

IBM Security QRadar SIEM
Version 7.1.0 (MR1)

Guide d'initiation



Remarque : Avant d'utiliser le présent document et le produit associé, lisez les information disponibles dans ["Avis et Marques"](#) à la [page 39](#)

A PROPOS DE CE MANUEL

Le guide d'initiation *IBM Security QRadar SIEM* fournit des instructions de démarrage à l'aide de QRadar SIEM. Nous vous conseillons de suivre les recommandations figurant dans ce manuel afin d'évaluer au mieux la fonctionnalité 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 que vous avez accès à QRadar SIEM et que vous maîtrisez votre réseau d'entreprise et les technologies réseau.

Conventions de la documentation Les conventions suivantes s'appliquent dans ce manuel :

- Indique que la procédure contient une seule instruction.

NOTE 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.



WARNING

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>)

CONTENU

A PROPOS DE CE MANUEL

Public cible	1
Conventions de la documentation	1
Documentation technique	1
Contacteur le service clients	2

1 PRÉSENTATION

Navigateurs Web pris en charge	3
Activation de Compatibility View pour Internet Explorer	4
Connexion à QRadar SIEM	4
Onglet Log Activity	6
Onglet Network Activity	6
Onglet Assets	6
Onglet Offenses	7
Onglet Reports	7

2 DÉPLOIEMENT DE QRADAR SIEM

Installation du dispositif QRadar SIEM	9
Première étape Configuration de QRadar SIEM	10
Modification de votre hiérarchie de réseau	10
Configuration des paramètres de mise à jour automatique	12
Collecte de données	13
Collecte d'événements	13
Collecte de flux	14
Importation des informations sur l'évaluation de la vulnérabilité	16
Réglage et configuration de QRadar SIEM	17
Indexation du contenu	17
Activation de l'indexation du contenu	18
Désactivation de l'indexation du contenu	18
Ajout automatique des serveurs aux éléments structurants	19
Ajout manuel des serveurs aux éléments structurants	20
Configuration des règles	21
Nettoyage du modèle SIM	21

3 UTILISATION DE QRADAR SIEM

Etude d'événements	23
------------------------------	----

Recherche d'événements	24
Enregistrement des critères de recherche	24
Configuration d'un graphique de série temporelle.	25
Etude des flux.	26
Recherche des flux	26
Enregistrement des critères de recherche	26
Création d'un élément de tableau de bord	27
Recherche d'actifs	27
Etude des violations	28
Affichage des violations.	29
Configuration des règles	29
Gestion des rapports	30
Activation des rapports	30
Création d'un rapport personnalisé	31

A GLOSSAIRE

B AVIS ET MARQUES

Avis.	39
Marques	41

INDEX

1

PRÉSENTATION

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.

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

Cette section comprend les rubriques suivantes :

- [Navigateurs Web pris en charge](#)
- [Connexion à QRadar SIEM](#)
- [Onglet Log Activity](#)
- [Onglet Network Activity](#)
- [Onglet Assets](#)
- [Onglet Offenses](#)
- [Onglet Reports](#)

Navigateurs Web pris en charge

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

Table 2-1 Navigateurs Web pris en charge

Navigateur Web	Versions prises en charge
Mozilla Firefox	<ul style="list-style-type: none">• 10.0 <p>Compte tenu du cycle d'édition court de Mozilla, nous ne pouvons pas soumettre au test les toutes dernières versions du navigateur Mozilla Firefox. Cependant, nous pouvons tout à fait soumettre à l'étude les différents problèmes signalés.</p>

Table 2-1 Navigateurs Web pris en charge

Navigateur Web	Versions prises en charge
Microsoft Windows Internet Explorer, avec vue de compatibilité activée	<ul style="list-style-type: none"> 8.0 9.0 <p>Pour obtenir des instructions sur la façon d'activer la vue Compatibility View, voir Activation de Compatibility View pour Internet Explorer.</p>

Activation de Compatibility View pour Internet Explorer

Pour activer Compatibility View pour Internet Explorer 8.0 et 9.0 :

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

Etape 2 Configurez les paramètres de compatibilité suivants :

Table 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 .

Connexion à QRadar SIEM

Pour vous connecter à QRadar SIEM :

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*.

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

NOTE Pour vous déconnecter de QRadar SIEM, cliquez sur **logout** en haut à gauche de l'interface utilisateur.

