IBM Security QRadar SIEM
Version 7.2

Guide d'initiation

Remarque : Avant d'utiliser le présent document et le produit associé, lisez les informations disponibles dans Avis et marques à la page 36.

SOMMAIRE

A PROPOS DE CE GUIDE

Public cible 1
Conventions de la documentation 1
Documentation technique 1
Contactez le service clients 1
Instructions relatives aux pratiques de bonne sécurité 2

1 PRÉSENTATION

onglet Log activity 3
Onglet Network activity 3
onglet Assets 4
onglet Offenses 4
onglet Reports 4

2 ACCÈS À L'INTERFACE UTILISATEUR QRADAR SIEM

Navigateurs Web pris en charge 7
Connexion à QRadar SIEM 8
Activation de l'affichage de compatibilité d'Internet Explorer 8

3 DÉPLOIEMENT DE QRADAR SIEM

Dispositif QRadar SIEM 9
    Installation du dispositif QRadar SIEM 10
Configuration de QRadar SIEM 10
Structure hiérarchique du réseau 10
    Révision de la structure hiérarchique de votre réseau 11
Mises à jour automatiques 12
    Configuration des paramètres de mise à jour automatique 12
Collecte de données 13
    Collecte d'événements 15
    Collecte de flux 15
    Importation des informations sur l'évaluation de la vulnérabilité 16
Réglage de QRadar SIEM 16
Indexation du contenu 17
    Activation de l'indexation du contenu 17
    Désactivation de l'indexation du contenu 18
Serveurs et blocs de construction 18

Ajout automatique de serveurs aux blocs de construction 19
Ajout manuel de serveurs aux blocs de construction 19
Règles QRadar SIEM. 20
Configuration des règles 20
Nettoyage du modèle SIM. 21

4 UTILISATION DE QRADAR SIEM

Recherche d'événements. 22
Sauvegarde des critères de recherche d'événements 23
Configuration d'un graphique de série temporelle. 23
Recherche de flux. 25
Sauvegarde des critères de recherche de flux 25
Création d'un élément de tableau de bord 26
Recherche d'actifs 26
Etude des événements. 27
Affichage des violations. 27
Configuration des règles 28
Gestion des rapports 28
Activation des rapports 29
Création d'un rapport personnalisé 30

A GLOSSAIRE

B AVIS ET MARQUES

Avis. 35
Marques 37

INDEX

A PROPOS DE CE GUIDE

Le guide d'initiation *IBM Security QRadar SIEM* fournit des instructions de démarrage à l'aide de QRadar SIEM.

Public cible

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

Conventions de la documentation

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, du périphérique ou du réseau.*

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

Documentation technique

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

Contactez 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)

Instructions relatives aux bonnes pratiques de sécurité

La sécurité informatique nécessite de protéger les systèmes et les informations via la prévention, la détection et la réponse aux accès inappropriées depuis l'intérieur et l'extérieur de votre entreprise. Un accès incorrect peut provoquer l'endommagement, la destruction ou l'utilisation non appropriée des informations ou peut endommager ou utiliser de façon inappropriée vos systèmes, y compris dans le cadre d'attaques ou autres. Aucun système ou produit informatique ne doit être considéré comme totalement sécurisé et aucun produit, service ou mesure de sécurité ne doit empêcher l'utilisation ou l'accès inapproprié. Les systèmes, produits et services IBM sont conçus pour faire partie d'une méthode de sécurité complète, qui impliquera nécessairement des procédures opérationnelles supplémentaires et peut nécessiter que d'autres systèmes, produits ou services soient plus efficaces. IBM NE GARANTIT PAS QUE LES SYSTEMES, PRODUITS OU SERVICES SONT PROTEGES OU PROTEGENT VOTRE ENTREPRISE CONTRE LA CONDUITE ILLEGALE OU MALVEILLANTE D'UN TIERS.

1 PRÉSENTATION

Vous pouvez effectuer la configuration QRadar SIEM de base, commencer à collecter des données d'événements et de flux et savoir comment générer vos propres rapports personnalisés ou par défaut.

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

Onglet Log activity

Vous pouvez contrôler et afficher des événements de réseau en temps réel ou effectuer des recherches avancées.

L'onglet **Log Activity** affiche des données sur l'événement sous forme d'enregistrements provenant d'une source de journal, comme un pare-feu ou un routeur. L'onglet **Log Activity** vous permet de :

- Effectuer des études approfondies des données d'événement.
- Etudier les journaux d'événements envoyés à QRadar SIEM en temps réel.
- Effectuer des recherches d'événements avancées.
- Afficher l'activité du journal à l'aide de graphiques en série temporelle configurables.
- Identifier rapidement les faux positifs et régler QRadar SIEM.

Pour plus d'informations, voir **Utilisation de QRadar SIEM**.

Onglet Network activity

Vous pouvez étudier des sessions de communication entre deux hôtes.

L'onglet **Network Activity** affiche des informations sur la façon dont le trafic est communiqué et quels éléments sont communiqués (si l'option de capture du contenu est activée). L'onglet **Network Activity** vous permet de :

- Etudier les flux envoyés à QRadar SIEM en temps réel.
- Effectuer des recherches performantes.
- Afficher l'activité du réseau à l'aide de graphiques en série temporelle configurables.

Pour plus d'informations, voir **Utilisation de QRadar SIEM**.

Onglet Assets

QRadar SIEM crée automatiquement des profils d'actifs en détectant vos actifs de réseau (serveurs et hôtes) en utilisant des données de flux passives et des données de vulnérabilité.

Les profils d'actifs fournissent des informations concernant chaque actif de votre réseau, y compris les services assurés. Les informations de profils d'actifs sont utilisées à des fins de comparaison, ce qui permet de réduire le nombre de faux positifs.

L'onglet **Assets** vous permet :

- de rechercher des actifs ;
- d'afficher tous les actifs étudiés ;
- d'afficher les informations d'identité des actifs étudiés ;
- de régler les vulnérabilités aux faux positifs.

Pour plus d'informations, voir **Utilisation de QRadar SIEM**.

Onglet Offenses

Vous pouvez étudier les violations pour déterminer la cause première d'un problème de réseau.

L'onglet **Offenses** vous permet d'afficher toutes les violations se produisant sur votre réseau. Pour localiser les violations, vous pouvez utiliser différentes options de navigation et de recherche. 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 ;
- de comparer les événements et les flux provenant de réseaux multiples vers la même adresse IP de destination ;
- d'étudier chaque violation de 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.

Pour plus d'informations sur l'onglet **Offenses** , voir **Onglet Offenses**.

Onglet Reports

Vous pouvez créer des rapports personnalisés dans QRadar SIEM ou utiliser des rapports par défaut.

Vous pouvez personnaliser et renommer des rapports par défaut et les distribuer à d'autres utilisateurs QRadar SIEM. Les administrateurs peuvent afficher tous les rapports créés par les autres utilisateurs QRadar SIEM. Les utilisateurs non administratifs peuvent uniquement afficher les rapports qu'ils ont créés ou des rapports partagés par d'autres utilisateurs. L'onglet **Reports** vous permet de :

- Créer, distribuer et gérer des rapports de tous types de données dans QRadar SIEM.
- Créer des rapports personnalisés pour une utilisation de fonctionnement et d'exécution.
- Combiner les informations (telles que celles de sécurité ou de réseau) en un seul rapport.
- Utiliser les modèles de rapports préinstallés.
- Renommer vos rapports en utilisant des logos personnalisés vous permettant de prendre en charge différents logos uniques pour chaque rapport. Cette option est intéressante pour la distribution des rapports auprès d'audiences différentes.

Pour plus d'informations sur les rapports, voir **Gestion des rapports**.

2 ACCÈS À L'INTERFACE UTILISATEUR QRADAR SIEM

Accédez à la console IBM Security QRadar SIEM à partir d'un navigateur Web pris en charge et connectez-vous à l'aide d'un nom d'utilisateur par défaut et d'un mot de passe attribué par votre administrateur.

Une clé de licence par défaut vous permet d'accéder à QRadar SIEM pendant cinq semaines. Une fois que vous êtes connecté, une fenêtre s'affiche et indique la date d'expiration de la clé de licence temporaire. Pour plus d'informations sur l'installation d'une clé de licence, consultez le guide d'administration *IBM Security QRadar SIEM* .

