v6) | destination IP (v6)** - Indiquez si vous souhaitez que ce test considère l'adresse IPv6 source ou de destination. • **IP (v6) addresses** - Indiquez les adresses IPv6 que ce test doive prendre en considération.

Tableau A-24 Règles communes : Tests de propriété communs (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Set	Validez lorsque l'une ou toutes les propriétés du flux ou de l'événement sont comprises dans l'un ou tous les ensembles de référence configurés.	lorsque **any** propriétés de **these properties** sont comprises dans **any** de **these reference set(s)**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés d'événements configurées. • **these properties** - Indiquez les propriétés d'événements ou de flux que ce test doive prendre en considération. • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** ensembles de référence configurés. • **these reference set(s)** - Indiquez les ensembles de référence que ce test doive prendre en considération.
Reference Map	Validez lorsque l'une ou toutes les propriétés ou flux d'événements dans une paire clé ou de valeur configurée sont comprises dans l'une ou toutes les cartes de référence configurées.	lorsqu'**any** de **these properties** est la clé et **any** de **these properties** est la valeur dans **any** de **these reference maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés de flux et d'événements communes configurées. • **these properties** - Indiquez les propriétés du flux que ce test doive prendre en considération • **these reference maps** - Indiquez les cartes de référence que ce test doive prendre en considération.
Reference Map of Sets	Validez lorsque l'une ou toutes les propriétés ou flux d'événements dans une paire clé ou de valeur configurée sont comprises dans l'une ou toutes les cartes de référence configurées.	lorsqu'**any** de **these properties** est la clé et **any** de **these properties** est la valeur dans **any** de **these reference map of sets**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés de flux et d'événements communes configurées. • **these properties** - Indiquez les propriétés du flux que ce test doive prendre en considération • **these reference map of sets** - Indiquez les ensembles de cartes de référence que ce test doive prendre en considération.

Tableau A-24 Règles communes : Tests de propriété communs (suite)

Test	Description	Nom du test par défaut	Paramètres
Reference Map of Maps	Validez lorsque l'une ou toutes les propriétés d'événements ou de flux dans une paire clé ou de valeur primaire et secondaire configurée sont comprises dans l'un ou toutes les cartes de cartes de référence configurées.	lorsqu'**any** de **these properties** est la clé de la première carte et **any** de **these properties** est la clé de la seconde carte d'**any** de **these properties** est la valeur dans un de **these reference map of maps**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** propriétés de flux et d'événements communes configurées. • **these properties** - Indiquez les propriétés du flux que ce test doive prendre en considération • **these reference map of maps** - Indiquez les cartes des cartes de référence que ce test doive considérer.
CVSS Risk (Host)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque l'hôte de **destination** possède une valeur de risque CVSS **greater than this amount**	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 de risque CVSS est supérieure, inférieure ou égale à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.
CVSS Risk (Port)	Validez lorsque l'hôte spécifié possède une valeur de risque CVSS qui correspond à la valeur configurée.	lorsque le port de **destination** possède une valeur de risque CVSS **greater than this amount**	• **source | destination | either** - Indiquez si le test prend en considération le port source ou de destination du flux. • **greater than | less than | equal to** - Indiquez si vous souhaitez que le niveau de menace soit supérieur, inférieur ou égal à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**.
Search Filter	Validez lorsque l'événement ou le flux correspond au filtre de la recherche spécifiée.	lorsque l'événement ou le flux correspond à **this search filter**	**this search filter** - Indiquez le filtre de recherche que ce test doive prendre en considération.

Tableau A-24 Règles communes : Tests de propriété communs (suite)

Test	Description	Nom du test par défaut	Paramètres
Regex	Validez lorsque la propriété configurée est associée à une chaîne d'expressions régulières particulières (regex). ***Remarque :*** *Ce test suppose une connaissance des expressions régulières (regex). Lorsque vous définissez les modèles d'expressions régulières personnalisés, acceptez les règles d'expressions régulières telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.*	lorsque **these properties** correspondent à **regex**	Configurez les paramètres suivants : • **these properties** - Indiquez la valeur que vous souhaitez associer à ce test. Les options comprennent toutes les propriétés d'événements et de flux normalisées et personnalisées. • **regex** - Indiquez la chaîne d'expression régulière que ce test doive prendre en considération.
Custom Rule Engines	Validez lorsque l'événement ou le flux est traité par les moteurs de règles personnalisées spécifiées.	lorsque l'événement ou le flux est traité par l'un de **these** Custom Rule Engines	**these** - Indiquez le moteur de règles personnalisées que ce test doive prendre en considération.
Hexadecimal	Validez lorsque la propriété configurée est associée à une valeur hexadécimale.	Si aucune de **these properties** ne contient **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'événements et de flux normalisées et personnalisées. • **these hexadecimal values** - Indiquez les valeurs hexadécimales que ce test doive prendre en considération.

Fonctions - tests de séquence La fonction - les tests de séquences comprennent :

Tableau A-25 Commun : Fonctions - Groupe de séquences

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 remplir aux conditions du 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 **rules, in|in any,** à partir de **the same|any source IP** vers **the same|any destination IP,** dans **this many seconds**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **in | in any** - Indiquez si ce test doive prendre en considération **in** ou **in any**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** sources configurées. • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test doive prendre en considération **same** ou **any** destinations configurées. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est **destination IP**. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **seconds**.