Une clé de licence par défaut vous permet d'accéder à l'interface utilisateur pendant cinq semaines. Une fenêtre s'affiche et indique la date d'expiration de la clé de licence temporaire. Pour plus d'informations sur l'installation d'une clé de licence, voir *IBM Security QRadar SIEM Administration Guide*.

NOTE

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. 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.

Onglet Log Activity

L'onglet **Log Activity** affiche des informations liées à un événement sous forme d'enregistrements provenant d'une source de journal, comme un pare-feu ou un routeur, ce qui vous permet de contrôler et étudier les événements en temps réel ou d'effectuer des recherches avancées. 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 [Etude d'événements](#).

Onglet Network Activity

L'onglet **Network Activity** vous permet d'étudier les sessions de communication entre deux hôtes. Vous pouvez utiliser ces informations pour déterminer 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 [Etude des flux](#).

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.

- Afficher tous les actifs étudiés.
- Afficher les informations d'identité des actifs étudiés.
- Régler les vulnérabilités aux faux positifs.

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

Onglet Offenses

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 une violation afin de déterminer la cause première d'un problème. L'onglet **Offenses** vous permet de :

- Etudier les violations, les adresses IP source et cible, les comportements de réseau et les anomalies de votre réseau.
- Comparer les événements et les flux provenant de réseaux multiples vers la même adresse IP de destination.
- Etudier 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 [Etude des violations](#).

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 DÉPLOIEMENT QRADAR SIEM

Avant de pouvoir évaluer les capacités clés QRadar SIEM, vous devez tout d'abord installer le dispositif QRadar SIEM, configurer votre installation et lancer la collecte de données.

Cette section comprend les rubriques suivantes :

- [Installation du dispositif QRadar SIEM](#)
- [première étape : configuration de QRadar SIEM](#)
- [Collecte de données](#)
- [Réglage et configuration de QRadar SIEM](#)

Installation du 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. 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)

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 component dans QRadar SIEM.

Pour plus d'informations, voir *IBM Security QRadar SIEM Administration Guide*.

NOTE

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 ce total.

Pour installer le dispositif QRadar SIEM :

- Etape 1** Connectez l'interface réseau de gestion au port ETH0.
- Etape 2** Vérifiez que les connexions de puissance dédiées sont branchées 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** S'il existe un panneau frontal sur le dispositif, 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.

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

Le dispositif lance le processus d'amorçage.

Première étape : configuration de QRadar SIEM

Vous pouvez accéder à la console à partir d'un navigateur Web standard. Lorsque vous accédez à QRadar SIEM, une invite s'affiche demandant un nom d'utilisateur et un mot de passe, configurés à l'avance par votre ingénieur Q1 Labs sur site. Pour plus d'informations sur l'ouverture de session de QRadar SIEM, voir [Connexion à QRadar SIEM](#). Pour plus d'informations sur les navigateurs Web pris en charge, voir [Navigateurs Web pris en charge](#).

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

Avant de commencer, confirmez que le bureau que vous prévoyez d'utiliser 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

Cette section comprend les rubriques suivantes :

- [Modification de votre hiérarchie de réseau](#)
- [Configuration des paramètres de mise à jour automatique](#)

Modification de votre hiérarchie de réseau

La fonction de hiérarchie de réseau vous permet d'effectuer les opérations suivantes :

- Afficher différentes zones de votre réseau organisées suivant leur fonction métier.

- 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 votre trafic réseau et vous permettre d'afficher l'activité de réseau.
- Contrôler les groupes logiques spécifiques ou les services de votre réseau tels que le marketing, DMZ ou VoIP.
- Contrôler tout le trafic et créer un profil du comportement de chaque groupe et hôte du groupe.
- Identifier les hôtes locaux et les hôtes 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.

NOTE

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, voir *IBM Security QRadar SIEM Administration Guide*.

Pour modifier votre hiérarchie de réseau :

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

Pour plus d'informations sur les paramètres disponibles sous l'onglet **Admin**, voir *IBM Security QRadar SIEM Administration Guide*.

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

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

NOTE

Les objets définis dans votre hiérarchie de réseau ne doivent pas nécessairement se trouver dans votre environnement. Chaque plage de réseau logique de votre infrastructure doit être définie comme un objet réseau.

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**.

La sous-fenêtre Properties For Regulatory Compliance s'affiche.

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.