La communication entre le navigateur Web et QRadar SIEM est chiffrée à l'aide de Secure Socket Layer (SSL) et Transport Layer Security (TLS).

Navigateurs Web pris en charge

L'interface utilisateur QRadar SIEM est accessible via un navigateur Web pris en charge.

Si vous utilisez Mozilla Firefox, vous devez ajouter une exception à Mozilla Firefox pour vous connecter à QRadar SIEM. Pour plus d'informations, voir votre documentation Mozilla. Si vous utilisez Internet Explorer, un message d'erreur de certificat s'affiche. Vous devez sélectionner l'option **Continue to this website** pour poursuivre.

Les navigateurs Web pris en charge sont décrits dans le tableau suivant :

Tableau 2-1 Navigateurs Web pris en charge par QRadar SIEM

Navigateur Web	Versions prises en charge
Mozilla Firefox	• 10.0 ESR • 17.0 ESR Compte tenu du cycle d'édition court de Mozilla, nous ne pouvons pas soumettre au test les toutes dernières versions du navigateur Mozilla Firefox. Cependant, nous pouvons tout à fait soumettre à l'étude les différents problèmes signalés.

Tableau 2-1 Navigateurs Web pris en charge par QRadar SIEM

Navigateur Web	Versions prises en charge
Microsoft Windows Internet Explorer, avec vue de compatibilité activée	• 8.0 • 9.0 Pour obtenir des instructions sur la façon d'activer la vue Compatibility View, voir **Activation de l'affichage de compatibilité d'Internet Explorer**.
Google Chrome	• Dernière version Nous pouvons soumettre à l'étude les différents problèmes signalés.

Connexion à QRadar SIEM

Vous pouvez accéder à QRadar SIEM à l'aide d'un nom d'utilisateur par défaut et d'un mot de passe attribués par votre administrateur.

A propos de cette tâche

QRadar SIEM utilise un certificat SSL auto-affecté pour le chiffrement. Ces certificats ne sont pas détectés par la plupart des navigateurs Web. Un message d'erreur peut s'afficher et indiquer un certificat SSL non valide.

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

Procédure

Etape 1 Ouvrez votre navigateur Web.

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

https://**<IP Address>**

Où **<IP Address>**correspond à l'adresse IP du système QRadar SIEM.

Etape 3 Tapez le nom d'utilisateur par défaut et le mot de passe par défaut.

Les valeurs par défaut sont les suivantes :

Nom d'utilisateur : **admin**

Mot de passe : **<root password>**

Où `<root password>` correspond au mot de passe affecté à QRadar SIEM lors du processus d'installation. Pour plus d'informations, voir *IBM Security QRadar SIEM Installation Guide*.

Clique sur **Login To QRadar**.

Activation de l'affichage de compatibilité d'Internet Explorer

Vous pouvez activer l'affichage de compatibilité d'Internet Explorer 8.0 et 9.0.

Procédure

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

Configurez les paramètres de compatibilité suivants :

Tableau 2-2 Paramètres de compatibilité d'Internet explorer

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

3 QRadar SIEM - Déploiement

Avant de pouvoir évaluer les capacités clés QRadar SIEM, vous devez tout d'abord déployer QRadar SIEM.

Les administrateurs peuvent effectuer les tâches suivantes :

- Installer le dispositif QRadar SIEM. Pour plus d'informations, voir **Installation du dispositif QRadar SIEM**.
- Configurer votre installation QRadar SIEM. Pour plus d'informations, voir **Configuration QRadar SIEM**.
- Collecter les données d'événements, de flux et d'évaluation de la vulnérabilité. Pour plus d'informations, voir **Collecte de données**.
- Affiner votre installation QRadar SIEM. Pour plus d'informations, voir **Réglage de QRadar SIEM**.

Dispositif QRadar SIEM

Le dispositif d'évaluation QRadar SIEM est un serveur d'installation de rails à deux unités. Les rails de guidage ou les rayonnages ne sont pas équipés de matériel d'évaluation.

Le dispositif QRadar SIEM comprend quatre interfaces réseau. Pour cette évaluation, utilisez l'interface ETH0 comme interface de gestion.

Vous pouvez utiliser les trois interfaces de contrôle restantes pour la collecte de flux. QRadar QFlow Collector propose une analyse complète des applications réseau et peut exécuter des captures de paquets au début de chaque conversation. Suivant le dispositif QRadar SIEM, l'analyse de flux est automatiquement lancée lorsqu'un port de durée ou un tap réseau est connecté à une interface autre qu'ETH0. Des étapes supplémentaires peuvent être requises pour activer le composant QRadar QFlow Collector dans QRadar SIEM.

Pour plus d'informations, consultez le guide d'administration *IBM Security QRadar SIEM* .

Remarque : Le dispositif d'évaluation QRadar SIEM comprend une limite de 50 Mbps pour l'analyse de flux. Vérifiez que le trafic d'agrégat des interfaces de contrôle pour la collecte de flux ne dépasse pas 50 Mbps.

Installation du dispositif QRadar SIEM

Les administrateurs doivent installer le dispositif QRadar SIEM pour autoriser l'accès à l'interface utilisateur.

Avant de commencer

Avant d'installer le dispositif d'évaluation QRadar SIEM, vérifiez que vous disposez des éléments suivants :

- Espace pour un dispositif à deux unités.
- Rails de guidage et rayonnages (montés).
- Clavier USB et un moniteur VGA standard pour l'accès à une console (facultatif).

Procédure

Etape 1 Connectez l'interface réseau de gestion au port ETH0.

Etape 2 Branchez les connexions de puissance dédiées à l'arrière du dispositif.

Etape 3 Si vous avez besoin d'un accès à la console, connectez le clavier USB et le moniteur VGA standard.

Etape 4 Si le dispositif possède un panneau frontal, retirez-le en appuyant sur les onglets situés sur le côté et en retirant le panneau du dispositif.

Etape 5 Mettez le dispositif sous tension.

Remarque : Le bouton d'alimentation se trouve à l'avant du dispositif.

Configuration QRadar SIEM

En configurant QRadar SIEM, vous pouvez consulter la structure hiérarchique du réseau et personnaliser les mises à jour automatiques.

Avant de configurer QRadar SIEM, confirmez que le bureau que vous utilisez pour accéder à la console QRadar SIEM comprend les éléments installés suivants :

- Java™ Runtime Environment (JRE) - Vous pouvez télécharger Java version 1.6.0_u20 à partir du site Web suivant : *http://java.com/*.
- Adobe Flash 10.x

Pour configurer votre configuration, procédez comme suit :

- Vérifiez la structure hiérarchique du réseau. Pour plus d'informations, voir **Structure hiérarchique du réseau** et **Révision de la structure hiérarchique de votre réseau**.
- Configurer les paramètres des mises à jour automatiques. Pour plus d'informations, voir **Configuration des paramètres de mise à jour automatique**.

Structure hiérarchique du réseau

Vous pouvez afficher différentes zones de votre réseau organisées selon leur fonction métier et définir les priorités des informations de menaces et de règles en fonction du risque des valeurs métier.

QRadar SIEM utilise la hiérarchie de réseau pour :

- Comprendre le trafic réseau et afficher l'activité de réseau.
- Contrôler les groupes logiques spécifiques ou les services de votre réseau tels que le marketing, DMZ ou VoIP.
- Contrôler le trafic et créer un profil du comportement de chaque groupe et hôte du groupe.
- Déterminer et identifier les hôtes locaux et distants.

Pour l'évaluation, une hiérarchie de réseau par défaut est proposée et contient les groupes logiques prédéfinis. Vérifiez l'exactitude et l'exhaustivité de la hiérarchie de réseau. Si votre environnement comprend des plages réseau non affichées dans la hiérarchie de réseau préconfigurée, vous devez les ajouter manuellement.

Les objets définis dans la structure hiérarchique de votre réseau ne doivent pas nécessairement se trouver dans votre environnement. Les plages de réseau logique de votre infrastructure doivent être définies comme un objet réseau.