Tableau A-25 Commun : Fonctions - Groupe de séquences (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 remplir aux conditions du test. Vous pouvez utiliser cette fonction pour détecter un nombre de règles spécifiées, en séquence, relatives à une source ou une destination dans un intervalle configuré.	lorsqu'au moins **this number** de ces **rules, in|in any, à partir de the same| any source IP** vers **the same|any destination IP** dans **this many seconds**	Configurez les paramètres suivants : • **this number** - Indiquez le nombre de règles que vous souhaitez que cette fonction considère. • **rules** - Indiquez les règles que ce test doive prendre en considération. • **in | in any** - Indiquez si vous souhaitez que le test considère **in** ou **in any**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** sources configurées. • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **the same | any** - Indiquez si vous souhaitez que ce test prenne en considération **same** ou **any** destinations configurées. • **destination IP | destination port** - Indiquez si vous souhaitez que ce test considère l'adresse IP de destination, le nom d'utilisateur ou le port de destination. La valeur par défaut est **destination IP**. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **seconds**.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Event Sequence Function Between Hosts	Vous permet de détecter une séquence des règles sélectionnées relatives aux mêmes hôtes source et de destination dans l'intervalle configuré. Vous pouvez également utiliser les blocs de construction sauvegardés, ainsi que d'autres règles pour remplir aux conditions du test.	lorsque cette séquence de **rules**, relative au même hôte source et de destination dans **this many seconds**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **seconds**.
Rule Function	Vous permet de détecter un nombre de règles spécifiques avec des propriétés d'événements identiques et différentes dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** dans**this many minutes** une fois que**these rules** correspondent.	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter un nombre défini de règles spécifiques avec les mêmes propriétés d'événements qui se produisent dans l'intervalle configuré.	lorsque **these rules** correspondent à au moins **this many** avec les mêmes **event properties** dans **this many minutes** une que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois défini avec des propriétés d'événements identiques et différentes dans un intervalle configuré après une série de règles spécifiques.	lorsque **these rules** correspondent au moins à ce **this many** avec les mêmes **event properties** et différentes **event properties** dans **this many minutes** après que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Rule Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois défini dans un intervalle configuré et après qu'une série de règles spécifiques se produit avec les mêmes propriétés d'événements.	lorsque **these rules** correspondent au moins à **this many** dans **this many minutes** après que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indique l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsque les règles spécifiques se produisent un nombre de fois défini avec les mêmes propriétés d'événements dans un intervalle configuré après qu'une série de règles spécifiques se produit avec les mêmes propriétés d'événements.	lorsque **these rules** correspondent à au moins **this many** avec les mêmes **event properties** dans **this many minutes** une fois que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsque des règles spécifiques se produisent un nombre de fois défini dans un intervalle configuré après qu'une série de règles spécifiques se produit avec les mêmes propriétés d'événements.	lorsque **these rules** correspondent à au moins **this many** avec les mêmes **event properties** et différentes **event properties** dans **this many minutes** une fois que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsqu'un nombre spécifique d'événements se produit avec des propriétés d'événements identiques et différentes dans un intervalle configuré après qu'une série de règles spécifiques se produit.	lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** et différentes **event properties** dans **this many minutes** une fois que **these rules** correspondent	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsqu'un nombre spécifique d'événements se produit avec les mêmes propriétés d'événements dans un intervalle configuré et après qu'une série de règles spécifiques se produit avec les mêmes propriétés d'événements.	lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** dans **this many minutes** après que **these rules** correspondent aux mêmes **event properties**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Tableau A-25 Commun : Fonctions - Groupe de séquences (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet d'être alerté lorsque le nombre spécifique d'événements se produit avec des propriétés d'événements identiques et différentes dans un intervalle et après qu'une série des règles spécifiques se produit avec les mêmes propriétés d'événements.	Lorsqu'au moins **this many** d'événements sont affichés avec les mêmes **event properties** et différentes **event properties** dans **this many** de fois **these rules** correspondent avec les mêmes **event properties**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **these event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées.

Fonction - tests de compteur La fonction - les tests de compteur comprennent :

Tableau A-26 Règles communes : Fonctions - Groupe de tests de compteurs

Test	Description	Nom du test par défaut	Paramètres
Multi-Event Counter Function	Vous permet de tester le nombre d'événements 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 remplir aux conditions du test.	lorsqu'une **source IP** correspond à **more than|exactly this many** de ces **rules** via **more than|exactly this many destination IP,** dans **this many minutes**	Configurez les paramètres suivants : • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère exactement le nombre de règles ou plus. • **this many** - Indiquez le nombre de règles que ce test doive prendre en considération. • **rules** - Indiquez les règles que ce test doive prendre en considération. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère le nombre exact d'adresses IP de destination, de ports de destination, de QID, d'ID d'événements source ou de sources de journal que vous sélectionnez dans la source précédente. • **this many** - Indiquez le nombre d'adresse IP, de ports, de QID, d'événements, de sources de journal ou des catégories que ce test doive prendre en considération. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que ce test doive prendre en considération. La valeur par défaut est **destination IP**. • **this many** - Indiquez le temps de la valeur que vous souhaitez affecter à ce test. • **seconds | minutes | hours | days** - Indiquez l'intervalle que cette règle doive prendre en considération. La valeur par défaut est **minutes**.

Tableau A-26 Règles communes : Fonctions - Groupe de tests de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Multi-Rule Function	Vous permet de détecter une série de règles pour une adresse IP ou un port spécifique par une série de règles spécifiques pour une adresse IP ou un port spécifique. Vous pouvez également utiliser les blocs de construction ou les règles existantes pour remplir aux conditions du test.	lorsque toutes ces **rules** ayant la même adresse **source IP** plus de **this many**, à travers **more than|exactly this many destination IP** dans **this many minutes**	Configurez les paramètres suivants : • **rules** - Indiquez les règles que ce test doive prendre en considération. • **source IP | source port | destination IP | destination port | QID | category** - Indiquez la source que ce test doive prendre en considération. La valeur par défaut est **source IP**. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **more than | exactly** - Indiquez si vous souhaitez que ce test considère le nombre exact d'adresses IP de destination, de ports de destination, de QID, d'ID d'événements source ou de sources de journal que vous sélectionnez dans la source préxédente. • **this many** - Indiquez le nombre que ce test doive prendre en considération selon l'option configurée dans le paramètre **source IP**. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Indiquez la destination que ce test doive prendre en considération. La valeur par défaut est **destination IP**. • **this many** - Indiquez l'intervalle que vous souhaitez affecter à ce test. • **seconds | minutes | hours | days** - Indiquez l'intervalle que cette règle doive prendre en considération. La valeur par défaut est **minutes**.

Tableau A-26 Règles communes : Fonctions - Groupe de tests de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter une série d'événements avec les mêmes propriétés d'événements dans l'intervalle configuré. Par exemple, si vous pouvez utiliser ce test lorsque 100 événements avec la même adresse IP source se produisent dans les 5 minutes.	Lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** dans **this many minutes**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.
Event Property Function	Vous permet de détecter une série d'événements des propriétés d'événements identiques et différentes dans l'intervalle 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 les 5 minutes.	Lorsqu'au moins **this many** événements sont affichés avec les mêmes **event properties** et différentes **event properties** dans **this many minutes**	Configurez les paramètres suivants : • **this many** - Indiquez le nombre d'événements que ce test doive prendre en considération. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.

Tableau A-26 Règles communes : Fonctions - Groupe de tests 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 d'événements qui se produisent dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.
Event Property Function	Vous permet de détecter un nombre de règles spécifiques avec les mêmes propriétés d'événements dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **event properties** de flux dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.

Tableau A-26 Règles communes : Fonctions - Groupe de tests de compteurs (suite)

Test	Description	Nom du test par défaut	Paramètres
Event Property Function	Vous permet de détecter un nombre de règles spécifiques des propriétés d'événements identiques et différentes dans l'intervalle configuré.	lorsque **these rules** correspondent au moins à **this many** avec les mêmes **event properties** et différentes **event properties** dans **this many minutes**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre de fois où les règles configurées doivent correspondre au test. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **event properties** - Indiquez les propriétés d'événements que ce test doive prendre en considération. Les options comprennent toutes les propriétés d'événements normalisées et personnalisées. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**.