Configuration des paramètres de mise à jour automatique

Grâce aux paramètres de mise à jour automatique, vous pouvez personnaliser la fréquence, le type de mise à jour, la configuration du serveur et les paramètres de sauvegarde. 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 le contenu supplémentaire de l'aide en ligne et les scripts mis à jour.

Pour configurer les paramètres de mise à jour automatique :

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**.

La fenêtre Updates s'affiche.

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

La page Update Configuration s'affiche.

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**.

Si cette case est décochée, une notification système s'affiche sous l'onglet **Dashboard** et indique que vous devez déployer les changements une fois les mises à jour installées. Par défaut, la case est cochée.

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**.

Vos paramètres de mise à jour automatique QRadar SIEM sont alors configurés. Pour plus d'informations sur les paramètres et les options de configuration, voir *IBM Security QRadar SIEM Users Guide*.

Collecte de données

QRadar SIEM peut accepter 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. Ces données sont classées en trois sections principales : événements, flux et informations Vulnerability Assessment (VA).

Cette section comprend les rubriques suivantes :

- [Collecte d'événements](#)
- [Collecte de flux](#)
- [Importation des informations sur l'évaluation de la vulnérabilité](#)

Collecte d'événements

Les sources de journaux telles que les pare-feux, les routeurs, les serveurs UNIX, Linux, ou Windows et les systèmes Intrusion Detection Systems (IDS) ou Intrusion Prevention Systems (IPS) génèrent des journaux d'événements. 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 ou un agent ou les deux 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, voir *Configuring DSMs Guide*.

NOTE

Certains types de sources de journaux tels que les routeurs et les commutateurs, n'envoient pas assez des 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, voir *Log Sources Users Guide*.

Pour modifier les sources de journaux :

- 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 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. QRadar SIEM accepte simultanément plusieurs formats de flux. Les informations de flux permettent à QRadar SIEM de détecter les menaces et les 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 que le port de la fonction miroir est 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.

Pour modifier les sources de flux :

- 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 sources 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**.

NOTE

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

QRadar SIEM peut importer des informations Vulnerability Assessment (VA) de différents scanners tiers. Les informations VA permettent à QRadar SIEM d'identifier les hôtes actifs, les ports ouvertes et les éventuelles vulnérabilités. QRadar SIEM utilise les informations VA pour classer l'ampleur des violations sur votre réseau. Suivant 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.

Pour ajouter des scanners VA :

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**.

La fenêtre VA Scanners s'affiche.

Etape 4 Cliquez sur **Add**.

La page Add Scanner s'affiche.

Etape 5 Entrez les valeurs des paramètres.

Les paramètres dépendent du type de scanner que vous souhaitez ajouter. Pour plus d'informations, voir *Managing Vulnerability Assessment Guide*.

NOTE

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**.

La fenêtre Scan Scheduling s'affiche.

Etape 9 Cliquez sur **Add**.

La page Add Schedule s'affiche.

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 et configuration de QRadar SIEM

Maintenant que vous avez installé et configuré votre dispositif d'évaluation QRadar SIEM, vous pouvez régler et configurer QRadar SIEM pour répondre aux besoins de votre environnement.



ATTENTION

Avant de commencer cette section, nous vous recommandons d'attendre 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.

Cette section comprend les rubriques suivantes :

- [Indexation du contenu](#)
- [Ajout automatique des serveurs aux éléments structurants.](#)
- [Ajout manuel des serveurs aux éléments structurants.](#)
- [Configuration des règles.](#)
- [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 fonction 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

*Le fait d'activer l'indexation de contenu peut diminuer les performances du système. Nous vous recommandons de contrôler les statistiques d'index 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*.*

Cette section comprend les rubriques suivantes :

- [Activation de l'indexation du contenu](#)
- [Désactivation de l'indexation du contenu](#)

Activation de l'indexation du contenu Pour activer l'indexation du contenu de la propriété Quick Filter :

- 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**.
La fenêtre Index Management s'affiche.
- Etape 4** Dans la zone **Quick Search**, saisissez **Quick Filter**.
La propriété Quick Filter s'affiche pour les événements et les flux.
- Etape 5** Cliquez sur la propriété **Quick Filter** que vous souhaitez indexer.
- Etape 6** Cliquez sur **Enable Index**.

NOTE Vous pouvez également cliquer avec le bouton droit de la souris sur une propriété et sélectionner **Enable Index** dans le menu.

- Etape 7** Cliquez sur **Save**.
- Etape 8** Cliquez sur **OK**.