Remarque : Si votre système ne comprend pas de hiérarchie de réseau complétée, utilisez l'onglet **Admin** pour créer une hiérarchie spécifique à votre environnement. Pour plus d'informations, consultez le guide d'administration*IBM Security QRadar SIEM* .

Révision de la structure hiérarchique de votre réseau

Vous pouvez analyser la structure hiérarchique de votre réseau.

Procédure

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

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

Etape 3 Cliquez sur l'icône **Network Hierarchy**.

Etape 4 Dans la liste **Manage Group:Top**, cliquez sur **Regulatory_Compliance_Servers**.

Si votre hiérarchie de réseau ne comprend pas de composant serveur pour le dispositif existant, vous pouvez utiliser votre composant de courrier pour le reste de cette procédure.

Etape 5 Cliquez sur l'icône **Edit this object**.

Etape 6 Pour ajouter des serveurs de conformité :

a Dans la zone **IP/CIDR(s)**, saisissez l'adresse IP ou la plage CIDR de vos serveurs de conformité.

b Cliquez sur **Add**.

c Répétez l'opération pour tous les serveurs de conformité.

d Cliquez sur **Save**.

e Répétez ce processus pour chacun des autres réseaux à modifier.

Etape 7 Dans le menu de l'onglet **Admin**, cliquez sur **Deploy Changes**.

Etape 8 Fermez la fenêtre Network Hierarchy.

Etape 9

Vous pouvez mettre à jour automatiquement ou manuellement vos fichiers de configuration pour vérifier que vos fichiers de configuration contiennent les dernières informations de sécurité du réseau. QRadar SIEM utilise les fichiers de configuration pour fournir des caractérisations des flux de données du réseau.

Mises à jour automatiques

La console doit être connectée à Internet pour recevoir les mises à jour. Si votre console n'est pas connectée à Internet, vous devez configurer un serveur de mise à jour interne à partir duquel votre console pourra télécharger les fichiers. Pour plus d'informations sur la configuration d'un serveur de mise à jour automatique, voir *IBM Security QRadar SIEM User Guide*.

Les fichiers de mise à jour sont disponibles en téléchargement manuel à partir du site Web suivant :

http://www.ibm.com/support/fixcentral/

Les fichiers de mise à jour peuvent inclure les mises à jour suivantes :

- Mises à jour de configuration comprenant les changements de fichier de configuration, la vulnérabilité, la mappe QID et les mises à jour des informations de menace à la sécurité.
- Mises à jour DSM comprenant des corrections apportées aux problèmes d'analyse syntaxique, des changements de scanner et des mises à jour de protocoles.
- Mises à jour majeures comprenant des éléments tels que des fichiers JAR mis à jour.
- Mises à jour mineures comprenant des éléments tels que du contenu supplémentaire d'aide en ligne ou des scripts mis à jour.

QRadar SIEM vous permet remplacer vos fichiers de configuration existants ou d'intégrer les fichiers mis à jour à vos fichiers existants pour maintenir l'intégrité de la configuration et des informations en cours.

Configuration des paramètres de mise à jour automatique

vous pouvez personnaliser la fréquence des mises à jour, des types de mise à jour, de la configuration du serveur et des paramètres de sauvegarde de QRadar SIEM.

A propos de cette tâche

En utilisant les paramètres de mise à jour automatique, les fichiers de mise à jour QRadar SIEM peuvent comprendre les mises à jour suivantes :

- Mises à jour de configuration comprenant les changements de fichier de configuration, la vulnérabilité, la mappe QID et les mises à jour des informations de menace à la sécurité.

- Mises à jour DSM comprenant des corrections apportées aux problèmes d'analyse syntaxique, des changements de scanner et des mises à jour de protocoles.
- Mises à jour majeures comprenant des éléments tels que les fichiers Java™ Archive (JAR) mis à jour.
- Mises à jour mineures comprenant des éléments tels que du contenu supplémentaire d'aide en ligne ou des scripts mis à jour.

Procédure

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

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

Etape 3 Cliquez sur l'icône **Auto Update**.

Etape 4 Dans le menu de navigation, cliquez sur **Change Settings**.

Etape 5 Dans la sous-fenêtre **Auto Update Schedule**, acceptez les paramètres par défaut.

Etape 6 Dans la sous-fenêtre **Update Types**, configurez les paramètres suivants :

a Dans la zone de liste **Configuration Updates**, sélectionnez **Auto Update**.

b Pour les paramètres suivants, acceptez les valeurs par défaut :

- DSM, Scanner, Protocol Updates.
- Major Updates.
- Minor Updates.

Etape 7 Décochez la case **Auto Deploy**.

Par défaut, la case est cochée. Si la case n'est pas cochée, une notification système s'affiche sur l'onglet **Dashboard** pour indiquer que vous devez déployer les changements une fois les mises à jour installées.

Etape 8 Cliquez sur l'onglet **Advanced**.

Etape 9 Dans la sous-fenêtre Server Configuration, acceptez les paramètres par défaut.

Etape 10 Dans la sous-fenêtre Other Settings, acceptez les paramètres par défaut.

Etape 11 Cliquez sur **Save** et fermez la fenêtre Updates.

Etape 12 Dans la barre d'outils, cliquez sur **Deploy Changes**.

Etape suivante

Pour plus d'informations sur les paramètres de mise à jour automatique et les options de configuration, consultez le guide d'utilisation *IBM Security QRadar SIEM* .

Collecte de données

QRadar SIEM accepte des informations dans différents formats et dans une large gamme de périphériques comme les événements de sécurité, le trafic réseau et les résultats d'analyse.

Les données collectées sont classées en trois sections principales : événements, flux et informations d'évaluation de la vulnérabilité.

Evénements

Les événements sont générés en fonction des sources de journaux telles que les pare-feu, les routeurs, les serveurs UNIX, Linux ou Windows et les systèmes Intrusion Detection Systems (IDS) ou Intrusion Prevention Systems (IPS).

La majorité des sources de journaux envoie des informations dans QRadar SIEM à l'aide du protocole syslog. QRadar SIEM prend également en charge Simple Network Management Protocol (SNMP), Java Database Connectivity (JDBC) et Security Device Event Exchange (SDEE).

Par défaut, QRadar SIEM détecte automatiquement les sources de journaux après un nombre spécifique de journaux identifiables reçus dans un intervalle de temps précis. Une fois les sources de journaux détectées, QRadar SIEM ajoute le module Device Support Module (DSM) approprié à la fenêtre Log Sources de l'onglet **Admin**.

Même si la plupart des modules DSM comprend une fonction d'envoi du journal natif, plusieurs modules DSM requièrent une configuration supplémentaire et/ou un agent pour envoyer des journaux. La configuration varie d'un type de module DSM à un autre. Vous devez vous assurer que les modules DSM sont configurés pour envoyer des journaux dans un format pris en charge par QRadar SIEM. Pour plus d'informations sur la configuration des modules DSM, consultez le guide de configuration *DSM*.

Certains types de sources de journaux, tels que les routeurs et les commutateurs, n'envoient pas assez de journaux pour que QRadar SIEM les détecte rapidement et les ajoute à la liste Log Source. Vous pouvez ajouter manuellement ces sources de journaux. Pour plus d'informations sur l'ajout manuel de sources de journaux, consultez le guide d'utilisation *Log Sources*.

Flux

Les flux fournissent des informations sur le trafic réseau et peuvent être envoyés vers QRadar SIEM dans différents formats, comme les fichiers flowlog, NetFlow, J-Flow, sFlow et Packeteer.

En acceptant plusieurs formats de flux simultanément, QRadar SIEM peut détecter des menaces et des activités qui seraient sinon manquées en se basant strictement sur les événements d'informations.

QRadar QFlow Collector propose une détection complète des applications de trafic réseau quel que soit le port sur lequel l'application fonctionne. Par exemple, si le protocole Internet Relay Chat (IRC) communique sur le port 7500/TCP, un QRadar QFlow Collector identifie le trafic en tant qu'IRC et fournit une capture de paquet du début de la conversation. NetFlow et J-Flow vous avertissent seulement qu'il y a du trafic sur le port 7500/TCP sans fournir plus d'informations sur le protocole utilisé.

Les emplacements de ports de fonction miroir courants sont la mémoire système, DMZ, le serveur et les commutateurs d'application, NetFlow fournissant des informations supplémentaires provenant des routeurs et des commutateurs de limite.