Fonction - tests simples La fonction - les tests simples :

Tableau A-27 Règles communes : Fonctions - Groupe de tests simples

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 remplir aux conditions du test. L'événement doit correspondre à l'une ou toutes les règles sélectionnées. Si vous souhaitez créer une instruction OR pour ce test de règles, spécifiez le paramètre **any**.	Lorsqu'un flux ou un événement correspond à **any|all** des **rules suivantes**	Configurez les paramètres suivants : • **any | all** - Indiquez soit **any** ou **all** les règles configurées qui devraient s'appliquer à ce test. • **rules** - Indiquez les règles que ce test doive prendre en considération.

Tests Date/Heure Les tests de date et d'heure comprennent :

Tableau A-28 Règles communes : Tests Date/Heure

Test	Description	Nom du test par défaut	Paramètres
Event/Flow Day	Validez lorsque l'événement ou le flux se produit sur les jours du mois configurés.	lorsque les flux ou les événements se produisent au **on** du jour du mois **selected**	Configurez les paramètres suivants : • **on | after | before** - Indiquez si vous souhaitez que ce test considère avant, après ou à la date configurée. La valeur par défaut est **on**. • **selected** - Indiquez le jour du mois que ce test doive prendre en considération.
Event/Flow Week	Validez lorsque l'événements ou le flux se produit sur les jours de la semaine configurés.	lorsque les flux ou les événements se produisent dans l'un de **these days of the week**	**these days of the week** - Indiquez les jours de la semaine que ce test doive prendre en considération.
Event/Flow Time	Validez lorsque l'événement ou le flux se produit dans, après ou avant l'heure configurée.	lorsque les flux ou les événements se produisent **after this time**	Configurez les paramètres suivants : • **after | before | at** - Indiquez si vous souhaitez que le test considère avant, après ou à la date configurée. La valeur par défaut est **after**. • **this time** - Indiquez l'heure que ce test doive prendre en considération.

Tests de propriété du réseau Le test de la propriété du réseau comprend :

Tableau A-29 Règles communes : Tests de propriété du réseau

Test	Description	Nom du test par défaut	Paramètres
Local Network Object	Validez lorsque l'événement se produit dans le réseau spécifié.	lorsque le réseau local est **one of the following**	**one of the following networks** - Indiquez les zones du réseau sur lesquelles vous souhaitez appliquer ce test.
Remote Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux distants.	lorsque **source IP** fait partie de l'un des emplacements de réseaux distants **suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • **remote network locations** - Indiquez les emplacements réseau dans lesquels vous souhaitez effectuer ce test.

Tableau A-29 Règles communes : Tests de propriété du réseau (suite)

Test	Description	Nom du test par défaut	Paramètres
Remote Services Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux des services distants configurés.	lorsque la **source IP** fait partie d'un **remote services network locations suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • **remote services network locations** - Indiquez les emplacements du réseau de services distants que vous souhaitez que le test considère.
Geographic Networks	Validez lorsque l'adresse IP fait partie de l'un ou de tous les emplacements de réseaux géographiques configurés.	lorsque **Source IP** fait partie d'un **geographic network locations suivants**	Configurez les paramètres suivants : • **source IP | destination IP | any IP** - Indiquez si vous souhaitez que ce test considère l'adresse IP source, l'adresse IP de destination ou n'importe quelle adresse IP. • **geographic network locations** - Indiquez les emplacements du réseau que souhaitez que le test considère.

Fonctions - tests négatifs Les test négatifs de fonctions comprennent :

Tableau A-30 Règles communes : Fonctions - Groupe de tests négatifs

Test	Description	Nom du test par défaut	Paramètres
Flow Property Function	Vous permet d'être alerté lorsque des règles spécifiées se produisent dans un intervalle configuré après qu'une série de règles spécifiques se produit avec les mêmes propriétés de flux.	Lorsqu'aucune de **these rules** ne correspond dans **this many minutes** après que **these rules** correspondent aux mêmes **flow properties**	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**. • **these** - Indiquez les règles que ce test doive prendre en considération. • **flow properties** - Indiquez les propriétés du flux que ce test doive prendre en considération. Les options comprennent toutes les propriétés de flux normalisées et personnalisées.
Rule Function	Vous permet d'être alerté lorsqu'aucune de ces règles spécifiées ne se produit dans un intervalle configuré après qu'une série de règles se produit.	Lorsqu'aucune de **these rules** ne correspond dans **this many minutes** après que **these rules** correspondent	Configurez les paramètres suivants : • **these rules** - Indiquez les règles que ce test doive prendre en considération. • **this many** - Indiquez le nombre d'intervalles que ce test doive prendre en considération. • **seconds | minutes | hours | days** - Indiquez l'intervalle que vous souhaitez affecter à ce test. La valeur par défaut est **minutes**. • **these rules** - Indiquez les règles que ce test doive prendre en considération.

Tests de règles de violation

Cette section fournit des informations sur les tests que vous pouvez appliquer aux règles de violation notamment :

- **Tests IP/Port**
- **Tests de fonction**
- **Tests Date/Heure**

- **Tests de source de journal**
- **Tests de propriétés de violation**

Tests IP/Port Les tests IP/Port comprennent :

Tableau A-31 Règles de violation : Groupe de tests IP/Port

Test	Description	Nom du test par défaut	Paramètres
Offense Index	Validez lorsque l'adresse IP source est l'une des adresses IP configurées.	lorsque la violation est indexée par l'une des **IP addresses** suivantes.	**IP addresses** - Indiquez les adresses IP que ce test doive prendre en considération. Vous pouvez saisir plusieurs entrées à l'aide d'une liste séparée par des virgules.
Destination IP Address	Validez lorsque la liste de destination est l'une des adresses IP configurées.	lorsque la liste de destination comprend **any IP addresses suivantes**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** destinations listées. La valeur par défaut est **any**. • **IP addresses** - Indiquez les adresses IP que ce test doive prendre 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 de 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 remplir aux conditions du test. La violation doit correspondre à une ou toutes les règles sélectionnées. Si vous souhaitez créer une instruction OR pour ce test de règles, spécifiez le paramètre **any**.	lorsque la violation correspond à **any** des **offense rules** suivantes.	Configurez les paramètres suivants : • **any | all** - Indiquez soit **any** ou **all** règles configurées qui devraient s'appliquer à ce test. La valeur par défaut est **any**. • **offense rules** - Indiquez les règles que ce test doive prendre en considération.

