IBM Security QRadar SIEM
Version 7.2.4

Guide d'initiation

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 25.

Ce document s'applique à IBM QRadar Security Intelligence Platform V7.2.4 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT 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.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Présentation du guide d'initiation à QRadar SIEM

Le guide d'initiation d'IBM Security QRadar SIEM présente les concepts clés et offre un aperçu du processus d'installation ainsi que des tâches de base pouvant être réalisées dans l'interface utilisateur.

Audience visée

Ces informations sont destinées aux administrateurs de sécurité responsables de l'étude et de la gestion de la sécurité réseau. Pour utiliser ce guide, vous devez connaître l'infrastructure réseau de votre société et maîtriser les technologies de mise en réseau.

Documentation technique

Pour savoir comment accéder à des informations plus techniques sous forme de documentation, fiche technique et notes sur l'édition, voir Accessing IBM® Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacter le service clients

Pour contacter le service clients, voir Support and Download Technical Note (en anglais) (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. L'accès incorrect peut engendrer la modification, la destruction, le détournement la mauvaise utilisation des informations ou peut engendrer l'endommagement ou la mauvaise utilisation des systèmes, en particulier pour l'utilisation dans les attaques ou autres. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar peut être utilisé uniquement de façon règlémentaire. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à

s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

Chapitre 1. Présentation de QRadar SIEM

IBM Security QRadar SIEM est une plateforme de gestion de sécurité des réseaux offrant une prise en charge de la géolocalisation et de la conformité. QRadar SIEM combine à la fois la connaissance du réseau de flux, la corrélation des événements de sécurité et l'évaluation de la vulnérabilité des actifs.

Pour commencer, vous devrez configurer une installation QRadar SIEM de base, collecter des données d'événements et de flux et générer des rapports.

Onglet Activité du journal

Dans IBM Security QRadar SIEM, vous pouvez surveiller et afficher les événements de réseau en temps réel ou réaliser des recherches avancées.

L'onglet **Activité du journal** 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 **Activité du journal** vous permet d'effectuer les tâches suivantes :

- Etudier les données d'événements.
- Etudier les journaux d'événements envoyés à QRadar SIEM en temps réel.
- Rechercher un événement.
- Surveiller les activités du journal à l'aide de graphiques en série temporelle configurables.
- Identifier les faux positifs pour régler QRadar SIEM.

Onglet Activité réseau

Dans IBM Security QRadar SIEM, vous pouvez examiner les sessions de communication entre deux hôtes.

L'onglet **Activité réseau** affiche des informations sur la façon dont le trafic réseau est communiqué, et sur ce qui a été communiqué, si l'option de capture de contenu est activée. L'onglet **Activité réseau** vous permet d'effectuer les tâches suivantes :

- Etudier les flux envoyés à QRadar SIEM en temps réel.
- Rechercher des flux de réseau.
- Surveiller les activités réseau à l'aide de graphiques de série temporelle configurables.

Onglet Actifs

QRadar SIEM crée automatiquement des profils d'actifs en utilisant des données de vulnérabilité et des données de flux passives pour détecter les serveurs et hôtes de votre réseau.

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 corrélation et elles aident à réduire le nombre de faux positifs.

L'onglet Actifs vous permet d'effectuer les tâches suivantes :

- Rechercher des actifs.
- Afficher tous les actifs acquis.
- Afficher les informations d'identité pour les actifs acquis.
- Ajuster les vulnérabilités de faux positifs.

Onglet Infractions

Dans IBM Security QRadar SIEM, vous pouvez étudier les infractions pour déterminer la cause première d'un problème de réseau.

Dans l'onglet **Infractions**, vous pouvez afficher toutes les infractions se produisant sur votre réseau et réaliser les tâches suivantes :

- Etudier les infractions, les adresses IP de source et de destination, les comportements de réseau ainsi que les anomalies de votre réseau.
- Mettre en corrélation les événements et les flux provenant de différents réseaux vers une même adresse IP de destination.
- Naviguer sur les différentes pages de l'onglet **Infractions** pour étudier les détails des événements et des flux.
- Identifier quels événements sont à l'origine d'une infraction.

Onglet Rapports

Dans IBM Security QRadar SIEM, vous pouvez créer des rapports personnalisés ou utiliser les rapports par défaut.

QRadar SIEM fournit des modèles de rapports par défaut que vous pouvez personnaliser, rebaptiser et distribuer aux utilisateurs de QRadar SIEM.

Les modèles de rapports sont regroupés par types de rapports, tels que les rapports de conformité, d'unité, de cadre ou de réseau. L'onglet **Rapports** vous permet de réaliser les tâches suivantes :

- Créer, distribuer et gérer des rapports pour les données QRadar SIEM.
- Créer des rapports personnalisés à des fins d'exploitation et d'exécution.
- Combiner les informations de sécurité et de réseau dans un rapport unique.
- Utiliser ou éditer les modèles de rapport pré-installés.
- Baptiser vos rapports avec des logos personnalisés. Cette fonction est utile si on souhaite distribuer les rapports à différentes audiences.
- Définir un planning de génération des rapports personnalisés et des rapports par défaut.
- Publier des rapports dans différents formats.

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.

On distingue trois catégories de données collectées : la collecte des données d'événements, la collecte des données de flux et les informations d'évaluation de la vulnérabilité.

Collecte de données d'événement

Les événements sont générés par des sources de journaux telles que les pare-feu, les routeurs, les serveurs et les systèmes de détection d'intrusion (IDS) ou les systèmes de prévention contre les intrusions (IPS).

La plupart des sources de journaux envoie des informations à QRadar SIEM à l'aide du protocole syslog. QRadar SIEM prend également en charge les protocoles suivants :

- Simple Network Management Protocol (SNMP)
- JDBC (connectivité à la base de données Java™)
- 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 de prise en charge de périphérique (DSM) approprié dans la fenêtre Sources de journal de l'onglet **Admin**.