Les QRadar QFlow Collector sont activés par défaut et requièrent la connexion d'une fonction miroir, d'une durée ou d'un tap réseau à une interface disponible du dispositif QRadar SIEM. L'analyse de flux commence automatiquement une fois le port de la fonction miroir connecté à l'une des interfaces réseau du dispositif QRadar SIEM. Par défaut, QRadar SIEM contrôle l'interface de gestion du trafic NetFlow sur le port 2055/UDP. Vous pouvez affecter des ports NetFlow supplémentaires, si nécessaire.

Informations sur l'évaluation de la vulnérabilité

QRadar SIEM peut importer des informations VA de différents scanners tiers. Les informations VA permettent à QRadar SIEM d'identifier les hôtes actifs, les ports ouverts et les éventuelles vulnérabilités. QRadar SIEM utilise les informations VA pour classer l'ampleur des violations sur votre réseau. Selon le type de scanner VA, QRadar SIEM peut importer les résultats de l'analyse provenant du serveur de scanner ou lancer une analyse à distance.

Collecte d'événements

En collectant les événements, vous pouvez étudier les journaux envoyés à QRadar SIEM en temps réel.

Procédure

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

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

Etape 3 Cliquez sur l'icône **Log Sources**.

Etape 4 Consultez la liste des sources de journaux et apportez les changements nécessaires à la source de journaux.

Pour plus d'informations sur la configuration des sources de journaux, voir *Log Sources User Guide*.

Etape 5 Fermez la fenêtre Log Sources.

Etape 6 Dans le menu de l'onglet **Admin**, cliquez sur **Deploy Changes**.

Collecte de flux

En collectant des flux, vous pouvez étudier des sessions de communication en réseau entre les hôtes.

Procédure

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

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources > Flows**.

Etape 3 Cliquez sur l'icône **Flow Sources**.

Etape 4 Consultez la liste des sources de flux et apportez les changements nécessaires à la source de flux.

Pour obtenir des instructions concernant la configuration des sources de flux, voir *IBM Security QRadar SIEM Administration Guide*.

Etape 5 Fermez la fenêtre Flow Sources.

Etape 6 Dans le menu de l'onglet **Admin**, cliquez sur **Deploy Changes**.

Remarque : Pour plus d'informations sur l'activation des flux sur des périphériques réseau tiers tels que des commutateurs et des routeurs, consultez la documentation de votre fournisseur.

Importation des informations sur l'évaluation de la vulnérabilité

En important des informations sur l'évaluation de la vulnérabilité, vous pouvez identifier les hôtes actifs, les ports ouverts et les éventuelles vulnérabilités.

Procédure

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

Etape 2 Dans le menu de navigation, cliquez sur **Data Sources > Vulnerability**.

Etape 3 Cliquez sur l'icône **VA Scanners**.

Etape 4 Cliquez sur **Add**.

Etape 5 Entrez les valeurs des paramètres.

Les paramètres dépendent du type de scanner que vous souhaitez ajouter. Pour plus d'informations, consultez le guide de configuration *Vulnerability Assessment*.

Remarque : La gamme CIDR indique les réseaux que QRadar SIEM intègre aux résultats de l'analyse. Par exemple, si vous souhaitez effectuer une analyse du réseau 192.168.0.0/16 et définir 192.168.1.0/24 comme gamme CIDR, seuls les résultats de la gamme 192.168.1.0/24 sont intégrés.

Etape 6 Cliquez sur **Save**.

Etape 7 Dans le menu de l'onglet **Admin**, cliquez sur **Deploy Changes**.

Etape 8 Cliquez sur l'icône **Schedule VA Scanners**.

Etape 9 Cliquez sur **Add**.

Etape 10 Indiquez les critères de fréquence d'analyse de votre choix.

Suivant le type d'analyse, ces éléments comprennent la fréquence à laquelle QRadar SIEM importe les résultats d'analyse ou lance une nouvelle analyse. Vous devez également indiquer les ports à inclure aux résultats d'analyse.

Etape 11 Cliquez sur **Save**.

Réglage de QRadar SIEM

Vous pouvez régler QRadar SIEM pour répondre aux besoins de votre environnement.

ATTENTION : *Avant de régler QRadar SIEM, attendez un jour pour laisser le temps au dispositif* QRadar SIEM *de détecter les serveurs de votre réseau, de*

stocker les événements et les flux et de créer des violations basées sur les règles en vigueur.

Les administrateurs peuvent effectuer les tâches de réglage suivantes :

- Optimiser les recherches de contenu d'événements et de flux en activant un index de contenu sur les propriétés de filtre rapide **Log Activity** et **Network Activity.** Pour plus d'informations, voir **Indexation du contenu**.
- Assurer un déploiement initial plus rapide et un réglage plus facile en ajoutant automatiquement ou manuellement des serveurs aux blocs de construction. Pour plus d'informations, voir **Serveurs et blocs de construction**.
- Configurer des réponses aux événements, aux flux et aux conditions de violation en créant ou modifiant des règles personnalisées et des règles de détection des anomalies. Pour plus d'informations, voir **QRadar SIEM règles**.
- S'assurer que chaque hôte de votre réseau crée des violations basées sur les règles les plus courantes, les serveurs reconnus et la hiérarchie du réseau. Pour plus d'informations, voir **Nettoyage du modèle SIM**.

Indexation du contenu

La fonction Quick Filter figurant dans les onglets **Log Activity** et **Network Activity** permet de rechercher le contenu des événements et des flux.

Pour optimiser cette fonction de recherche, vous pouvez activer un index de contenu pour la propriété Quick Filter. Par défaut, la durée de conservation des index de contenu est une semaine. Pour plus d'informations, voir *IBM Security QRadar SIEM Administration Guide*.

ATTENTION : *L'activation de l'indexation de contenu peut diminuer les performances du système. Contrôlez les statistiques après avoir activé l'indexation de contenu de la propriété Quick Filter. Pour plus d'informations sur la gestion des index et leurs statistiques, voir IBM Security QRadar SIEM Administration Guide.*

Activation de l'indexation du contenu

Vous pouvez optimiser les recherches de contenu d'événements et de flux en activant un index de contenu sur les propriétés de filtre rapide **Log Activity** et **Network Activity.**

Procédure

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

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

Etape 3 Cliquez sur l'icône **Index Management**.

Etape 4 Dans la zone **Quick Search**, saisissez **Quick Filter**.

Etape 5 Cliquez sur la propriété **Quick Filter** que vous souhaitez indexer.

Etape 6 Cliquez sur **Enable Index**.

Etape 7 Cliquez sur **Save**.

Etape 8 Cliquez sur **OK**.

Etape suivante

Pour plus d'informations sur les paramètres affichés dans la fenêtre Index Management, voir *IBM Security QRadar SIEM Administration Guide*.

Désactivation de l'indexation du contenu

Vous pouvez désactiver l'indexation de contenu sur les onglets **Log** et **Network Activity** de la propriété Quick Filter.

Procédure

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

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

Etape 3 Cliquez sur l'icône **Index Management**.

Etape 4 Dans la zone **Quick Search**, saisissez **Quick Filter**.

Etape 5 Cliquez sur la propriété **Quick Filter** que vous souhaitez désactiver.

Etape 6 Sélectionnez l'une des options suivantes :

- Cliquez sur **Disable Index**.
- Cliquez avec le bouton droit de la souris sur une propriété et sélectionnez **Disable Index** dans le menu.

Etape 7 Cliquez sur **Save**.

Etape 8 Cliquez sur **OK**.

Résultats

Les propriétés sélectionnées ne sont plus indexées. Dans les listes des propriétés d'événement ou de flux, les noms des propriétés indexées ne sont plus ajoutés au texte suivant : `[Indexed]`.

Etape suivante

Pour plus d'informations sur les paramètres affichés dans la fenêtre Index Management, voir *IBM Security QRadar SIEM Administration Guide*.

Serveurs et blocs de construction

QRadar SIEM reconnaît et classifie automatiquement les serveurs de votre réseau en proposant un déploiement initial plus rapide et un réglage plus facile en cas de changements apportés au réseau.