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

NOTE 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 Pour désactiver l'indexation du contenu de la propriété Quick Filter :

- 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**.
La fenêtre Index Management s'affiche.
- Etape 4** Dans la zone **Quick Search**, saisissez **Quick Filter**.
La propriété Quick Filter s'affiche pour les événements et les flux.
- Etape 5** Cliquez sur la propriété **Quick Filter** que vous souhaitez désactiver.
- Etape 6** Cliquez sur **Disable Index**.

NOTE Vous pouvez également cliquer avec le bouton droit de la souris sur une propriété et sélectionner **Disable Index** dans le menu.

- Etape 7** Cliquez sur **Save**.

Une fenêtre de confirmation s'affiche.

Etape 8 Cliquez sur **OK**.

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

NOTE

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

Ajout automatique des serveurs aux éléments structurants

QRadar SIEM reconnaît et classe 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 éléments structurants.

NOTE

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

Les éléments structurants vous permettent de réutiliser les tests de règles spécifiques dans d'autres règles. QRadar SIEM utilise les éléments structurants 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 se focaliser sur l'identification des actifs critiques métier.

Pour ajouter automatiquement des serveurs aux éléments structurants :

Etape 9 Cliquez sur l'onglet **Assets**.

Etape 10 Dans le menu de navigation, cliquez sur **Server Discovery**.

Etape 11 Dans la zone de liste **Server Type**, sélectionnez le type de serveur à reconnaître. Laissez le reste des paramètres comme paramètres par défaut.

Etape 12 Cliquez sur **Discover Servers**.

Etape 13 Dans la table **Matching Servers**, cochez la case de tous les serveurs que vous souhaitez affecter au rôle de serveur.

Etape 14 Cliquez sur **Approve Selected Servers**.

NOTE

Si nécessaire, 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 des serveurs aux éléments structurants

Si un serveur n'est pas automatiquement détecté, vous pouvez l'ajouter manuellement à ses éléments structurants de définition d'hôte correspondants. Cela vous permet de vous assurer que les règles appropriées s'appliquent 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 serveurs non conformes aux protocoles uniques dans leurs éléments structurants de définition d'hôte respectifs. Par exemple, le fait d'ajouter les types de serveurs suivants à des éléments structurants permet de réduire le besoin de réglage supplémentaire des faux positifs :

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

Pour ajouter manuellement des serveurs aux éléments structurants :

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

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

La page des règles s'affiche.

Etape 3 Dans la zone de liste **Display**, sélectionnez **Building Blocks**.

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

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

Les éléments structurants contiennent les hôtes automatiquement reconnus lorsque vous avez exécuté la tâche [Ajout automatique des serveurs aux éléments structurants](#).

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

La fenêtre Rule Wizard s'affiche.

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**.

Une fenêtre Rules Wizard s'affiche.

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 à l'élément structurant.

Etape 8 Cliquez sur **Add**.

Etape 9 Cliquez sur **Submit**.

Etape 10 Cliquez sur **Finish**.

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

Configuration des règles

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. Nous vous recommandons de modifier les règles par défaut afin qu'elles répondent à vos besoins de sécurité si nécessaire. Pour plus d'informations sur la modification des critères de règles, voir *IBM Security QRadar SIEM Administration Guide*. L'onglet **Offenses** vous permet de :

- Activer ou désactiver les règles.
- Modifier les critères de règles.

Pour configurer les règles :

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

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

La page des règles s'affiche.

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

La liste des règles désactivées s'affiche en haut de la liste.

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

La fonction Clean SIM Model permet de s'assurer que les violations sont basées sur les règles les plus courantes, les serveurs reconnus et la hiérarchie du réseau. Dans votre évaluation, les violations de faux positifs peuvent se produire avant d'exécuter les tâches de réglage. Nous vous recommandons de réinitialiser le modèle de données afin de vous assurer que chaque hôte de votre réseau crée de nouvelles violations basées sur votre configuration en cours.

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.

Pour nettoyer le modèle SIM :

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

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

La fenêtre Reset SIM Data Model s'affiche.

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

3

UTILISATION DE QRADAR SIEM

Une fois que vous avez déployé et réglé QRadar SIEM pour votre environnement, vous pouvez utiliser QRadar SIEM pour :

- Effectuer des recherches d'événements, de flux et d'actifs.
- Etudier les violations.
- 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.