Même si la plupart des modules DSM comprend une fonction d'envoi du journal natif, certains 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 Source de journal. 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 *Sources de journal*.

On distingue trois catégories de données collectées : la collecte des données d'événements, la collecte des données de flux et les informations d'évaluation de la vulnérabilité.

Collecte de données 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.

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.

Les Collecteurs QRadar QFlow offrent 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 uniquement de la présence d'un 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 Collecteurs QRadar QFlow sont activés par défaut et requièrent la connexion d'un port miroir, d'un port de réplication ou d'un tap réseau à une interface disponible du dispositif QRadar SIEM. L'analyse de flux commence automatiquement une fois le port 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 Risk Manager d'identifier les hôtes actifs, les ports ouverts et les éventuelles vulnérabilités.

QRadar Risk Manager utilise les informations VA pour classer l'ampleur des infractions sur votre réseau.

Selon le type de scanner VA, QRadar Risk Manager peut importer les résultats de l'analyse provenant du serveur de scanner ou lancer une analyse à distance.

Règles QRadar SIEM

Les règles effectuent des tests sur les événements, les flux ou les infractions et 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, voir le manuel *IBM Security QRadar SIEM Administration Guide*.

La liste suivante décrit deux catégories de règles :

- Les règles personnalisées effectuent des tests sur les événements, les flux et les infractions pour détecter une activité inhabituelle sur votre réseau.
- Les règles de détection des anomalies effectuent des tests sur les résultats de recherches d'événements ou de flux sauvegardés afin de détecter des modèles de trafic inhabituels dans votre réseau.

Important : Un utilisateur non administrateur peut créer des règles pour les zones du réseau auxquelles il a accès. Vous devez disposer des autorisations de rôles appropriées pour gérer les règles. Pour plus d'informations sur les autorisations de rôles, voir le manuel *IBM Security QRadar SIEM Administration Guide*.

Navigateurs Web pris en charge

Pour assurer une bonne exécution des fonctions des produits IBM Security QRadar, vous devez utiliser un navigateur Web pris en charge.

Lorsque vous accédez au système QRadar, vous êtes invités à indiquer un nom d'utilisateur et un mot de passe. Le nom d'utilisateur et le mot de passe doivent être configurés à l'avance par l'administrateur.

Le tableau suivant répertorie les versions prises en charge des navigateurs Web.

Tableau 1. Navigateurs Web pris en charge par les produits QRadar

Navigateur Web	**Version prise en charge**
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer 32 bits, avec mode document et mode navigateur activés	9.0 10
Google Chrome	Version en cours à la date d'édition des produits IBM Security QRadar V7.2.4

Chapitre 2. Initiation au déploiement de QRadar SIEM

Avant de pouvoir évaluer les fonctions clés d'IBM Security QRadar SIEM, l'administrateur doit déployer QRadar SIEM.

Pour déployer QRadar SIEM, l'administrateur doit réaliser les tâches suivantes :

- Installer le dispositif QRadar SIEM.
- Configurer votre installation QRadar SIEM.
- Collecter les données d'événements, de flux et d'évaluation de la vulnérabilité.
- Affiner votre installation QRadar SIEM.

Installation du dispositif QRadar SIEM

Les administrateurs doivent installer le dispositif QRadar SIEM pour permettre 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).
- Facultatif. Un clavier USB et un moniteur VGA standard pour l'accès à la console.

Procédure

1. Connectez l'interface réseau de gestion au port Ethernet 1.
2. Branchez les connexions de puissance dédiées à l'arrière du dispositif.
3. Si vous avez besoin d'un accès à la console, connectez le clavier USB et le moniteur VGA standard.
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.
5. Mettez le dispositif sous tension.

Le dispositif QRadar SIEM

Le dispositif d'évaluation QRadar SIEM est un serveur monté en rack à deux unités. Les rails de guidage ou les rayonnages ne sont pas fournis avec l'équipement d'évaluation.

Le dispositif QRadar SIEM comprend quatre interfaces réseau. Pour cette évaluation, utilisez l'interface Ethernet 1 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 réplication ou TAP réseau est connecté à une interface autre qu'Ethernet 1. Des étapes supplémentaires peuvent être nécessaires pour activer le composant QRadar QFlow Collector dans QRadar SIEM.

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

Restriction : Le dispositif d'évaluation QRadar SIEM a 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.

Configuration de QRadar SIEM

En configurant QRadar SIEM, vous pouvez vérifier la hiérarchie de votre réseau et personnaliser les mises à jour automatiques.

Procédure

1. Vérifiez que les applications suivantes sont installées sur tous les systèmes bureautiques que vous utilisez pour accéder à l'interface utilisateur du produit QRadar :
   - Java Runtime Environment (JRE) version 1.7 or IBM 64-bit Runtime Environment for Java V7.0
   - Adobe Flash version 10.x
2. Vérifiez que le navigateur Web utilisé est pris en charge. Voir «Navigateurs Web pris en charge», à la page 4.
3. Si vous utilisez Internet Explorer, activez le mode document et le mode navigateur.
   a. Dans votre navigateur Web Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre Outils de développement.
   b. Cliquez sur **Mode navigateur** et sélectionnez la version de votre navigateur Web.
   c. Cliquez sur **Mode document** et sélectionnez **Normes d'Internet Explorer 7.0**.
4. Connectez-vous à l'interface utilisateur de QRadar SIEM en tapant l'adresse URL suivante :

   https://<Adresse IP>

   où <Adresse IP> correspond à l'adresse IP de la QRadar SIEM Console.

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 suivant le risque de chaque valeur métier.

QRadar SIEM utilise la structure hiérarchique du réseau pour exécuter les tâches suivantes :

- Comprendre le trafic réseau et afficher l'activité 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 structure hiérarchique préconfigurée du réseau, 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 possède aucune structure hiérarchique de réseau définie, utilisez l'onglet **Admin** pour créer une structure hiérarchique spécifique à votre environnement.