La fonction Server Discovery utilise la base de données de profils d'actifs pour reconnaître plusieurs types de serveurs sur votre réseau. La fonction Server Discovery répertorie automatiquement les serveurs reconnus en vous laissant sélectionner les serveurs que vous souhaitez intégrer à vos blocs de construction.

Remarque : Pour plus d'informations sur la reconnaissance des serveurs, voir *IBM Security QRadar SIEM Administration Guide*.

Les blocs de construction vous permettent de réutiliser les tests de règles spécifiques dans d'autres règles. QRadar SIEM utilise les blocs de construction

pour régler le système et permet d'activer des règles de corrélation supplémentaires. Cela vous permet de réduire le nombre de faux positifs détectés par QRadar SIEM et de vous focaliser sur l'identification des actifs critiques métier.

Ajout automatique de serveurs aux blocs de construction

Vous pouvez ajouter automatiquement des serveurs aux blocs de construction.

Procédure

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

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

Etape 3 Dans la zone de liste **Server Type**, sélectionnez le type de serveur à reconnaître.

Laissez le reste des paramètres comme paramètres par défaut.

Etape 4 Cliquez sur **Discover Servers**.

Etape 5 Dans la table **Matching Servers**, cochez la case de tous les serveurs que vous souhaitez affecter au rôle de serveur.

Etape 6 Cliquez sur **Approve Selected Servers**.

Remarque : Vous pouvez cliquer avec le bouton droit de la souris sur une adresse IP ou un nom d'hôte afin d'afficher les informations de résolution DNS.

Ajout manuel de serveurs aux blocs de construction

Si un serveur n'est pas automatiquement détecté, vous pouvez l'ajouter manuellement à ses blocs de construction de définition d'hôte correspondants.

A propos de cette tâche

Pour s'assurer que les règles de propriété sont appliquées au type de serveur, vous pouvez ajouter des périphériques individuels ou des plages d'adresses de périphériques complètes Vous pouvez saisir manuellement les types de serveur non conformes aux protocoles uniques dans leurs blocs de construction de définition d'hôte respectifs. Par exemple, l'ajout des types de serveur suivants à des blocs de construction permet de réduire le besoin de réglage supplémentaire des faux positifs :

- Ajoutez les **serveurs de gestion de réseau** au bloc de construction BB:HostDefinition: Network Management Servers.
- Ajoutez les **serveurs proxy** au bloc de construction BB:HostDefinition: Proxy Servers.
- Ajoutez les **serveurs de mises à jour de virus et de fenêtres** au bloc de construction BB:HostDefinition: Virus Definition and Other Update Servers.
- Ajoutez les **scanners VA** au bloc de construction BB-HostDefinition: VA Scanner Source IP.

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 **Building Blocks**.

Etape 4 Dans la zone de liste **Group**, sélectionnez **Host Definitions**.

Le nom du bloc de construction correspond au type de serveur. Par exemple, *BB:HostDefinition: Proxy Servers* s'applique à tous les serveurs proxy de votre environnement.

Les blocs de construction contiennent les hôtes automatiquement reconnus lorsque vous avez exécuté la tâche **Ajout automatique de serveurs aux blocs de construction**.

Etape 5 Pour ajouter manuellement un hôte ou un réseau, cliquez deux fois sur le bloc de construction de définition d'hôte correspondant adapté à votre environnement.

Etape 6 Dans la zone **Building Block**, cliquez sur la valeur soulignée après la phrase ***si la source ou l'adresse IP de destination est l'une des suivantes***.

Etape 7 Dans la zone **Enter an IP address or CIDR and click 'Add'**, entrez les noms d'hôtes ou les plages d'adresses IP à affecter au bloc de construction.

Etape 8 Cliquez sur **Add**.

Etape 9 Cliquez sur **Submit**.

Etape 10 Cliquez sur **Finish**.

Etape suivante

Répétez ces étapes pour chaque type de serveur que vous souhaitez ajouter.

QRadar SIEM règles

Les règles effectuent des tests sur les événements, les flux ou les violations. Si les conditions d'un test sont satisfaites, la règle génère une réponse.

QRadar SIEM comprend les règles qui permettent de détecter une large gamme d'activités, comme les refus excessifs de pare-feu, les tentatives répétées de connexion ayant échoué et une éventuelle activité botnet. Pour plus d'informations sur les règles, consultez le guide d'administration *IBM Security QRadar SIEM* .

Les deux catégories de règles sont les suivantes :

- Custom Rules - les règles personnalisées effectuent des tests sur les événements, les flux ou les violations pour détecter une activité inhabituelle sur votre réseau.
- Anomaly Detection Rules - les Règles de détection des anomalies effectuent des tests sur les résultats de flux enregistrés ou les événements recherchés pour détecter les modèles de trafic inhabituels sur votre réseau.

Remarque : Un utilisateur non administrateur peut créer des règles d'accès aux zones du réseau autorisées. Vous devez disposer des autorisations de rôles appropriés pour gérer les règles. Pour plus d'informations sur les autorisations de rôle d'utilisateur, consultez le guide d'administration *IBM Security QRadar SIEM*.

Configuration des règles

Vous pouvez modifier les règles par défaut QRadar SIEM afin qu'elles répondent à vos besoins de sécurité si nécessaire.

Procédure

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

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

Etape 3 Cliquez sur l'en-tête de colonne **Enabled** pour trier les règles par statut activé ou désactivé.

Etape 4 Dans la zone de liste **Group**, sélectionnez **Compliance**.

Etape 5 Sélectionnez la règle **Compliance: Compliance Events Become Offenses** .

Etape 6 Dans le menu, sélectionnez **Actions > Enable/Disable**.

Etape 7 Pour modifier les critères de règles, sélectionnez **Action > Edit**.

Nettoyage du modèle SIM

Vous pouvez vérifier que chaque hôte crée des violations basées sur les règles les plus courantes, les serveurs reconnus et la hiérarchie du réseau.

A propos de cette tâche

Lorsque vous nettoyez le modèle SIM, toutes les violations existantes sont clôturées. Le fait de nettoyer le modèle SIM n'affecte pas les événements et flux existants.

Procédure

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

Etape 2 Dans le menu **Advanced**, sélectionnez **Clean SIM Model**.

Etape 3 Sélectionnez l'option **Hard Clean**.

Etape 4 Cochez la case **Are you sure you want to reset the data model?**.

Etape 5 Cliquez sur **Proceed**.

Etape suivante

Une fois le processus de réinitialisation SIM terminé, actualisez votre navigateur.

4 UTILISATION DE QRADAR SIEM

Vous pouvez utiliser QRadar SIEM pour effectuer des recherches d'événements, de flux et d'actifs, d'étudier des violations et de créer des rapports.

QRadar SIEM propose un moteur puissant et flexible permettant de rechercher de grands volumes d'informations. Vous pouvez rechercher des informations à l'aide des recherches par défaut (Saved Searches) des onglets Log Activity et Network Activity ou créer et enregistrer vos propres recherches personnalisées.

Les administrateurs peuvent effectuer les tâches suivantes :

- Rechercher des données d'événement en utilisant des critères spécifiques et afficher des données qui correspondent aux critères de recherche dans une liste de résultats. Sélectionner, organiser et grouper les colonnes de données d'événement. Pour plus d'informations, voir **Recherche d'événements**.
- Contrôler visuellement et étudier les données de flux en temps réel ou effectuer des recherches avancées pour filtrer les flux affichés. Afficher les informations de flux pour déterminer le trafic réseau et la façon dont il est communiqué. Pour plus d'informations, voir **Recherche de flux**.
- Afficher tous les actifs étudiés ou rechercher des actifs précis dans votre environnement. Pour plus d'informations, voir **Recherche d'actifs**.
- Etudier les violations, les adresses IP source et cible, les comportements de réseau et les anomalies de votre réseau. Pour plus d'information, voir **Etude des événements**.
- Modifier, créer, planifier et distribuer des rapports par défaut ou personnalisés. Pour plus d'informations, voir **Gestion des rapports**.

Recherche d'événements

Vous pouvez rechercher tous les événements d'authentification reçus par QRadar SIEM au cours des six dernières heures.

Procédure

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

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

Etape 3 Dans la sous-fenêtre Time Range, définissez l'intervalle de recherche des événements :

a Sélectionnez l'option **Recent**.

b Dans la zone de liste de l'option **Recent**, sélectionnez **Last 6 Hours**.