Cette section comprend les rubriques suivantes :

- [Etude d'événements](#)
- [Etude des flux](#)
- [Recherche d'actifs](#)
- [Etude des violations](#)
- [Gestion des rapports](#)

Etude d'événements

Grâce à la fonction de recherche, vous pouvez rechercher des données d'événement en utilisant des critères spécifiques et afficher dans une liste de résultats les événements qui correspondent aux critères de recherche. Vous pouvez créer une nouvelle recherche ou charger un ensemble de critères de recherche précédemment enregistré. Vous pouvez sélectionner, organiser et grouper les colonnes de données d'événement à afficher dans les résultats de la recherche.

Cette section comprend les rubriques suivantes :

- [Recherche d'événements](#)
- [Enregistrement des critères de recherche](#)
- [Configuration d'un graphique de série temporelle](#)

Recherche d'événements Pour rechercher tous les événements d'authentification que QRadar SIEM a reçus au cours des six dernières heures :

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

La page Log Activity affiche les événements en mode temps réel.

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

La page de recherche d'un nouvel événement s'affiche.

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**.

Tous les événements d'authentification des 6 dernières heures s'affichent, triés via la colonne **Event Name**.

Enregistrement des critères de recherche Pour enregistrer les critères de recherche spécifiés pour une utilisation ultérieure :

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

La fenêtre Save Criteria s'affiche.

Etape 2 Dans la zone **Search Name**, entrez le nom **Example Search 1**.

Etape 3 Dans la sous-fenêtre d'options Timespan, sélectionnez l'option **Recent**.

Etape 4 Dans la zone de liste, sélectionnez **Last 6 Hours**.

Etape 5 Cochez les cases **Include in my Quick Searches** et **Include in my Dashboard**.

NOTE

*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 6 Cliquez sur **OK**.

Configuration d'un graphique de série temporelle

les graphiques de série temporelle vous permettent d'afficher des graphiques à courbes interactifs représentant les enregistrements comparés par une recherche d'intervalle de temps spécifique.

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 [Enregistrement des critères de recherche](#).

Pour configurer un graphique de série temporelle :

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

Les options de configuration s'affichent.

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**.

La liste des événements se met à jour pour afficher l'activité du journal en fonction de la configuration de votre graphique de série temporelle.

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 est 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**.

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

Etude des flux

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. Vous pouvez afficher les informations de flux afin de déterminer la façon dont le trafic est communiqué et quels éléments sont communiqués.

Cette section comprend les rubriques suivantes :

- **Recherche des flux**
- **Enregistrement des critères de recherche**
- **Création d'un élément de tableau de bord**

Recherche des flux Pour rechercher les flux :

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

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

La page de recherche d'un nouveau flux s'affiche.

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**.

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**.

Enregistrement des critères de recherche

Enregistrez vos critères de recherche :

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

La fenêtre Save Criteria s'affiche.

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**.

Création d'un élément de tableau de bord

Pour créer un élément de tableau de bord :

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**.

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, voir *IBM Security QRadar SIEM Users Guide*.

Recherche d'actifs

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

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.

Pour rechercher les actifs :

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

La page Assets Profile Search s'affiche.

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**.

La liste des actifs s'affiche.

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

La fenêtre Asset Profile s'affiche avec toutes les informations connues concernant l'hôte, comme :

- Adresse MAC
- Dernier nom d'utilisateur connu
- Nom d'hôte
- Informations sur le système d'exploitation
- Informations sur le propriétaire métier et technique
- Ports ouverts et vulnérabilités connues

Vous pouvez afficher l'historique des événements.

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**.

La fenêtre Event Search s'affiche et est préalablement renseignée par les critères de recherche d'événements.

Etape 5 Cliquez sur **Search**.

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

Etude 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. 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.

Cette section comprend les rubriques suivantes :

- [Affichage des violations](#)

- **Configuration des règles**

Affichage des violations Pour afficher une violation :

- Etape 1** Cliquez sur l'onglet **Offenses**.
- Etape 2** Cliquez deux fois sur la violation à étudier.
La page *Offense Summary* s'affiche.
- 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**.
La fenêtre *List of Events* affiche tous les événements associés à la violation. Pour plus d'informations sur la recherche, le tri et le filtrage des événements, voir [Recherche d'événements](#).

Configuration des règles Les onglets **Log Activity**, **Network Activity** et **Offenses** vous permettent de configurer les règles ou les éléments structurants. Les règles réalisent des tests sur les événements, les flux ou les violations. Si toutes les conditions d'un test sont respectées, la règle génère une réponse. Pour obtenir une liste complète des règles par défaut, voir *IBM Security QRadar SIEM Administration Guide*.