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

Révision de la structure hiérarchique de votre réseau

Cette section explique comment réviser la structure hiérarchique de votre réseau.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le panneau de navigation, cliquez sur **Configuration système**.
3. Cliquez sur l'icône **Hiérarchie du réseau**.
4. Dans la liste **Gérer les groupes : Principaux**, cliquez sur **Serveurs_conformité_réglementations**.

   Si la structure hiérarchique de votre réseau n'inclut aucun composant serveur de conformité aux réglementations, vous pouvez utiliser votre composant Messagerie pour la suite de cette procédure.
5. Cliquez sur l'icône **Editer cet objet**.
6. Pour ajouter des serveurs de conformité :
   a. Dans la zone **IP/CIDR(s)**, tapez l'adresse IP ou la plage CIDR de vos serveurs de conformité.
   b. Cliquez sur **Ajouter**.
   c. Répétez l'opération pour tous les serveurs de conformité.
   d. Cliquez sur **Sauvegarder**.
   e. Répétez ce processus pour chacun des autres réseaux à modifier.
7. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les changements**.

   Vous pouvez mettre à jour vos fichiers de configuration avec les dernières informations de sécurité du réseau de façon manuelle ou automatique. QRadar SIEM utilise les fichiers de configuration pour fournir des caractérisations des flux de données du réseau.

Mises à jour automatiques

La console QRadar SIEM doit être connectée à Internet pour pouvoir recevoir des mises à jour. Si votre console n'est pas connectée à Internet, vous devez configurer un serveur de mise à jour interne.

Pour savoir comment configurer un serveur de mise à jour automatique, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*.

QRadar SIEM vous permet de remplacer vos fichiers de configuration existants ou d'intégrer les fichiers mis à jour à vos fichiers existants.

Les mises à jour du logiciel peuvent être téléchargées depuis le 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 des contenus d'aide en ligne supplémentaires ou des scripts mis à jours.

Configuration des paramètres de mise à jour automatique

Vous pouvez personnaliser la fréquence des mises à jour QRadar SIEM, ainsi que les types de mises à jour, la configuration du serveur et les paramètres de sauvegarde.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le panneau de navigation, cliquez sur **Configuration système**.
3. Cliquez sur l'icône **Mise à jour automatique**.
4. Dans le panneau de navigation, cliquez sur **Modifier les paramètres**.
5. Dans la sous-fenêtre **Planification de la mise à jour automatique**, acceptez les paramètres par défaut.
6. Dans le panneau **Types de mise à jour**, configurez les paramètres suivants :
   a. Dans la zone de liste **Mises à jour de configuration**, sélectionnez **Mise à jour automatique**.
   b. Acceptez les valeurs par défaut des paramètres suivants :
      - DSM, Scanner, Protocol Updates.
      - Major Updates.
      - Minor Updates.
7. Désélectionnez la case **Déploiement automatique**.

   Par défaut, cette case est cochée. Si la case n'est pas cochée, une notification système s'affiche sur l'onglet **Tableau de bord** pour indiquer que vous devez déployer les changements une fois les mises à jour installées.
8. Cliquez sur l'onglet **Avancé**.
9. Dans le panneau **Configuration du serveur**, acceptez les paramètres par défaut.
10. Dans le panneau **Autres paramètres**, acceptez les paramètres par défaut.
11. Cliquez sur **Sauvegarder** et fermez la fenêtre Mises à jour.
12. Dans la barre d'outils, cliquez sur **Déployer les changements**.

Collecte d'événements

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

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le panneau de navigation, cliquez sur **Sources de données**.
3. Cliquez sur l'icône **Sources de journal**.
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 le guide intitulé *Guide d'utilisation des sources de journal*.
5. Fermez la fenêtre Sources de journal.
6. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les changements**.

Collecte de flux

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

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.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Sources de données** > **Flux**.
3. Cliquez sur l'icône **Sources de flux**.
4. Consultez la liste des sources de flux et apportez les changements nécessaires à la source de flux.

   Pour plus d'informations sur la configuration des sources de flux, voir le manuel *IBM Security QRadar SIEM Administration Guide*.
5. Fermez la fenêtre Sources de flux.
6. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les changements**.

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 d'éventuelles vulnérabilités.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Sources de données** > **Vulnérabilité**.
3. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
4. Dans la barre d'outils, cliquez sur **Ajouter**.
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*.

   Important : 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.

6. Cliquez sur **Sauvegarder**.
7. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les changements**.
8. Cliquez sur l'icône **Planifier les scanners d'analyse des vulnérabilités**.
9. Cliquez sur **Ajouter**.
10. Indiquez les critères de fréquence d'analyse de votre choix.

    Suivant le type d'analyse, ceci inclura la fréquence à laquelle QRadar SIEM importe les résultats d'analyse ou démarre une nouvelle analyse. Vous devez également indiquer les ports à inclure aux résultats d'analyse.
11. Cliquez sur **Sauvegarder**.

Réglage de QRadar SIEM

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

Avant de régler QRadar SIEM, attendez un jour pour permettre à QRadar SIEM de détecter les serveurs de votre réseau, de stocker les événements et les flux et de créer des infractions basées sur des règles existantes.

Les administrateurs peuvent effectuer les tâches de réglage suivantes :

- Optimiser les recherches de contenus d'événements et de flux en activant l'index de contenu dans la propriété **Filtrage rapide** de **Activité du journal** et **Activité réseau**.
- Assurer un déploiement initial plus rapide et un réglage plus facile en ajoutant automatiquement ou manuellement des serveurs aux 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.
- S'assurer que chaque hôte de votre réseau crée des infractions basées sur les règles les plus courantes, les serveurs reconnus et la hiérarchie du réseau.