Etape 4 Dans la sous-fenêtre **Search Parameters**, définissez les paramètres de recherche :

a Dans la première zone de liste, sélectionnez **Category**.

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

c Dans la zone de liste **High Level Category**, sélectionnez **Authentication**.

Laissez les options de la zone de liste **Low Level Category Any**.

d Cliquez sur **Add Filter**.

Le filtre s'affiche dans la zone de texte **Current Filters**.

Etape 5 Dans la zone de liste **Display** de la sous-fenêtre Column Definition, sélectionnez **Event Name**.

Etape 6 Cliquez sur **Search**.

Etape suivante

Enregistrez votre critère de recherche d'événements.Pour plus d'informations, voir **Sauvegarde des critères de recherche d'événements**.

Sauvegarde des critères de recherche d'événements

Vous pouvez enregistrer les critères de recherche d'événements spécifiés pour une utilisation ultérieure.

Procédure

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

Etape 2 Dans la barre d'outils Log Activity, cliquez sur **Save Criteria**.

Etape 3 Dans la zone **Search Name**, entrez le nom `Example Search 1`.

Etape 4 Dans la sous-fenêtre d'options Timespan, sélectionnez l'option **Recent**.

Etape 5 Dans la zone de liste, sélectionnez **Last 6 Hours**.

Etape 6 Cochez les cases **Include in my Quick Searches** et **Include in my Dashboard** .

Remarque : *Si la case à cocher **Include in my Dashboard** ne s'affiche pas, cliquez sur **Search > Edit Search** afin de vérifier que vous avez sélectionné **Event Name** dans la sous-fenêtre* Column Definition.

Etape 7 Cliquez sur **OK**.

Etape suivante

Configurez un graphique de série temporelle. Pour plus d'informations, voir **Configuration d'un graphique de série temporelle**.

Configuration d'un graphique de série temporelle

Vous pouvez afficher des graphiques de série temporelle représentant les enregistrements comparés par une recherche d'intervalle de temps spécifique.

Avant de commencer

Cette procédure implique que vous ayez effectué une recherche d'événements et que vous ayez enregistré vos critères de recherche. Pour plus d'informations, voir **Recherche d'événements** et **Sauvegarde des critères de recherche d'événements**.

Procédure

Etape 1 Dans la barre de titre du graphique de gauche, cliquez sur l'icône **Configure**.

Etape 2 Dans la zone de liste **Value to Graph**, sélectionnez **Destination IP (Unique Count)**.

Etape 3 Dans la zone de liste **Chart Type** , sélectionnez **Time Series**.

Etape 4 Cochez la case **Capture Time Series Data**.

Etape 5 Cliquez sur **Save**.

Attendez quelques minutes que les données de la série temporelle soient collectées et que le graphique s'affiche.

Etape 6 Cliquez sur **Update Details**.

Etape 7 Filtrez les résultats de votre recherche :

a Cliquez avec le bouton droit de la souris sur l'événement à filtrer.

b Sélectionnez **Filter on Event Name is <Event Name>**.

La liste d'événements est actualisée pour ne contenir que cet événement précis.

Etape 8 Pour afficher la liste des événements regroupée par nom d'utilisateur, sélectionnez **Username** dans la zone de liste **Display** de la barre d'outils.

Etape 9 Vérifiez que votre recherche est disponible dans le tableau de bord :

a Cliquez sur l'onglet **Dashboard**.

b Cliquez sur l'icône **New Dashboard**.

c Dans la zone **Name**, tapez `Example Custom Dashboard`.

d Cliquez sur **OK**.

Le nouveau tableau de bord s'affiche sur la page Dashboard et apparaît dans la zone de liste **Show Dashboard**. Par défaut, le tableau de bord est vide.

e Dans la zone de liste **Add Item** , sélectionnez **Log Activity > Event Searches > Example Search 1**.

Résultats

Les résultats de votre recherche d'événements sauvegardée s'affichent dans le tableau de bord.

Recherche de flux

Vous pouvez rechercher, contrôler visuellement et étudier des données de flux en temps réel.

Procédure

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

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

Etape 3 Dans la sous-fenêtre **Time Range**, définissez l'intervalle de recherche des flux :

- **a** Sélectionnez l'option **Recent**.
- **b** Dans la zone de liste, sélectionnez **Last 6 Hours**.

Etape 4 Dans la sous-fenêtre Search Parameters, définissez vos critères de recherche :

- **a** Dans la première zone de liste, sélectionnez **Flow Direction**.
- **b** Dans la seconde zone de liste, sélectionnez **Equals**.
- **c** Dans la troisième zone de liste, sélectionnez **R2L**.
- **d** Cliquez sur **Add Filter**.

  Le filtre s'affiche dans la zone de texte **Current Filters**.

Etape 5 Dans la zone de liste **Display** de la sous-fenêtre Column Definition, sélectionnez **Application**.

Etape 6 Cliquez sur **Search**.

Résultats

Tous les flux allant dans le sens distant vers local (R2L) au cours des 6 dernières heures s'affichent, triés via la zone **Application Name**.

Etape suivante

Sauvegardez votre critère de recherche de flux.Pour plus d'informations, voir **Sauvegarde des critères de recherche de flux**.

Sauvegarde des critères de recherche de flux

Vous pouvez sauvegarder les critères de recherche de flux spécifiés pour une utilisation ultérieure.

Etape 1 Dans la barre d'outils Network Activity, cliquez sur **Save Criteria**.

Etape 2 Dans la zone **Search Name**, entrez le nom `Example Search 2`.

Etape 3 Dans la zone de liste de l'option **Recent**, sélectionnez **Last 6 Hours**.

Etape 4 Cochez les cases **Include in my Dashboard** et **Include in my Quick Searches**.

Etape 5 Cliquez sur **OK**.

Etape suivante

Créez un élément de tableau de bord. Pour plus d'informations, voir **Création d'un élément de tableau de bord**.

Création d'un élément de tableau de bord

Vous pouvez créer un élément de tableau de bord à l'aide des critères de recherche de flux sauvegardés.

Procédure

Etape 1 Dans la barre d'outils Network Activity, sélectionnez **Quick Searches > Example Search 2**.

La page de résultats de la recherche affiche les résultats de votre recherche de flux.

Etape 2 Vérifiez que votre recherche est disponible dans le tableau de bord :

a Cliquez sur l'onglet **Dashboard**.

b Dans la zone de liste **Show Dashboard**, sélectionnez **Example Custom Dashboard**.

La page Example Custom Dashboard s'affiche dans le nouveau tableau de bord.

c Dans la zone de liste **Add Item**, sélectionnez **Flow Searches > Example Search 2**.

Les résultats de votre recherche sauvegardée s'affichent dans le tableau de bord.

Etape 3 Configurez votre graphique de tableau de bord :

a Cliquez sur l'icône **Settings** pour accéder aux options de configuration.

b Grâce aux options de configuration, changez la valeur du graphique, le nombre d'objets affichés, le type de graphique ou l'intervalle affiché dans le graphique.

Le graphique est mis à jour pour représenter les modifications apportées à votre configuration de graphique.

Etape 4 Pour étudier les flux actuellement affichés dans le graphique, cliquez sur **View in Network Activity**.

Résultats

La page Network Activity affiche les résultats correspondant aux paramètres de votre graphique de série temporelle. Pour plus d'informations sur les graphiques de série temporelle, consultez le guide d'utilisation *IBM Security QRadar SIEM* .

Recherche d'actifs

L'onglet **Assets** vous permet d'afficher tous les actifs étudiés ou de rechercher des actifs précis dans votre environnement réseau.

A propos de cette tâche

QRadar SIEM reconnaît automatiquement des actifs de votre réseau en fonction des flux, des données de vulnérabilité, des adresses MAC et des informations d'authentification. QRadar SIEM utilise ces informations pour créer un profil d'actif pour chaque hôte. Les profils d'actif affichent les services proposés pour chaque actif. QRadar SIEM utilise les données de profil pour réduire les faux positifs.

Par exemple, si un exploit se produit sur un actif, QRadar SIEM peut déterminer si l'actif est vulnérable à cet exploit en comparant ce dernier au profil d'actif.