Tests Date/Heure Les tests de date et d'heure comprennent :

Tableau A-33 Règles de violation : Tests Date/Heure

Test	Description	Nom du test par défaut	Paramètres
Offense Day	Validez lorsque la violation se produit au jour du mois configuré.	lorsque les violations se produisent au **on** le jour du mois **selected**	Configurez les paramètres suivants : • **on | after | before** - Indiquez si vous souhaitez que cette règle s'applique avant, après ou à la date sélectionnée. La valeur par défaut est **on**. • **selected** - Indiquez la date que ce test doive prendre en considération.
Offense Week	Validez lorsque la violation se produit le jour de la semaine configuré.	lorsque les violations se produisent au **on these days of week**	Configurez les paramètres suivants : • **on | after | before** - Indiquez si vous souhaitez que cette règle s'applique avant, après ou le jour sélectionné. La valeur par défaut est **on**. • **these days of the week** - Indiquez les jours que ce test doive prendre en considération.
Offense Time	Validez lorsque la violation se produit avant, après ou à l'heure configurée.	lorsque les violations se produisent **after this time**	Configurez les paramètres suivants : • **on | after | before** - Indiquez si vous souhaitez que ce test s'applique avant, après ou à l'heure spécifiée. La valeur par défaut est **after**. • **this time** - Indiquez l'heure que ce test doive prendre en considération.

Tests de Source de journal Les tests de de la source du journal comprennent :

Tableau A-34 Règles de violation : Tests des sources du journal

Test	Description	Nom du test par défaut	Paramètres
Log Source Types	Validez lorsque l'un des types de la source du journal configurée est la source de la violation.	lorsque le type de la source du journal qui a détecté la violation est l'un des **log source types suivants**	**log source types** - Indiquez les types de la source du journal que ce test doit détecter.
Number of Log Source Type	Validez lorsque le nombre des types de source du journal est supérieur à la valeur configurée.	lorsque le nombre des types de source du journal qui ont détecté la violation est **greater than this number**	Configurez les paramètres suivants : • **greater than | equal to** - Indiquez si vous souhaitez que le niveau de menace soit supérieur ou égal à la valeur configurée. • **this number** - Indiquez le nombre des types de la source du journal que ce test doive prendre en considération.

Tests de propriétés de violation Les tests de propriétés de violation comprennent :

Tableau A-35 Règles de violation : Tests des propriétés de violation

Test	Description	Nom du test par défaut	Paramètres
Network Object	Validez lorsque le réseau est influencé par any ou all des réseaux configurés.	lorsque les réseaux influencés sont **any** des **the following réseaux**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** réseaux. La valeur par défaut est **any**. • **the following networks** - Indiquez les réseaux que ce test doive prendre en considération.
Offense Category	Validez lorsque la catégorie de l'événement est l'une ou toutes les catégories de l'événement configuré.	lorsque les catégories des violations incluent **any** des **list of categories suivantes**	Configurez les paramètres suivants : • **any | all** - Indiquez si vous souhaitez que ce test considère **any** ou **all** catégories. La valeur par défaut est **any**. • **list of categories** - Indiquez les catégories que ce test doive prendre en considération. Pour plus d'informations sur les catégories d'événements, voir *IBM Security QRadar SIEM le guide d'administration*.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Severity	Validez lorsque la gravité est supérieure, inférieure ou égale aux valeurs configurées.	lorsque la gravité de violation est **greater than 5 {par défaut}**	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 le test doive prendre en considération. La valeur par défaut est **5**.
Credibility	Validez lorsque la crédibilité est supérieure, inférieure ou égale à la valeur configurée.	lorsque la crédibilité de violation est **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 le test doive prendre en considération.
Relevance	Validez lorsque la pertinence est supérieure, inférieure ou égale à la valeur configurée.	lorsque la pertinence de violation est **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 le test doive prendre en considération.
Offense Context	Le contexte de violation est la relation entre la source et la destination de la violation. Par exemple, un attaquant local vers une cible distante. Validez si le contexte de violation est l'une options suivantes : • Local to Local • Local to Remote • Remote to Local • Remote to Remote	lorsque le contexte de violation est **this context**	**this context** - Indiquez le contexte dans lequel vous souhaitez effectuer ce test. Les options sont : • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Validez lorsque la source est locale ou distante.	lorsque la source est locale ou **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**.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Destination Location	Validez lorsque la destination est locale ou distante.	lorsque la liste de destination comprend des **local or remote IP addresses {par défaut : remote}**	**locate IPs | remote IPs** - Indiquez si vous souhaitez que la cible soit locale ou distante. La valeur par défaut est **remote IPs**.
Destination Count in an Offense	Validez lorsque le nombre de destinations pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre de destinations attaquées est **greater than this number**	Configurez les paramètres suivants : • **greater than | equal to** - Indiquez si vous souhaitez que le nombre des destinations soit supérieur ou égal à la valeur configurée. • **this number** - Indiquez la valeur que ce test doive prendre en considération.
Event Count in an Offense	Validez lorsque le nombre des événements pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre des événements qui composent la violation est **greater than this number**	Configurez les paramètres suivants : • **greater than | less than | equal to** - Indiquez si vous souhaitez que le comptage d'événements soit supérieur, inférieur ou égal à la valeur configurée. • **this number** - Indiquez la valeur que ce test doive prendre en considération.
Flow Count in an Offense	Validez lorsque le nombre de flux pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre de flux qui composent la violation est **greater than this number**	Configurez les paramètres suivants : • **greater than | less than | equal to** - Indiquez si vous souhaitez que le comptage de flux soit supérieur, inférieur ou égal à la valeur configurée. • **this number** - Indiquez la valeur que ce test doive prendre en considération.
Total Event/Flow Count in an Offense	Validez lorsque le nombre total d'événements et de flux pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre d'événements et de flux composent la violation est **greater than this number**	Configurez les paramètres suivants : • **greater than | less than | equal to** - Indiquez si vous souhaitez que le comptage d'événements et de flux soit supérieur, inférieur ou égal à la valeur configurée. • **this number** - Indiquez la valeur que ce test doive prendre en considération.

Tableau A-35 Règles de violation : Tests des propriétés de violation (suite)

Test	Description	Nom du test par défaut	Paramètres
Category Count in an Offense	Validez lorsque le nombre de catégories d'événements pour une violation est supérieur, inférieur ou égal à la valeur configurée.	lorsque le nombre de catégories impliquées dans la violation est **greater than this number**	Configurez les paramètres suivants : • **greater than | equal to** - Indiquez si vous souhaitez que le nombre de catégories soit supérieur ou égal à la valeur configurée. • **this number** - Indiquez la valeur que ce test doive prendre en considération. Pour plus d'informations sur les catégories d'événements, voir *IBM Security QRadar SIEM le guide d'administration*.
Offense ID	Validez lorsque l'ID de violation est la valeur configurée.	lorsque l'ID de violation est **this ID**	**this ID** - Indiquez l'ID de violation que ce test doive prendre en considération.
Offense Creation	Validez lorsqu'une nouvelle violation est créée.	lorsqu'une nouvelle violation est créée	
Offense Change	Validez lorsque la propriété de la violation configurée se situe au-dessus de la valeur configurée.	lorsque **property** de violation a augmenté d'au moins **this percent**	Configurez les paramètres suivants : • **Magnitude | Severity | Credibility | Relevance| Destination count | Source count | Category count | Annotation count | Event count** - Indiquez la propriété que ce test doive prendre en considération. La valeur par défaut est **Magnitude**. • **this** - Indiquez le pourcentage ou la valeur unitaire que ce test doive considérer. • **percent** | **unit(s)** - Indiquez si vous souhaitez que ce test considère le pourcentage ou les unités.