Indexation du contenu

La fonction **Filtrage rapide** disponible dans les onglets **Activité du journal** et **Activité réseau** permet de rechercher le contenu des événements et des flux.

Pour optimiser la fonction **Filtrage rapide**, vous pouvez activer un index de contenu sur la propriété **Filtrage rapide**.

L'activation de l'indexation de contenu peut diminuer les performances du système. Contrôlez les statistiques après avoir activé l'indexation de contenu sur la propriété **Filtrage rapide**.

Pour plus d'informations sur la gestion des index et leurs statistiques, voir le manuel *IBM Security QRadar SIEM Administration Guide*.

Activation de l'indexation du contenu

Cette section décrit comment optimiser les recherches de contenus d'événements ou de flux en activant un index de contenu dans la propriété **Filtrage rapide** de **Activité du journal** et **Activité réseau**.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le panneau de navigation, cliquez sur **Configuration système**.
3. Cliquez sur l'icône **Gestion de l'index**.
4. Dans la zone **Recherche rapide**, saisissez **Filtrage rapide**.
5. Cliquez sur la propriété **Filtrage rapide** que vous souhaitez indexer.
6. Cliquez sur **Activer l'index**.
7. Cliquez sur **Sauvegarder**.
8. Cliquez sur **OK**.
9. Facultatif : Pour désactiver un index de contenu, sélectionnez l'une des options suivantes :
   - Cliquez sur **Désactiver l'index**.
   - Cliquez avec le bouton droit de la souris sur une propriété et sélectionnez **Désactiver l'index** dans le menu.

Que faire ensuite

Pour obtenir des informations détaillées sur les paramètres affichés dans la fenêtre Gestion de l'index, consultez le *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.

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 serveurs non conformes à des protocoles uniques dans leurs blocs de construction de définition d'hôte respectifs. Par exemple, l'ajout des types de serveurs suivants à des blocs de construction permet de réduire le besoin de réglage supplémentaire des faux positifs :

- Ajout de serveurs de gestion au bloc de construction **BB:HostDefinition: Network Management Servers**.
- Ajout de serveurs proxy au bloc de construction **BB:HostDefinition: Proxy Servers**.
- Ajout de serveurs de mises à jour de virus et Windows au bloc de construction **BB:HostDefinition: Virus Definition and Other Update Servers**.
- Ajout de scanners d'évaluation de la vulnérabilité au bloc de construction **BB-HostDefinition: VA Scanner Source IP**.

La fonction Reconnaissance des serveurs utilise la base de données de profils d'actifs pour reconnaître plusieurs types de serveurs sur votre réseau. Elle établit de façon automatique une liste des serveurs reconnus qui vous permet de sélectionner les serveurs que vous souhaitez intégrer aux blocs de construction.

Pour plus d'informations sur la détection des serveurs, voir le manuel *IBM Security QRadar SIEM Administration Guide*.

Les blocs de construction vous permettent de réutiliser des tests de règles spécifiques dans d'autres règles. Vous pouvez réduire le nombre de faux positifs en utilisant les blocs de constructions pour régler QRadar SIEM et activer des règles de corrélation supplémentaires.

Ajout automatique de serveurs aux blocs de construction

Cette section décrit comment ajouter des serveurs aux blocs de construction de façon automatique.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, cliquez sur **Reconnaissance des serveurs**.
3. Dans la liste **Type de serveur**, sélectionnez le type de serveur que vous souhaitez détecter.

   Laissez les paramètres restants définis sur les valeurs par défaut.
4. Cliquez sur **Reconnaître les serveurs**.
5. Dans le panneau Matching Servers, sélectionnez la case de tous les serveurs que vous souhaitez affecter au rôle de serveur.
6. Cliquez sur **Approuver les serveurs sélectionnés**.

   A faire : 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 détecté automatiquement, vous pouvez l'ajouter manuellement au bloc de construction de définition d'hôte qui lui correspond.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans le panneau de navigation, cliquez sur **Règles**.
3. Dans la liste **Afficher**, sélectionnez **Blocs de construction**.
4. Dans la liste **Groupe**, sélectionnez **Définitions d'hôte**.

   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.
5. Pour ajouter un hôte ou un réseau manuellement, cliquez deux fois sur le bloc de construction de définition d'hôte correspondant à votre environnement.
6. Dans la zone **Blocs de construction**, cliquez sur la valeur soulignée après la phrase **si la source ou l'adresse IP de destination est l'une des suivantes**.
7. Dans la zone **Entrez une adresse IP ou CIDR**, tapez les noms d'hôtes ou les plages d'adresses IP que vous souhaitez affecter au bloc de construction.
8. Cliquez sur **Ajouter**.
9. Cliquez sur **Soumettre**.
10. Cliquez sur **Terminer**.
11. Répétez ces étapes pour chaque type de serveur que vous souhaitez ajouter.

Configuration des règles

Les onglets **Activité du journal**, **Activité réseau** et **Infractions** permettent de configurer des règles ou des blocs de construction.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Cliquez deux fois sur l'infraction à étudier.
3. Cliquez sur **Afficher** > **Règles**.
4. Cliquez deux fois sur une règle.

   Vous pouvez encore ajuster les règles. Pour plus d'informations sur l'optimisation des règles, voir le manuel *IBM Security QRadar SIEM Administration Guide*
5. Fermez l'assistant Règles.
6. Sur la page Règles, cliquez sur **Actions**.
7. Facultatif : Si vous souhaitez empêcher que l'infraction soit supprimée de la base de données une fois sa durée de conservation écoulée, sélectionnez **Protéger l'infraction**.
8. Facultatif : Si vous souhaitez affecter l'infraction à un utilisateur QRadar SIEM, sélectionnez **Affecter**.

Concepts associés:

«Règles QRadar SIEM», à la page 4
Les règles effectuent des tests sur les événements, les flux ou les infractions et si les conditions d'un test sont satisfaites, la règle génère une réponse.