Procédure

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

Etape 2 Sélectionnez l'une des options suivantes :

- **a** Pour rechercher des profils d'actif précis, configurez les valeurs des critères de recherche et cliquez sur **Search**.
- **b** Pour rechercher tous les profils d'actif de votre déploiement, cliquez sur **Show All**.

Etape 3 Cliquez deux fois sur un actif pour obtenir des informations supplémentaires sur l'hôte particulier.

Etape 4 Pour afficher l'historique des événements :

- **a** Cliquez deux fois sur l'actif à étudier.
- **b** Dans la barre d'outils, cliquez sur **History**.

Etape 5 Cliquez sur **Search**.

Résultats

Les résultats de la recherche affichent tous les événements des dernières 24 heures qui concernent l'actif que vous étudiez.

Etude des événements

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.

A propos de cette tâche

QRadar SIEM peut comparer les événements et les flux aux adresses IP cible localisées dans plusieurs réseaux de la même violation et, si possible, le même incident de réseau. Cela vous permet d'étudier de manière efficace chaque violation de votre réseau.

Affichage des violations

Procédure

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

Etape 2 Cliquez deux fois sur la violation à étudier.

Etape 3 Dans la barre d'outils, sélectionnez **Display > Destinations**.

Vous pouvez étudier chaque destination pour déterminer si elle est compromise ou fait état d'un comportement suspect.

Etape 4 Dans la barre d'outils, cliquez sur **Events**.

Résultats

La fenêtre **List of Events** affiche tous les événements associés à la violation. Vous pouvez rechercher, trier et filtrer des critères de recherche. Pour plus d'informations, voir **Recherche d'événements**.

Configuration des règles

Les onglets **Log Activity**, **Network Activity** et **Offenses** vous permettent de configurer les règles ou les blocs de construction.

Pour plus d'informations sur les règles QRadar SIEM, voir **QRadar SIEM rules**.

Procédure

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

Etape 2 Cliquez deux fois sur la violation à étudier.

Etape 3 Cliquez sur **Display > Rules**.

Etape 4 Cliquez deux fois sur une règle.

Remarque : Vous pouvez encore ajuster les règles. Pour plus d'informations sur le réglage des règles, consultez le guide d'administration *IBM Security QRadar SIEM* .

Etape 5 Fermez l'assistant Rules.

Etape 6 Dans la page Rules, cliquez sur **Actions** et sélectionnez l'une des options suivantes :

Tableau 4-1 Paramètres de la page Rules

Option	Description
Follow up	Sélectionnez cette option pour baliser la violation afin d'en assurer un suivi
Hide	Sélectionnez cette option pour masquer la violation.
Protect Offense	Sélectionnez cette option pour empêcher la violation d'être supprimée de la base de données une fois sa durée de conservation écoulée.
Close	Sélectionnez cette option pour fermer la violation.
Email	Sélectionnez cette option pour envoyer par e-mail un récapitulatif de la violation à un administrateur.
Add note	Sélectionnez cette option pour ajouter une note à une violation.
Assign	Sélectionnez cette option pour affecter la violation à un utilisateur.

Remarque : Pour plus d'informations sur l'onglet **Offenses**, consultez le guide d'utilisation IBM Security QRadar SIEM.

Gestion des rapports

QRadar SIEM propose des modèles de rapports par défaut que vous pouvez utiliser pour générer des rapports.

Ces modèles sont regroupés par types de rapports tels que Compliance, Device, Executive et Network reports. L'onglet Reports vous permet de :

- Modifier un modèle de rapport par défaut pour présenter les données personnalisées.
- Créer des modèles de rapports personnalisés.
- Définir un planning de génération des rapports personnalisés et des rapports par défaut.
- Publier le rapport dans différents formats.
- Distribuer les rapports aux autres utilisateurs QRadar SIEM.

Activation des rapports

L'onglet **Reports** vous permet d'activer, de désactiver et de modifier les modèles de rapports.

A propos de cette tâche

Cette tâche fournit un exemple d'activation des modèles de rapports Payment Card Industry (PCI).

Procédure

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

Etape 2 Décochez la case **Hide Inactive Reports**.

Etape 3 Dans la zone de liste **Group**, sélectionnez **Compliance > PCI**.

La liste des modèles PCI s'affiche.

Etape 4 Sélectionnez tous les modèles de rapports de la liste :

a Cliquez sur le premier rapport de la liste.

b Sélectionnez tous les modèles de rapports en appuyant sur la touche Shift et en la maintenant enfoncée tout en cliquant sur le dernier rapport de la liste.

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

Tous les modèles de rapports PCI sont activés. La prochaine exécution de génération de rapports s'affiche dans la colonne **Next Run Time**.

Etape 6 Pour accéder aux rapports générés :

a Dans la zone de liste de la colonne **Generated Reports**, sélectionnez l'horodatage du rapport à afficher.

b Dans la colonne **Format**, cliquez sur l'icône du format de rapport à afficher.

Le rapport s'affiche au format sélectionné.

Etape suivante

Créez un rapport personnalisé. Pour plus d'informations, voir **Création d'un rapport personnalisé**.

Création d'un rapport personnalisé

Vous pouvez créer un rapport en important une recherche ou en créant un critère de recherche personnalisé.

A propos de cette tâche

Cette tâche fournit un exemple de création d'un rapport basé sur les recherches d'événements et de flux créées dans **Recherche d'événements** et **Recherche de flux**.

Procédure

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

Etape 2 Dans la zone de liste **Actions**, sélectionnez **Create**.

La fenêtre Report Wizard s'affiche.

Remarque : Vous pouvez cocher la case pour désactiver la page Welcome.

Etape 3 Cliquez sur **Next**.

Etape 4 Configurez le planning des rapports :

- **a** Sélectionnez l'option **Daily**.
- **b** Sélectionnez les options **Monday**, **Tuesday**, **Wednesday**, **Thursday** et **Friday**.
- **c** A l'aide des zones de liste, sélectionnez **8:00** et **AM**.
- **d** Vérifiez que l'option **Yes - Manually generate report** est sélectionnée.
- **e** Cliquez sur **Next**.

Etape 5 Configurez la présentation de votre rapport :

- **a** Dans la zone de liste **Orientation**, sélectionnez **Landscape**.
- **b** Sélectionnez la présentation avec deux conteneurs de graphiques.
- **c** Cliquez sur **Next**.

Etape 6 Dans la zone **Report Title**, tapez **Sample Report**.

Etape 7 Configurez le conteneur de graphique supérieur :

- **a** Dans la zone de liste **Chart Type**, sélectionnez **Events/Logs**.

  La page Container Details - Events/Logs s'affiche.
- **b** Dans la zone **Chart Title**, tapez **Sample Event Search**.
- **c** Dans la zone de liste **Limit Events/Logs To Top**, sélectionnez **10**.
- **d** Dans la zone de liste **Graph Type** , sélectionnez **Stacked Bar**.
- **e** Sélectionnez l'option **All data from the previous (24 hours)**.
- **f** Dans la zone de liste **Base this event report on**, sélectionnez **Example Search 1**.

  Le reste des paramètres est automatiquement renseigné à l'aide des paramètres de la recherche sauvegardée *Example Search 1* .
- **g** Cliquez sur **Save Container Details**.

Etape 8 Configurez le conteneur de graphique inférieur :

a. Dans la zone de liste **Chart Type**, sélectionnez **Flows**.

b. Dans la zone **Chart Title**, tapez **Sample Flow Search**.

c. Dans la zone de liste **Limit Flows To Top**, sélectionnez **10**.

d. Dans la zone de liste **Graph Type** , sélectionnez **Stacked Bar**.

e. Sélectionnez l'option **All data from the previous 24 hours**.

f. Dans la zone de liste **Available Saved Searches**, sélectionnez **Example Search 2**.

Le reste des paramètres est automatiquement renseigné à l'aide des paramètres de la recherche sauvegardée *Example Search 2* .

g. Cliquez sur **Save Container Details**.

La page Report Layout Preview s'affiche.

Etape 9 Cliquez sur **Next**.

Un aperçu du rapport s'affiche.

Etape 10 Cliquez sur **Next**.

La fenêtre Report Format s'affiche.