Tests de règles de détection d'anomalies

Cette section fournit des informations sur les tests que vous pouvez appliquer aux règles de détection d'anomalies notamment :

- **Tests de règles d'anomalies**
- **Tests de règles de comportements**
- **Tests de règles de seuil de temps**

Tests de règles d'anomalies

Cette section fournit des informations sur les tests de règles d'événements que vous pouvez appliquer aux règles notamment :

Tests d'anomalies

Le groupe de tests d'anomalies comprend :

Tableau A-36 Règles d'anomalies : Tests d'anomalies

Test	Description	Nom du test par défaut	Paramètres
Anomaly	Validez lorsque la propriété accumulée a augmenté ou diminué selon le pourcentage spécifié pendant une courte période en comparaison avec la plus grande période spécifiée. Par exemple, si votre moyenne d'octets de destination 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 règles de détection d'anomalies à intervalles d'une minute. Pour plus d'informations sur l'accumulateur, consultez le guide d'administrationIBM Security QRadar SIEM.*	lorsque la valeur moyenne (par intervalle) de **this accumulated property** au cours de la dernière **1 min** est au moins **percentage** différent de la valeur moyenne par intervalle de la même propriété au cours de la dernière **1 min**	Configurez les paramètres suivants : • **this accumulated property** - Indiquez la propriété accumulée que ce test doive prendre en considération. • **1 min** - Indiquez l'intervalle que ce test doive prendre en considération. La valeur par défaut est **1 min**. • **40** - Indiquez le pourcentage que ce test doive prendre en considération. Le pourcentage par défaut est **40**. • **1 min** - Indiquez l'intervalle qu'utilise ce test pour comparer la durée de l'intervalle. L'intervalle par défaut est **1 min**.
Minimum Value	Validez lorsque la valeur testée pour l'intervalle accumulé dépasse la valeur configurée.	lorsque les intervalles d'accumulation sont uniquement considérés si la valeur testée pour cet intervalle dépasse **some value**	**some value** - Indiquez la valeur que vous souhaitez considérer pour l'intervalle d'accumulation configuré.

Tests de seuil de temps

Le groupe de tests de seuil de temps comprend :

Tableau A-37 Règles d'anomalies : Tests de seuil de temps

Test	Description	Nom du test par défaut	Paramètres
Date Range	Validez lorsqu'une activité anormale est détectée dans la plage de dates spécifiée.	lorsque la date est entre **this date** et **this date**	Configurez les paramètres suivants : • **this date** - Indiquez la date de début de votre plage de dates. • **this date** - Indiquez la date de fin de votre plage de dates.

Tableau A-37 Règles d'anomalies : Tests de seuil de temps (suite)

Test	Description	Nom du test par défaut	Paramètres
Day of the Week	Validez lorsqu'une activité anormale est détectée dans un jour de la semaine spécifié.	lorsque le jour de la semaine est **these selected days**	**these selected days** - Indiquez les jours que ce test doive prendre en considération.
Time Range	Validez lorsqu'une activité anormale est détectée dans la plage de temps spécifiée.	lorsque l'heure du jour est entre **this time** et **this time**	Configurez les paramètres suivants : • **this time** - Indiquez l'heure de début de votre plage de dates. • **this time** - Indiquez l'heure de fin de votre plage de dates.

Tests de règles de comportements

Cette section fournit des informations sur les tests de règles de comportements que vous pouvez appliquer aux règles notamment :

- **Tests de comportements**
- **Tests de seuil de temps**

Tests de comportements

Le groupe de tests de comportements comprend :

Tableau A-38 Règles de comportements : Tests de comportements

Test	Description	Nom du test par défaut	Paramètres
Accumulated Property	Indiquez la propriété accumulée considérée par cette règle.	lorsque **this accumulated property** est la propriété testée	**this accumulated property** - Indiquez la propriété accumulée que ce test doive prendre en considération.
Current Traffic Level	Validez lorsque le niveau du trafic actuel représente un changement saisonnier spécifié dans des données dans la plage de temps spécifiée dans ce test de durée de saison. Par exemple, le test de niveau du trafic actuel peut comparer les données en cours avec les données de la même plage de temps qu'hier.	lorsque l'importance du niveau du trafic actuel (sur une échelle de 0 à 100) est **importance** comparée au comportement et aux tendances du trafic étudié	**70** - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que ce test doive prendre en considération. La valeur par défaut est **70**.

Tableau A-38 Règles de comportements : Tests de comportements (suite)

Test	Description	Nom du test par défaut	Paramètres
Current Traffic Trend	Validez lorsque la tendance du trafic représente un effet saisonnier spécifique dans les données pour chaque intervalle. Par exemple, le test de la tendance du trafic actuel peut effectuer un test lorsque les données augmentent de la même façon de la semaine 2 à la semaine 3 comme cela s'est produit de la semaine 1 à la semaine 2.	lorsque l'importance de la tendance du trafic actuel (sur une échelle de 0 à 100) est **importance** comparée au comportement et aux tendances du trafic étudié	**30** - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que ce test doive prendre en considération. Le pourcentage par défaut est **30**.
Current Traffic Behavior	Validez lorsque le comportement du trafic change dans les données pour chaque intervalle. Par exemple, le test du trafic actuel peut tester pour les changements de données lors de la comparaison de cette minute à la minute précédente.	lorsque l'importance du niveau du trafic actuel (sur une échelle de 0 à 100) est **importance** comparée au comportement et aux tendances du trafic étudié	**30** - Indiquez le niveau d'importance, sur une échelle de 0 à 100, que ce test doive prendre en considération. Le pourcentage par défaut est **30**.
Deviation	Validez 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 **deviation** % de l'extrapolé (valeur de la zone prévue).	**50** - Indiquez le pourcentage de déviation que vous souhaitez que ce test considère. La valeur par défaut est **50**.
Season Length	Validez lorsque la durée de la saison représente l'intervalle que vous souhaitez tester. Généralement, pour le trafic du réseau, vous pouvez définir la durée de la saison comme une semaine. Lors du contrôle du traffic à partir des systèmes automatisés, définissez la durée de la saison comme un jour.	lorsque la durée de la saison est **season**	**a day | a week | a month** - Indiquez la durée de la saison que ce test doive prendre en considération.
Minimum Value	Validez lorsque la valeur testée pour l'intervalle accumulé dépasse la valeur configurée.	lorsque les intervalles d'accumulation sont uniquement considérés si la valeur testée pour cet intervalle dépasse **0**	**0** - Indiquez la valeur que vous souhaitez considérer pour l'intervalle d'accumulation configuré.