Nettoyage du modèle SIM

Nettoyez le modèle SIM pour vous assurer que chaque hôte crée des infractions basées sur les règles les plus courantes, les serveurs reconnus et la structure hiérarchique du réseau.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans la barre d'outils, sélectionnez **Avancé** > **Nettoyer le modèle SIM**.
3. Cliquez sur l'option requise :

   `Nettoyage léger` pour que les infractions deviennent inactives.

   `Nettoyage léger` avec l'option facultative `Désactiver toutes les infractions` pour fermer toutes les infractions.

   `Nettoyage forcé` pour effacer toutes les entrées.
4. Cliquez sur **Voulez-vous vraiment réinitialiser le modèle de données ?**.
5. Cliquez sur **Continuer**.
6. Une fois le processus de réinitialisation SIM terminé, actualisez votre navigateur.

Résultats

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

Chapitre 3. Initiation à QRadar SIEM

Cette section décrit comment mettre en route IBM Security QRadar SIEM et rechercher des événements, flux et actifs. Elle explique également comment étudier les infractions et créer des rapports.

Par exemple, vous pouvez rechercher des informations à l'aide des recherches sauvegardées par défaut des onglets **Activité du journal** et **Activité réseau**. Vous pouvez également créer et sauvegarder 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.
- 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.
- Afficher tous les actifs étudiés ou rechercher des actifs précis dans votre environnement.
- Etudier les infractions, les adresses IP de source et de destination, les comportements de réseau ainsi que les anomalies de votre réseau.
- Modifier, créer, planifier et distribuer des rapports par défaut ou personnalisés.

Recherche d'événements

Vous pouvez rechercher tous les événements d'authentification reçus par QRadar SIEM au cours des 6 dernières heures.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
3. Dans le panneau Intervalle, définissez l'intervalle de la recherche d'événements :
   a. Cliquez sur **Récent**.
   b. Dans la liste **Récent**, sélectionnez **6 dernières heures**.
4. Dans le panneau Paramètres de recherche, définissez les paramètres de recherche :
   a. Dans la première liste, sélectionnez **Catégorie**.
   b. Dans la deuxième liste, sélectionnez **Est égal à**.
   c. Dans la liste **Catégorie de niveau supérieur**, sélectionnez **Authentification**.
   d. Dans la liste **Catégorie de niveau inférieur**, acceptez la valeur par défaut **Any**.
   e. Cliquez sur **Ajouter un filtre**.
5. Dans le panneau Définition de colonne, sélectionnez **Nom d'événement** dans la liste **Afficher**.
6. Cliquez sur **Rechercher**.

Sauvegarde des critères de recherche d'événements

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

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la barre d'outils, cliquez sur **Sauvegarder les critères**.
3. Dans la zone **Nom de la recherche**, entrez sur **Exemple de recherche 1**.
4. Dans le panneau Options d'intervalle, cliquez sur **Récent**.
5. Dans la liste **Récent**, sélectionnez **6 dernières heures**.
6. Cliquez sur **Inclure dans mes recherches rapides**.
7. Cliquez sur **Inclure dans mon tableau de bord**.

   Si l'option **Inclure dans mon tableau de bord** n'est pas affichée, cliquez sur **Rechercher** > **Editer la recherche** pour vérifier que vous avez sélectionné **Nom d'événement** dans le panneau Définition de colonne.
8. Cliquez sur **OK**.

Que faire ensuite

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 correspondant à une recherche d'intervalle de temps spécifique.

Procédure

1. Dans la barre de titre du graphique, cliquez sur l'icône **Configurer**.
2. Dans la liste **Valeur vers graphique**, sélectionnez **IP de destination (Nombre unique)**.
3. Dans la liste **Type de graphique**, sélectionnez **Série temporelle**.
4. Cliquez sur **Capture des données de séries temporelles**.
5. Cliquez sur **Sauvegarder**.
6. Cliquez sur **Mettre à jour les détails**.
7. Filtrez les résultats de votre recherche :
   a. Avec le bouton droit de la souris, cliquez sur l'événement à filtrer.
   b. Cliquez sur **Filter on Event Name is <Event Name>**.
8. Pour afficher la liste des événements groupée par nom d'utilisateur, sélectionnez **Nom d'utilisateur** dans la liste **Afficher**.
9. Vérifiez que votre recherche est visible sur le **Tableau de bord** :
   a. Cliquez sur l'onglet **Tableau de bord**.
   b. Cliquez sur l'icône **Nouveau tableau de bord**.
   c. Dans la zone **Nom**, tapez **Exemple de tableau de bord personnalisé**.
   d. Cliquez sur **OK**.
   e. Dans la liste **Ajouter un article**, sélectionnez **Activité du journal** > **Recherches d'événements** > **Exemple de recherche 1**.

Résultats

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

Recherche de flux

Cette section explique comment rechercher, surveiller et étudier les données de flux en temps réel.

Elle indique également comment effectuer des recherches avancées pour filtrer les flux affichés et comment afficher les informations de flux pour déterminer le trafic réseau et la façon dont il est communiqué.

Procédure

1. Cliquez sur l'onglet **Activité réseau**.
2. Dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
3. Dans la sous-fenêtre Intervalle, définissez l'intervalle de recherche des flux :
   a. Cliquez sur **Récent**.
   b. Dans la liste **Récent**, sélectionnez **6 dernières heures**.
4. Dans la sous-fenêtre Paramètres de recherche, définissez vos critères de recherche :
   a. Dans la première liste, sélectionnez **Direction du flux**.
   b. Dans la deuxième liste, sélectionnez **Est égal à**.
   c. Dans la troisième liste, sélectionnez **R2L**.
   d. Cliquez sur **Ajouter un filtre**.
5. Dans la liste **Afficher** du panneau Définition de colonne, sélectionnez **Application**.
6. Cliquez sur **Rechercher**.