Etape 11 Choisissez le format du rapport :

a. Cochez les cases **PDF** et **HTML**.

b. Cliquez sur **Next**.

Etape 12 Choisissez les canaux de distribution du rapport :

a. Vérifiez que la case **Report Console** est cochée.

b. Cochez la case **Email**.

Les paramètres supplémentaires s'affichent.

c. Dans la zone **Enter the report destination email address(es)**, tapez votre adresse électronique.

d. Cochez la case **Include Report as attachment**.

e. Cliquez sur **Next**.

Etape 13 Indiquez les derniers détails de Report Wizard :

a. Dans la zone **Report Description**, tapez une description du modèle.

b. Cochez la case **Yes - Run this report when the wizard is complete**.

c. Cliquez sur **Finish**.

La page Reports Wizard se ferme. Attendez que le rapport soit généré. La génération de rapport peut prendre quelques minutes.

Etape 14 Dans la zone de liste de la colonne **Generated Reports**, sélectionnez l'horodatage de votre rapport.

Etape 15 Cliquez sur l'icône **PDF** ou **HTML** pour afficher le rapport.

A GLOSSAIRE

Amplitude Indique l'importance relative de la violation et constitue une valeur pondérée calculée à partir des mesures de pertinence, de gravité et de 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.

Chiffrement Le chiffrement offre une plus grande sécurité à l'intégralité du trafic QRadar 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

CIDR Voir Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR) Schéma d'adressage Internet 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.

Demilitarized Zone (DMZ) Une zone démilitarisée, ou réseau de périmètre, est une zone de réseau située entre un réseau interne d'une organisation et un réseau externe, généralement Internet. Elle est séparée par un pare-feu qui permet seulement à certains types de trafic réseau d'entrer ou de sortir.

Device Support Module (DSM) Les modules Device Support Modules vous permettent d'intégrer QRadar avec des sources de journaux.

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.

DNS Voir Domain Name System.

Données de flux Caractéristiques d'un flux comprenant : adresses IP, ports, protocole, octets, paquets, balises, direction, ID d'application et donnée de contenu (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.

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 Session de communication entre deux hôtes. Un flux décrit la façon dont le trafic est communiqué, 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.

Gravité Indique la menace que représente une source par rapport au niveau de préparation de la cible contre l'attaque. Cette valeur est mappée vers une catégorie d'événement de la mappe QID qui est comparée à la violation.

Heure système Dans l'angle droit de l'interface utilisateur s'affiche l'heure du système qui correspond à l'heure de la console QRadar. 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.

Intervalle de rapport Intervalle de temps configurable selon lequel le processeur d'événement doit envoyer la totalité des événements capturés et des données de flux vers la console.

IP Voir protocole IP.

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.

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.
Payment Card Industry	Norme de sécurité des informations pour les organisations traitant des informations de carte de paiement. Cette norme permet d'augmenter les contrôles et prouve la conformité du traitement des données sensibles.
PCI	Voir Payment Card Industry.
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 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.
R2L	Voir Remote To Local.
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.
Règles	Collecte des conditions et des actions qui en découlent. Vous pouvez configurer les règles qui permettent à QRadar de capturer des séries d'événements précises et d'y répondre. Les règles vous permettent de détecter les événements spécifiques et spécialisés et de transmettre les notifications à l'onglet **Offenses** , de consigner le fichier ou d'envoyer un courriel à un utilisateur.
Remote to Local (R2L)	Trafic externe entre un réseau distant et un réseau local.
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).
TCP	Voir Transmission Control Protocol.
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	Message envoyé ou événement généré en réponse à une condition contrôlée. Par exemple, une violation peut vous informer sur une violation des règles ou une attaque du réseau.

B AVIS ET MARQUES

Dans cette annexe :

- **Avis**
- **Marques**

Cette section décrit quelques avis et marques importants et fournit des informations sur la conformité.

Avis

Ces informations étaient destinées aux produits et services offerts aux Etats-Unis.

IBM peut ne pas offrir les produits, les services ou les fonctions décrits dans ce document dans d'autres pays. Contactez votre interlocuteur IBM habituel pour obtenir des informations sur les produits et services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre produit, programme ou service fonctionnellement équivalent peut être utilisé, s'il n'enfreint pas les droits de propriété intellectuelle d'IBM. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier le fonctionnement de tout produit, programme ou service non IBM.

IBM peut détenir des brevets ou des demandes de brevet en instance couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Vous pouvez soumettre des demandes de licences par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octets peuvent être obtenues auprès du service IBM Intellectual Property Department de votre pays/région 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 est disponible sur la page Web “Copyright and trademark information” à l'adresse *www.ibm.com/legal/copytrade.shtml*.

Les noms suivants sont des marques ou des marques déposées d'autres sociétés :

Java et toutes les marques et tous les logos Java sont des marques ou des marques déposées d'Oracle et/ou de ses filiales.

Linux est une marque de Linus Torvalds aux Etats-Unis, dans d'autres pays ou les deux.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis, dans d'autres pays ou les deux.

UNIX est une marque de The Open Group aux Etats-Unis et dans d'autres pays.

INDEX

A

activation
- affichage de compatibilité d'Internet Explorer 7
- indexation de contenu 17

activation et désactivation
- rapports 29

affichage
- violations 27

ajout automatique
- bloc de construction 19

ajout manuel
- bloc de construction 19

B

blocs de construction
- ajout automatique 19
- ajout manuel 19
- réglage de QRadar SIEM 18

C

collecte
- événements QRadar SIEM 15
- flux QRadar SIEM 15

collecte d'événements
- onglet log activity 15
- QRadar SIEM 15

collecte de données
- QRadar SIEM 13

collecte de flux
- onglet network activity 15
- QRadar SIEM 15

configuration
- graphiques de série temporelle 23
- paramètres de mise à jour automatique 12
- QRadar SIEM 10
- règles 20, 28

connexion
- QRadar SIEM 7

conventions 1

création
- élément de tableau de bord 26

D

Dispositif QRadar SIEM 9

dispositif QRadar SIEM
- installation 10

E

élément de tableau de bord
- création 26

événements
- collecte 15
- recherche 22

F

flux
- collecte 15
- recherche 25

G

glossaire 32

graphiques de série temporelle
- configuration 23

I

importation
- informations d'évaluation de la vulnérabilité 16

indexation de contenu 17
- activation 17
- désactivation 18
- propriété de filtre rapide 17
- réglage QRadar SIEM 17

informations d'évaluation de la vulnérabilité
- importation 16

installation
- dispositif QRadar SIEM 10

InternetExplorer
- activation de l'affichage de compatibilité 7

M

modèle sim
- nettoyage 21

N

navigateurs Web

pris en charge 6
navigateurs Web pris en charge 6
nettoyage
modèle sim 21

O

onglet assets 4
recherche d'actifs 26
onglet log activity 3
collecte d'événements 15
recherche d'événements 22
sauvegarde des critères de recherche 23
onglet network activity 3
collecte de flux 15
recherche de flux 25
sauvegarde des critères de recherche 25
onglet offenses 4
affichage des violations 27
étude des violations 27
onglet reports 4
activation et désactivation des rapports 29
création d'un rapport personnalisé 30
gestion des rapports 28

P

paramètres de mise à jour automatique
configuration 12
propriété de filtre rapide
indexation de contenu 17

Q

QRadar SIEM
collecte d'événements 15
collecte de données 13
collecte de flux 15
configuration 10
connexion 7
règles 20
structure hiérarchique du réseau 10

R

rapports
activation et désactivation 29
création d'un rapport personnalisé 30
gestion 28
rapports personnalisés 30
recherche
actifs 26
événements 22
flux 25
sauvegarde des critères de recherche des événements 23
sauvegarde des critères de recherche des flux 25
réglage de QRadar SIEM 16
activation de l'indexation de contenu 17
configuration des règles 20
serveurs et blocs de construction 18
réglage QRadar SIEM 17
indexation de contenu 17
règles
configuration 20, 28
QRadar SIEM 20
révision
structure hiérarchique du réseau 11

S

serveurs
réglage de QRadar SIEM 18
structure hiérarchique du réseau
QRadar SIEM 10
révision 11

V

violations
affichage 27
étude 27