Tests de seuil de temps

Le groupe de tests de seuil de temps comprend :

Tableau A-39 Règles d'anomalies : Tests de seuil de temps

Test	Description	Nom du test par défaut	Paramètres
Date Range	Validez lorsqu'une activité anormale est détectée dans la plage de dates spécifiée.	lorsque la date est entre **this date** et**this date**	Configurez les paramètres suivants : • **this date** - Indiquez la date de début de votre plage de dates. • **this date** - Indiquez la date de fin de votre plage de dates.
Day of the Week	Validez lorsqu'une activité anormale est détectée pour un jour spécifié de la semaine.	lorsque le jour de la semaine est **these selected days**	**these selected days** - Indiquez les jours que ce test doive prendre en considération.
Time Range	Validez lorsqu'une activité anormale est détectée dans la plage de temps spécifiée.	lorsque l'heure du jour est entre **this time** et **this time**	Configurez les paramètres suivants : • **this time** - Indiquez l'heure de début de votre plage de dates. • **this time** - Indiquez l'heure de fin de votre plage de dates.

Tests de règles de seuil de temps

Cette section fournit des informations sur les tests de règles de seuil que vous pouvez appliquer aux règles notamment :

- **Tests de seuil de zone**
- **Tests de seuil de temps**

Tests de seuil de zone

Le groupe de tests de seuil de zone comprend :

Tableau A-40 Règles de seuil : Tests de seuil de la zone

Test	Description	Nom du test par défaut	Paramètres
Threshold Value	Validez lorsque la gravité est supérieure, inférieure ou égale aux valeurs configurées. Vous pouvez indiquer l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété.	lorsque **this accumulated property** est **greater than this value** (accumulée dans un intervalle de **1 min**)	• **this accumulated property** - Indiquez la propriété accumulée que ce test doive prendre en considération. • **greater than | less than | equal to** - Indiquez si la valeur de la propriété accumulée est supérieure, inférieure ou égale à la valeur configurée. • **0** - Indiquez la valeur que ce test doive prendre en considération. La valeur par défaut est **0**. • **1 min** - Indiquez l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété. La valeur par défaut est **1 min**.

Tableau A-40 Règles de seuil : Tests de seuil de la zone (suite)

Test	Description	Nom du test par défaut	Paramètres
Threshold Range	Validez lorsque la propriété accumulée est dans un intervalle spécifié. Vous pouvez indiquer l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété.	Lorsque **this accumulated property** est entre **this value** et **this value** (accumulée dans des intervalles d'**1 min**)	• **this accumulated property** - Indiquez la propriété accumulée que ce test doive prendre en considération. • **0** - Indiquez la valeur que ce test doive prendre en considération en tant que début d'intervalle. La valeur par défaut est **0**. • **0** - Indiquez la valeur que ce test doive prendre en considération en tant que fin d'intervalle. La valeur par défaut est **0**. • **1 min** - Indiquez l'intervalle, en minutes, dans lequel vous souhaitez accumuler la propriété. La valeur par défaut est **1 min**.

Tests de seuil de temps

Le groupe de tests de seuil de temps comprend :

Tableau A-41 Règles de seuil : Tests de seuil de l'heure

Test	Description	Nom du test par défaut	Paramètres
Date Range	Validez lorsqu'une activité anormale est détectée dans la plage de dates spécifiée.	lorsque la date est entre **this date** et **this date**	Configurez les paramètres suivants : • **this date** - Indiquez la date de début de votre plage de dates. • **this date** - Indiquez la date de fin de votre plage de dates.
Day of the Week	Validez lorsqu'une activité anormale est détectée dans un jour de la semaine spécifié.	lorsque le jour de la semaine est **these selected days**	**these selected days** - Indiquez les jours que ce test doive prendre en considération.
Time Range	Validez lorsqu'une activité anormale est détectée dans la plage de temps spécifiée.	lorsque l'heure du jour est entre **this time** et **this time**	Configurez les paramètres suivants : • **this time** - Indiquez le temps de début de votre plage de dates. • **this time** - Indiquez le temps de fin de votre plage de dates.

B GLOSSAIRE

Accumulateur L'accumulateur réside sur l'hôte qui contient un processeur d'événements pour aider à l'analyse des flux, des événements, des rapports, à l'écriture des données de bases de données et à l'alerte d'un DSM.

Adresse IP virtuelle du cluster L'adresse IP virtuelle du cluster est l'adresse IP utilisée pour communiquer avec un cluster à haute disponibilité. Lorsque vous configurez la haute disponibilité, l'adresse IP de l'hôte à haute disponibilité principal devient l'adresse IP virtuelle du cluster. Si l'hôte à haute disponibilité principal tombe en panne, l'adresse IP virtuelle du cluster sera remplacée par l'hôte à haute disponibilité secondaire.

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 a été imparti.

Anomalie Ecart du comportement attendu du réseau.

ARP Voir Protocole de résolution d'adresse.

ASN Voir Numéro de système autonome (ASN).

Base de données OSVDB (Open Source Vulnerability Database) Une base de données OSVDB (Open Source Vulnerability Database) est une base de données open source créée par et pour la communauté de la sécurité du réseau. La base de données fournit des informations techniques sur les vulnérabilités de sécurité réseau.

Capture de contenu QFlow Collector capturent 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 SIEM 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)	Un 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.
Cluster à haute disponibilité	Un cluster à haute disponibilité est constitué d'un hôte à haute disponibilité principal et d'un hôte à haute disponibilité secondaire qui se comporte comme un hôte de secours pour l'hôte principal.
Code HMAC (Hash-Based Message Authentication)	Code cryptographique qui utilise une fonction de hachage chiffrée 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.
Comportement	Indique les conditions normales dans lesquelles le système ou le réseau fonctionne.
Console	Interface Web pour QRadar SIEM. QRadar SIEM 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, à configurer à l'avance par l'administrateur QRadar SIEM.
Conversion d'adresses réseau (NAT)	La conversion d'adresses réseau traduit l'adresse IP dans un réseau en une adresse IP différente dans un autre réseau.
Couche réseau	Couche 3 dans l'architecture de l'interconnexion de systèmes ouverts (OSI) ; la couche qui établit un chemin entre des systèmes ouverts.