Pour étudier les règles ayant contribué à une violation :

- Etape 1** Cliquez sur l'onglet **Offenses**.
La page *All Offenses* s'affiche.
- Etape 2** Cliquez deux fois sur la violation à étudier.
- Etape 3** Cliquez sur **Display > Rules**.
Une liste de toutes les règles générées au cours de la violation s'affiche.
- Etape 4** Cliquez deux fois sur une règle.
La page *Rules Wizard* s'affiche et vous permet de modifier la règle sélectionnée. Si nécessaire, vous pouvez encore régler les règles. Pour plus d'informations sur le réglage des règles, voir *IBM Security QRadar SIEM Administration Guide*.
- Etape 5** Fermez l'assistant *Rules*.
- Etape 6** Dans la page *Rules*, cliquez sur **Actions** et sélectionnez l'une des options suivantes :
 - **Follow up** - Sélectionnez cette option pour baliser la violation pour 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.

NOTE

Pour plus d'informations sur l'onglet **Offenses**, consultez le guide d'utilisateur 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.

Cette section comprend les rubriques suivantes :

- [Activation des rapports](#)
- [Création d'un rapport personnalisé](#)

Activation des rapports

Par défaut, certains modèles de rapports sont désactivés dans QRadar SIEM. L'onglet **Reports** vous permet d'activer, des désactiver et de modifier les modèles de rapports si nécessaire. Dans l'exemple suivant, vous activez les modèles de rapports Payment Card Industry (PCI).

Pour activer les rapports :

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

La page Reports s'affiche.

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 :

- Cliquez sur le premier rapport de la liste.
- 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 :

- Dans la zone de liste de la colonne **Generated Reports**, sélectionnez l'horodatage du rapport à afficher.
- Dans la colonne **Format**, cliquez sur l'icône du format de rapport à afficher. Le rapport s'affiche au format sélectionné.

Création d'un rapport personnalisé Pour créer un rapport personnalisé, vous pouvez importer une recherche ou créer des critères personnalisés. Dans la procédure suivante, vous créez un rapport basé sur les recherches d'événements et de flux créées dans **Etude d'événements** et **Etude des flux**.

Pour créer un rapport personnalisé :

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

La page Reports s'affiche.

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

La fenêtre Report Wizard s'affiche.

NOTE

Vous pouvez cocher la case pour désactiver la page Welcome.

Etape 3 Cliquez sur **Next**.

Etape 4 Configurez le planning des rapports :

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

Etape 5 Configurez la présentation de votre rapport :

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

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

Etape 7 Configurez le conteneur de graphique supérieur :

- Dans la zone de liste **Chart Type**, sélectionnez **Events/Logs**.
La page Container Details - Events/Logs s'affiche.
- 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**.
L'écran de présentation de rapport s'affiche.

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**.

La fenêtre Finishing Up s'affiche.

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.

Vous venez de compléter la configuration initiale, effectuer le réglage et exécuter QRadar SIEM.

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 un 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.
données de flux	Caractéristiques d'un flux comprenant : les adresses IP, les ports, le protocole, les octets, la paquets, les balises, la direction, l'ID d'application et les données de contenu (facultatif).

DNS	Voir Domain Name System.
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).
élément	Option du tableau de bord qui crée un portail personnalisé affichant toutes les vues possibles pour le contrôle.
événement	Enregistrement d'un périphérique décrivant une action sur un réseau ou un hôte.
faux positif	Lorsqu'un événement est paramétré sur faux positif, il ne contribue plus aux règles personnalisées, c'est pourquoi les violations ne sont pas générées en fonction de l'événement de faux positif. L'événement reste stocké dans la base de données et contribue à la génération de rapports.
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 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	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.
R2L	Voir Remote To Local.
Remote to Local (R2L)	Trafic externe entre un réseau distant et un réseau 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 des événements précis et spécialisés et de transférer les notifications vers l'onglet Offenses ou le fichier journal ou encore d'envoyer un e-mail à un utilisateur.
Simple Network Management Protocol (SNMP)	Protocole de gestion de réseau utilisé pour contrôler les routeurs IP, les autres périphériques réseau et les réseaux auxquels ils sont associés.
SNMP	Voir Simple Network Management Protocol.
sources de flux	Source de flux reçue par QFlow Collector. Grâce à l'éditeur de déploiement, vous pouvez ajouter des sources de flux internes et externes provenant du système ou de l'élément Event Views de l'éditeur de déploiement.
source de journal	Les sources de journaux sont des sources de journaux d'événements externes telles que le matériel de sécurité (par exemple les pare-feux et les IDS) et le matériel de réseau (par exemple les commutateurs et les routeurs).
TCP	Voir Transmission Control Protocol.