Résultats

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

Sauvegarde des critères de recherche de flux

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

Procédure

1. Dans la barre d'outils de l'onglet **Activité réseau**, cliquez sur **Sauvegarder les critères**.
2. Dans la zone **Nom de la recherche**, entrez le nom **Exemple de recherche 2**.
3. Dans la liste **Récent**, sélectionnez **6 dernières heures**.
4. Cliquez sur **Inclure dans mon tableau de bord** et **Inclure dans mes recherches rapides**.
5. Cliquez sur **OK**.

Que faire ensuite

Créer 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 des flux sauvegardés.

Procédure

1. Dans la barre d'outils **Activité réseau**, sélectionnez **Recherches rapides** > **Exemple de recherche 2**.
2. Vérifiez que votre recherche est disponible dans le tableau de bord :
   a. Cliquez sur l'onglet **Tableau de bord**.
   b. Dans la liste **Afficher le tableau de bord**, sélectionnez **Exemple de tableau de bord personnalisé**.
   c. Dans la liste **Ajouter un article**, sélectionnez **Recherches de flux** > **Exemple de recherche 2**.
3. Configurez votre graphique de tableau de bord :
   a. Cliquez sur l'icône **Paramètres**.
   b. A l'aide des options de configuration, changez la valeur du graphique, le nombre d'objets affichés, le type de graphique ou l'intervalle affiché dans le graphique.
4. Pour étudier les flux actuellement affichés dans le graphique, cliquez sur **Afficher dans Activité réseau**.

Résultats

La page Activité réseau affiche les résultats correspondant aux paramètres de votre graphique de série temporelle. Pour plus d'informations sur les graphiques de série temporelle, voir le manuel *IBM Security QRadar SIEM - Guide d'utilisation*.

Recherche d'actifs

Lorsque vous accédez à l'onglet **Actifs**, la page Asset s'affiche avec tous les actifs détectés dans votre réseau. Pour affiner cette liste, vous pouvez configurer des paramètres de recherche pour afficher uniquement les profils d'actifs à rechercher.

Pourquoi et quand exécuter cette tâche

Utilisez la fonction de recherche pour rechercher des profils d'hôtes, des actifs et des informations d'identité. Les informations d'identité fournissent des détails supplémentaires tels que des informations sur les systèmes de noms de domaines, les connexions d'utilisateurs et les adresses MAC de votre réseau.

Par exemple :

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, cliquez sur **Profils d'actifs**.
3. Dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
4. Pour charger une recherche sauvegardée, procédez comme suit :

a. Facultatif : Dans la liste **Groupe**, sélectionnez le groupe de recherche d'actif que vous souhaitez afficher dans la liste **Recherches sauvegardées disponibles**.
b. Sélectionnez l'une des options suivantes :
   - Dans la zone **Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste**, saisissez le nom de la recherche à charger.
   - Dans la liste **Recherches sauvegardées disponibles**, sélectionnez la recherche sauvegardée que vous souhaitez charger.
c. Cliquez sur **Charger**.

5. Dans la sous-fenêtre Paramètres de recherche, définissez vos critères de recherche :
   a. Dans la première liste, sélectionnez le paramètre d'actif que vous souhaitez rechercher. Par exemple, **Nom d'hôte**, **Classification des risques de vulnérabilité** ou **Propriétaire technique**.
   b. Dans la deuxième liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche.
   c. Dans la zone **Entrée**, entrez les informations spécifiques relatives à votre paramètre de recherche.
   d. Cliquez sur **Ajouter un filtre**.
   e. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter aux critères de recherche.
6. Cliquez sur **Rechercher**.

Exemple

Une notification s'affiche indiquant que CVE ID: CVE-2010-000 est utilisé de manière active. Pour déterminer si les hôtes de votre déploiement sont vulnérables à cette utilisation, procédez comme suit :

1. Dans la liste des paramètres de recherche, sélectionnez **Référence externe de vulnérabilité**.
2. Sélectionnez **CVE**.
3. Entrez 2010-000 pour afficher une liste de tous les hôtes vulnérables à cet ID de CVE spécifique.

Pour plus d'informations, voir le site Web de la base de données de vulnérabilité de source ouverte (*http://osvdb.org/*) et la base de données de vulnérabilité nationale (*http://nvd.nist.gov/*).

Etude des infractions

Dans l'onglet **Infractions**, vous pouvez étudier les infractions, les adresses IP de source et de destination, 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.

Affichage des infractions

Cette section explique comment étudier les infractions se produisant dans votre réseau.

Vous pouvez par exemple étudier les infractions, les adresses IP de source et de destination, les comportements de réseau et les anomalies de votre réseau.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Cliquez deux fois sur l'infraction à étudier.
3. Dans la barre d'outils, sélectionnez **Afficher** > **Destinations**.

   Vous pouvez étudier chaque destination afin de déterminer si elle n'est pas fiable ou si elle présente un comportement suspect.
4. Dans la barre des outils, cliquez sur **Evénements**.

Résultats

La fenêtre List of Events affiche tous les événements associés à l'infraction. Vous pouvez rechercher, trier et filtrer des critères de recherche.

Exemple : activation des modèles de rapport PCI

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

Dans cette tâche d'initiation, vous allez activer les modèles de rapports PCI (Payment Card Industry).

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Décochez la case **Masquer les rapports inactifs**.
3. Dans la liste **Groupe**, sélectionnez **Conformité** > **PCI**.
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 maintenant la touche Maj enfoncée, tout en cliquant sur le dernier rapport de la liste.
5. Dans la liste **Actions**, sélectionnez **Basculer la planification**.
6. Accédez aux rapports générés :
   a. Dans la colonne **Rapports générés**, sélectionnez l'horodatage du rapport que vous souhaitez afficher.
   b. Dans la colonne **Format**, cliquez sur l'icône du format de rapport que vous souhaitez afficher.