Crédibilité	Indique l'intégrité d'un événement ou d'une violation telle que déterminée par l'évaluation de la crédibilité qui est configurée dans la source du journal. La crédibilité augmente lorsque plusieurs sources signalent le même événement.
Destination d'acheminement	QRadar SIEM vous permet de transmettre les données de journal brutes provenant de sources de journal et de données d'événements normalisés QRadar SIEM à un ou plusieurs systèmes de fournisseur, tels que des systèmes de billetterie ou d'alerte. Sur l'interface d'utilisateur QRadar SIEM ces systèmes des fournisseurs sont appelés les destinations d'acheminement.
Device Support Module (DSM)	Les modules de support de périphérique (DSM) vous permettent d'intégrer QRadar SIEM à des sources de journaux.
DNS	Voir Domain Name System.
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 : adresses IP, ports, protocole, octets, paquets, balises, direction, ID d'application et données utiles (facultatif).
Données utiles	Données d'application réelles (excluant les informations d'en-tête ou administratives) contenues dans un flux IP.
DSM	Voir Device Support Module (DSM).
Elément	Option du tableau de bord qui crée un portail personnalisé affichant toutes les vues possibles pour le contrôle.
Evénement	Enregistrement d'un périphérique décrivant une action sur un réseau ou un hôte.
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.
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.
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.

FQNN Voir Nom de réseau complet.

Gravité Indique la menace que représente une source par rapport au niveau de préparation de la cible contre l'attaque. Cette valeur est mappée vers une catégorie d'événement de la carte QID qui est comparée à la violation.

HA Voir Haute disponibilité.

Haute disponibilité La caractéristique à haute disponibilité (HA) garantit la disponibilité des données QRadar SIEM dans l'éventualité d'une panne matérielle ou réseau. Un cluster à haute disponibilité est constitué d'un hôte principal et d'un hôte secondaire qui se comporte comme un hôte de secours pour l'hôte principal. L'hôte secondaire conserve les mêmes données que l'hôte principal par l'une des deux méthodes suivantes : la réplication de données ou le stockage externe partagé. A intervalles réguliers, toutes les 10 secondes par défaut, l'hôte secondaire envoie un signal commande ping à l'hôte principal pour détecter une panne matérielle ou réseau. Si l'hôte secondaire détecte une panne, l'hôte secondaire prend automatiquement toutes les responsabilités de l'hôte principal.

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 SIEM. 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).

Host Context Surveille tous les composants QRadar SIEM pour s'assurer que chaque composant fonctionne comme prévu.

Hôte à haute disponibilité principal Dans un cluster à haute disponibilité, l'hôte à haute disponibilité principal est l'hôte auquel vous voulez ajouter une protection à haute disponibilité. Vous pouvez configurer la haute disponibilité pour n'importe quel système (console ou autre) dans votre déploiement. Lorsque vous configurez la haute disponibilité, l'adresse IP de l'hôte à haute disponibilité principal devient l'adresse IP virtuelle du cluster ; par conséquent, vous devez configurer une nouvelle adresse IP pour l'hôte principal.

Hôte à haute disponibilité secondaire Dans un cluster à haute disponibilité, l'hôte à haute disponibilité secondaire est le secours de l'hôte principal. Si l'hôte principal tombe en panne, l'hôte à haute

disponibilité secondaire prend automatiquement toutes les responsabilités de l'hôte à haute disponibilité principal.

ICMP Voir ICMP (Protocole de message de gestion inter-réseau).

Identité QRadar SIEM recueille des informations d'identité, si disponible 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 SIEM contient une adresse IP et au moins un des éléments suivants : nom d'utilisateur ou adresse MAC. Toutes les sources de journal ne génèrent pas des informations d'identité.

IDS Voir Système de détection d'intrusion.

Indicateurs TCP Type de marqueur qui peut être ajouté à un paquet pour alerter le système en cas d'activité anormale. Seules quelques combinaisons spécifiques d'indicateurs sont valides et caractéristiques, dans un trafic normal. Des combinaisons anormales d'indicateurs indiquent souvent une attaque ou une condition anormale du réseau.

Interconnexion de systèmes ouverts (OSI) Cadre général des normes ISO pour la communication entre différents systèmes réalisés par différents fournisseurs, dans lesquels le processus de communication est organisé en sept catégories différentes qui sont placées dans une séquence stratifiée en fonction de leur relation avec l'utilisateur. Chaque couche utilise la couche immédiatement inférieure et fournit un service à la couche au-dessus. Les couches 7 à 4 traitent la communication de bout en bout entre la source et la destination du message, et les couches 3 à 1 se chargent des fonctions réseau.

Intervalle Période par défaut dans le système. Affecte les intervalles de mise à jour des graphiques et la durée contenue dans chaque fichier journal de flux.

Intervalle de coalescence L'intervalle de coalescence (groupage) des événements est de 10 secondes, en commençant par le premier événement qui ne correspond à aucun événement en cours de coalescence. Dans l'intervalle, les trois premiers événements correspondants sont immédiatement publiés dans le processeur d'événements et le quatrième événement et les suivants sont fusionnés afin que le contenu et d'autres caractéristiques ne soient pas inclus dans le quatrième événement. Chaque arrivée d'un événement correspondant pendant l'intervalle incrémente le comptage d'événements du quatrième événement. A la fin de l'intervalle, l'événement fusionné est publié dans le processeur d'événements et l'intervalle suivant commence pour des événements correspondants. Si aucun événement correspondant n'arrive pendant cet intervalle, le processus redémarre. Dans le cas contraire, la coalescence continue avec tous les événements comptés et publiés selon des intervalles de 10 secondes.

Intervalle de rapport Intervalle de temps configurable selon lequel le processeur d'événement doit envoyer la totalité des événements capturés et des données de flux vers la console.