Transmission Control Protocol (TCP)	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.
violation	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.

B

AVIS ET MARQUES

Dans cet annexe :

- [Avis](#)
- [Marques](#)

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

Avis

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

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

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

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

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues auprès du service IBM Intellectual Property Department de votre pays ou par écrit à l'adresse suivante :

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : INTERNATIONAL BUSINESS MACHINES CORPORATION LIVRE LE PRESENT DOCUMENT "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER, TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties explicites ou implicites pour certaines transactions, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Ces informations peuvent contenir des inexactitudes techniques ou des erreurs typographiques. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

*IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA*

Ces informations peuvent être soumises à des dispositions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions d'IBM Customer Agreement, d'IBM International Program License Agreement ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via

d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les prix IBM indiqués sont des prix de détail suggérés par IBM, sont à jour et peuvent être modifiés sans préavis. Les prix distributeurs peuvent donc varier.

Ces informations contiennent des exemples de données et de rapports utilisés dans les opérations métier habituelles. Pour les illustrer aussi complètement que possible, les exemples incluent les noms des personnes, des sociétés, des marques et des produits. Tous ces noms sont fictifs et toute ressemblance avec des noms et adresses utilisés par une société réelle serait purement fortuite.

Si vous visualisez la copie électronique de ces informations, les photographies et illustrations en couleur peuvent ne pas apparaître.

Marques

IBM, le logo IBM et ibm.com 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 États-Unis et dans d'autres pays.

INDEX

A

onglet assets 5
 recherche des actifs 23
paramètres de mise à jour automatique
 configuration 10
ajout automatique
 éléments structurants 16

B

éléments structurants
 ajout automatique 16
 ajout manuel 16

C

nettoyage
 modèle sim 18
collecte de données
 événements 11
 flux 11
 informations sur l'évaluation de la vulnérabilité 11
collecte d'événements 11
collecte de flux 12
configuration
 paramètres de mise à jour automatique 10
 règles 17
 heure système 8
 graphiques de série temporelle 21
conventions 1
création
 élément de tableau de bord 23
 faux positifs 25
rapports personnalisés 26

D

élément de tableau de bord
 création 23

E

activation et désactivation
 rapports 26
événements
 recherche 20

F

faux positifs 25
flux
 étude 22

recherche 22

G

glossaire 29

I

importation
 informations sur l'évaluation de la vulnérabilité 13
étude
 événements 19
 flux 22
 règles 25

L

onglet log activity 5
 collecte d'événements 11
 étude des événements 19
 étude des règles 25
 sauvegarde des critères de recherche 20
 recherche d'événements 20
connexion à QRadar 4

M

ajout manuel
 éléments structurants 16

N

onglet network activity 5
 collecte de flux 12
 étude des flux 22
 étude des règles 25
 sauvegarde des critères de recherche 22
 recherche de flux 22
hiérarchie de réseau
 modification 8

O

violations
 étude 24
 affichage 24
onglet offenses 6
 étude des violations 24
 étude des règles 25
 affichage des violations 24

Q

- QRadar
 - connexion 4
 - réglage 14

R

- rapports
 - création d'un rapport personnalisé 26
 - activation et désactivation 26
 - gestion 25
- onglet reports 6
 - création d'un rapport personnalisé 26
 - activation et désactivation des rapports 26
 - gestion des rapports 25
- modification
 - hiérarchie de réseau 8
- règles
 - configuration 17
 - étude 25

S

- recherche
 - actifs 23
 - événements 20
 - flux 22
 - sauvegarde des critères de recherche d'événements 20
 - sauvegarde des critères de recherche de flux 22
- modèle sim
 - nettoyage 18
- heure système
 - configuration 8

T

- graphiques de série temporelle
 - configuration 21
- réglage
 - création d'un faux positif 25
 - QRadar 14

V

- affichage
 - violations 24
- informations sur l'évaluation de la vulnérabilité
 - importation 13