Exemple : création d'un rapport personnalisé à partir d'une recherche sauvegardée

Vous pouvez créer un rapport en important une recherche ou en créant des critères personnalisés.

Pourquoi et quand exécuter cette tâche

Dans cette tâche d'initiation, vous pouvez créer un rapport à partir des recherches d'événements ou de flux créées dans la section «Recherche d'événements», à la page 17.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Dans la liste **Actions**, sélectionnez **Créer**.
3. Cliquez sur **Suivant**.
4. Configurez la planification de rapport.
   a. Sélectionnez l'option **Quotidienne**.
   b. Sélectionnez les options **Lundi, Mardi, Mercredi, Jeudi et Vendredi**.
   c. A l'aide des listes, sélectionnez **8:00** et **AM**.
   d. Vérifiez que l'option **Oui - Générer manuellement le rapport** est sélectionnée.
   e. Cliquez sur **Suivant**.
5. Configurez la présentation de rapport :
   a. Dans la liste **Orientation**, sélectionnez **Paysage**.
   b. Sélectionnez la présentation avec deux conteneurs de graphiques.
   c. Cliquez sur **Suivant**.
6. Dans la zone **Titre du rapport**, tapez **Exemple de rapport**.
7. Configurez le conteneur de graphique supérieur :
   a. Dans la liste **Type de graphique**, sélectionnez **Evénements/Journaux**.
   b. Dans la zone **Titre du graphique**, saisissez **Exemple de recherche d'événement**.
   c. Dans la liste **Limiter Evénements/Journaux aux premiers**, sélectionnez **10**.
   d. Dans la liste **Type de graphique**, sélectionnez **Barres empilées**.
   e. Cliquez sur **Toutes les données de la journée précédente (24 heures)**.
   f. Dans la liste **Baser ce rapport d'événement sur**, sélectionnez **Exemple de recherche 1**.

      Le reste des paramètres est automatiquement renseigné à l'aide des paramètres de la recherche sauvegardée Exemple de recherche 1.
   g. Cliquez sur **Sauvegarder les détails du conteneur**.
8. Configurez le conteneur de graphique inférieur :
   a. Dans la liste **Type de graphique**, sélectionnez **Flux**.
   b. Dans la zone **Titre du graphique**, saisissez **Exemple de recherche de flux**.
   c. Dans la liste **Limiter Flux aux premiers**, sélectionnez **10**.
   d. Dans la liste **Type de graphique**, sélectionnez **Barres empilées**.
   e. Cliquez sur **Toutes les données de la journée précédente (24 heures)**.
   f. Dans la liste **Recherches sauvegardées disponibles**, sélectionnez **Exemple de recherche 2**.

      Le reste des paramètres est automatiquement renseigné à l'aide des paramètres de la recherche sauvegardée Exemple de recherche 2.
   g. Cliquez sur **Sauvegarder les détails du conteneur**.
9. Cliquez sur **Suivant**.
10. Cliquez sur **Suivant**.
11. Sélectionnez le format du rapport :
    a. Cliquez sur les cases **PDF and HTML**.
    b. Cliquez sur **Suivant**.
12. Sélectionnez les canaux de distribution du rapport :
    a. Cliquez sur **Console de rapports**.

b. Cliquez sur **E-mail**.
c. Dans la zone **Entrez les adresse(s) e-mails de destination du rapport**, saisissez votre adresse électronique.
d. Cliquez sur **Inclure le rapport sous forme de pièce jointe**.
e. Cliquez sur **Suivant**.

13. Entrez les derniers détails de l'assistant de rapport :
    a. Dans la zone **Description du rapport**, entrez une description du modèle.
    b. Cliquez sur **Oui - Exécuter ce rapport à la fin de l'assistant**.
    c. Cliquez sur **Terminer**.
14. A l'aide de la zone de liste de la colonne **Rapports générés**, sélectionnez l'horodatage de votre rapport.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

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

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues 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.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT 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 implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. 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 conditions 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 de l'ICA, des Conditions internationales d'utilisation des logiciels IBM 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 tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées d'International Business Machines Corporation aux États-Unis et/ou dans d'autres pays. Si ces marques et d'autres marques d'IBM sont accompagnées d'un symbole de marque (® ou ™), ces symboles signalent des marques d'IBM aux Etats-Unis à la date de publication de ce document. Ces marques peuvent également être des marques ou des marques déposées dans d'autres pays. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Remarques sur les règles de confidentialité

Les produits IBM Software, notamment les logiciels sous forme de services ("Offres logicielles"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations d'utilisation en vue d'améliorer l'expérience de l'utilisateur final, d'ajuster les interactions avec l'utilisateur final ou à d'autres fins. Dans de nombreux cas, aucune information identifiant la personne n'est collectée par les offres logicielles. Certaines de nos Offres logicielles vous permettent de collecter des informations identifiant la personne. Si cette Offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des informations spécifiques sur l'utilisation de cookies par cette offre sont énoncées ci-dessous.

Selon les configurations déployées, cette Offre logicielle peut utiliser des cookies de session qui collectent chaque ID de session à des fins de gestion de la session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres personnes via des cookies et d'autres technologies, vous devez vous renseigner sur

l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

Pour plus d'informations sur l'utilisation de diverses technologies, notamment de cookies, à ces fins, reportez-vous aux Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et à la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site http://www.ibm.com/privacy/details/fr/fr, ainsi qu'à la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site http://www.ibm.com/software/info/product-privacy (en anglais).

Glossaire

Ce glossaire contient les termes et définitions du logiciel et des produits IBM Security QRadar SIEM.

Les références croisées suivantes sont utilisées :

- *Voir* vous renvoie d'un terme moins utilisé au terme généralement utilisé ou d'une abréviation à la forme développée.
- *Voir également* vous renvoie à un terme connexe ou à un antonyme.