Intrusion Detection System (IDS)	Application ou dispositif qui identifie une activité suspecte sur le réseau.
Intrusion Prevention System (IPS)	Application qui réagit aux intrusions sur le réseau.
IP	Voir protocole IP.
IPS	Voir Intrusion Prevention System.
Journaux de flux	Enregistrement des flux permettant au système de comprendre le contexte d'une transmission précise via le réseau. Les flux sont stockés dans les journaux de flux.
L2L	Voir Local to Local.
L2R	Voir Local to Remote.
LAN	Voir réseau local.
LDAP	Voir Protocole LDAP.
Local to Local (L2L)	Trafic interne d'un réseau local vers un autre réseau local.
Local To Remote (L2R)	Trafic interne d'un réseau local vers un réseau distant.
Magistrate	Fournit les composants de traitement de base de l'option SIEM. Magistrate fournit des rapports, des alertes et une analyse du trafic réseau et des événements de sécurité. Magistrate traite l'événement par rapport aux règles personnalisées définies pour créer une violation.
Masque de sous-réseau	Masque de bits qui est combiné de manière logique à l'aide de l'opération ET avec l'adresse IP de destination d'un paquet IP afin de déterminer l'adresse réseau. Un routeur achemine les paquets en utilisant l'adresse réseau.
Minuteur d'actualisation	Les onglets **Dashboard**, **Log Activity**, et **Network Activity** disposent d'une barre de statut dynamique qui affiche la durée restante avant que QRadar SIEM actualise automatiquement les données d'activité du réseau actuel, l'actualisation intégrée peut être actualisée manuellement à tout moment.
Multidiffusion IP	La multidiffusion IP réduit le trafic sur un réseau en délivrant un flux unique d'information à plusieurs utilisateurs en même temps.
NAT	Voir conversion d'adresses réseau (NAT).
NetFlow	Technologie exclusive de comptabilité 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 SIEM pour accepter NDE's et ainsi devenir un collecteur NetFlow.
Nom de domaine complet (FQDN)	Partie d'une adresse URL Internet qui identifie complètement le programme serveur auquel une demande Internet est adressée.
Nom de réseau complet (FQNN)	Chemin d'accès complet d'un point spécifique dans la hiérarchie du réseau. Par exemple, la hiérarchie de la société A contient un objet de service qui contient un objet marketing. Par conséquent, le nom de réseau FQNN est le Department.de Marketing de la société A.
Numéro de système autonome	Un système autonome est un ensemble de tous les réseaux IP qui adhèrent à la même politique de routage spécifique et clairement définie. Un numéro de système autonome (ASN) est un numéro d'identification unique attribué à chaque système autonome.
Objets de feuille de base de données	Objets de point final dans une hiérarchie. Au niveau de chaque point dans la hiérarchie au-dessus de ce point, se trouve un objet parent qui contient les valeurs agrégées de tous les objets de feuille en dessous.
Objets réseau	Composants de la hiérarchie de réseau. Vous pouvez ajouter des couches à la hiérarchie en ajoutant des objets du réseau supplémentaires et en les associant à des objets déjà définis. (Les objets qui contiennent d'autres objets sont appelés groupes.)
OSI	Voir interconnexion des systèmes ouverts.
Packeteer	Les périphériques Packeteer collectent, regroupent et stockent les données de performances du réseau. Lorsque vous configurez une source de flux externe pour Packeteer, vous pouvez envoyer les informations de flux d'un périphérique Packeteer vers QRadar SIEM.
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 SIEM où des données sont extraites.
Pondération du 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 SIEM et distribuées dans la zone appropriée, en fonction du type d'événement.
Protocole	Ensemble de règles et de formats déterminant le comportement de communication des entités de couche en matière de performances des fonctions de couche. Il peut continuer à requérir un échange d'autorisations avec un module de règles ou un serveur de règles externes avant la validation.
Protocole de message de gestion inter-réseau (ICMP)	Protocole de couche réseau Internet entre un hôte et une passerelle.
Protocole DHCP	Un protocole qui permet l'attribution dynamique d'adresses IP pour l'équipement installé chez le client.
Protocole DHCP	Voir Protocole DHCP.
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 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 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 SOAP	Voir Protocole SOAP.
Protocole SOAP (Simple Object Access Protocol)	Protocole qui permet à un programme en cours d'exécution sur un type de système d'exploitation de communiquer avec un programme sur le même ou sur un autre type de système d'exploitation.
QFlow Collector	Recueille des données à partir de périphériques et de divers flux données en direct ou enregistrés, tels que des TAP réseau, des ports SPAN/miroir, NetFlow et des journaux de flux QRadar SIEM.
QID	QRadar SIEM Identificateur. Mappage d'un événement unique d'un périphérique externe à un identificateur unique Q1 Labs.

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.

Règle Collecte des conditions et des actions qui en découlent. Vous pouvez configurer les règles qui permettent à QRadar SIEM 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 e-mail 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 SIEM peut émettre une réinitialisation TCP vers le client ou le serveur dans une conversation. Cela arrête la communication entre le client et le serveur.

Remote To Local (R2L) Trafic externe entre un réseau distant et un réseau local.

Remote To Remote (R2R) Trafic externe provenant d'un réseau distant vers un autre réseau distant.

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.

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.

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 SIEM 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.

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-feu 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-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.
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.
Stratégie de marque	Une option de rapport qui permet à un utilisateur QRadar SIEM 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 actif	Dans un cluster à haute disponibilité, le système actif est celui dont tous les services sont en cours d'exécution. L'hôte à haute disponibilité principal ou secondaire peut être l'hôte actif. Si l'hôte à haute disponibilité secondaire est l'hôte actif, le basculement s'est produit.
Système de notation de vulnérabilité commune (CVSS)	Un score CVSS est un indicateur permettant d'évaluer la gravité d'une vulnérabilité. QRadar SIEM utilise les scores CVSS pour mesurer les inquiétudes justifiées par une vulnérabilité par rapport à d'autres vulnérabilités.

Système de secours Dans un cluster à haute disponibilité, le système de secours est l'hôte qui sert de solution de secours pour le système actif. Seul l'hôte à haute disponibilité secondaire peut être le système de secours. Le système de secours ne dispose d'aucun service en cours d'exécution. Si la réplication de disque est activée, le système de secours réplique des données du système actif. Si le système actif tombe en panne, le système de secours prend automatiquement le rôle actif.

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 SIEM est installé.

Whois Vous permet de rechercher des informations sur les noms et les numéros enregistrés sur Internet.

C AVIS ET MARQUES

Dans cette annexe :

Cette section décrit quelques avis et marques importants et fournit des informations sur la conformité.

Avis

Ces informations étaient destinées aux produits et services offerts aux Etats-Unis.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Contactez votre interlocuteur IBM habituel pour obtenir des informations sur les produits et services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier le fonctionnement de tout produit, programme ou service non IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Vous pouvez soumettre des demandes de licences par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues auprès du service IBM Intellectual Property Department de votre pays ou par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s’applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : INTERNATIONAL BUSINESS MACHINES CORPORATION LIVRE LE PRESENT DOCUMENT "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER, TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties explicites ou implicites pour certaines transactions, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Ces informations peuvent contenir des inexactitudes techniques ou des erreurs typographiques. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Ces informations peuvent être soumises à des dispositions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions d'IBM Customer Agreement, d'IBM International Program License Agreement ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via

d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les prix IBM indiqués sont des prix de détail suggérés par IBM, sont à jour et peuvent être modifiés sans préavis. Les prix distributeurs peuvent donc varier.

Ces informations contiennent des exemples de données et de rapports utilisés dans les opérations métier habituelles. Pour les illustrer aussi complètement que possible, les exemples incluent les noms des personnes, des sociétés, des marques et des produits. Tous ces noms sont fictifs et toute ressemblance avec des noms et adresses utilisés par une société réelle serait purement fortuite.

Si vous visualisez la copie électronique de ces informations, les photographies et illustrations en couleur peuvent ne pas apparaître.

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM (Informations relatives au copyright) est disponible sur le Web à l'adresse *http:\\www.ibm.com/legal/copytrade.shtml*.

Les noms suivants sont des marques ou des marques déposées d'autres sociétés :

Java et toutes les marques et tous les logos Java sont des marques ou des marques déposées d'Oracle et/ou de ses filiales.

Linux est une marque de Linus Torvalds aux Etats-Unis, dans d'autres pays ou les deux.

INDEX

G

I

L

M

O

P

Q

R

S

T

U

V