Pour tout autre terme et définition, veuillez vous référer au site Web de terminologie IBM (ouvre une nouvelle fenêtre).

A

accumulateur
Registre dans lequel une opérande d'une opération peut être stockée et remplacée ensuite par le résultat de cette opération.

actif Objet gérable déployé ou conçu pour être déployé dans un environnement opérationnel.

adresse IP virtuelle du cluster
Adresse IP partagée entre l'hôte principal ou secondaire et le cluster haute disponibilité.

ampleur
Mesure de l'importance relative d'une infraction. L'ampleur est une valeur pondérée calculée à partir des mesures de pertinence, de gravité et de crédibilité.

analyse immédiate
Analyse de vulnérabilité qui génère des données de rapport à partir de résultats d'analyse d'après le nom de session.

anomalie
Ecart par rapport au comportement attendu du réseau.

ARP Voir protocole de résolution d'adresse.

ASN Voir numéro de système autonome.

C

capture de contenu
Processus permettant de capturer une quantité configurable de contenus et de stocker ensuite les données dans un journal de flux.

chiffrement
Dans le cadre de la sécurité informatique, processus de conversion de données dans une forme inintelligible, de sorte que les données d'origine ne puissent pas être obtenues ou puisse l'être uniquement via un processus de déchiffrement.

cible hors site
Périphérique situé en dehors du site principal recevant des flux d'événements ou de données d'un collecteur d'événements.

CIDR Voir routage CIDR.

client Programme logiciel ou ordinateur demandant des services à un serveur.

cluster à haute disponibilité
Une configuration haute disponibilité se compose d'un serveur principal et d'un serveur secondaire.

code d'authentification de message basé sur le hachage (HMAC)
Code cryptographique qui utilise une fonction de hachage chiffrée et une clé secrète.

comportement
Effets observables d'une opération ou d'un événement, y compris de ses résultats.

console
Clavier-écran à partir duquel un opérateur peut contrôler et observer le fonctionnement du système.

contexte d'hôte
Service surveillant les composants pour s'assurer que chaque composant fonctionne comme prévu.

couche réseau
Dans une architecture OSI, couche fournissant des services pour établir un chemin d'accès entre les systèmes ouverts avec une qualité de service prévisible.

crédibilité
Classement numérique compris entre 0 et 10, utilisé pour déterminer l'intégrité d'un événement ou la présence d'une infraction. La crédibilité augmente lorsque plusieurs sources signalent le même événement ou la même violation.

CVSS Voir système de notation de vulnérabilité commune.

D

destination d'acheminement
Système d'un ou plusieurs fournisseurs recevant des données brutes et normalisées de sources de journal et de sources de flux.

dispositif d'analyse externe
Machine qui est connectée au réseau pour la collecte de données de vulnérabilité concernant des actifs du réseau.

distant à distant (R2R)
Trafic externe entre un réseau distant et un autre réseau distant.

distant à local (R2L)
Trafic externe entre un réseau distant et un réseau local.

DNS Voir système de noms de domaine.

données d'identification
Ensemble d'informations accordant certains droits d'accès à un utilisateur ou à un processus.

données utiles
Données d'application contenues dans un flux IP, excluant l'en-tête et les informations administratives.

DSM Voir module de support de périphérique.

Dynamic Host Configuration Protocol (DHCP)
Protocole de communication utilisé pour gérer les informations de configuration de façon centralisée. Par exemple, DHCP affecte automatiquement des adresses IP aux ordinateurs d'un réseau.

E

ensemble de référence
liste d'éléments uniques dérivés d'événements ou de flux sur un réseau (liste d'adresses IP ou liste de noms d'utilisateur, par exemple).

extension de source de journal
Fichier XML qui inclut l'ensemble des schémas d'expression régulière requis pour identifier et catégoriser les événements de contenu d'événement.

F

faux positif
Résultat de test classé comme positif (indiquant que le site est vulnérable aux attaques) et que l'utilisateur décide de classer comme négatif (il ne s'agit pas d'une vulnérabilité).

feuille Dans une arborescence, entrée ou noeud ne possédant pas d'enfant.

fichier de clés
Dans la sécurité informatique, fichier contenant les clés publiques, les clés privés, les ports sécurisés et les certificats.

flux Transmission de données unique passant par un lien lors d'une conversation.

flux double
Plusieurs instances de la même transmission de données provenant de sources de flux distinctes.

fournisseur d'accès à Internet (FAI)
Organisation fournissant un accès à Internet.

G

gravité
Mesure de la menace relative qu'une source représente pour une destination.

H

HA Voir haute disponibilité.

haute disponibilité (HA)
Se dit d'un système en cluster reconfiguré en cas de défaillance d'un noeud ou d'un démon, de telle sorte que la charge puisse être redistribuée entre les autres noeuds du cluster.

HMAC
Voir code d'authentification de message basé sur le hachage.

hôte à haute disponibilité principal
Ordinateur principal connecté au cluster haute disponibilité.

hôte à haute disponibilité secondaire
Ordinateur de secours connecté au cluster haute disponibilité. L'hôte à haute disponibilité secondaire assume la responsabilité de l'hôte à haute disponibilité principal en cas de défaillance de ce dernier.

I

ICMP Voir protocole de message de gestion inter-réseau.

identité
Collection d'attributs provenant d'une source de données et représentant une personne, une organisation, un lieu ou un élément.

IDS Voir système de détection d'intrusion.

interconnexion de systèmes ouverts
Interconnexion de systèmes ouverts conforme aux normes ISO (International Organization for Standardization) pour l'échange d'informations.

intervalle de coalescence
Fréquence à laquelle les événements sont regroupés. Le regroupement d'événements se produit à des intervalles de 10 secondes et commence avec le premier événement qui ne correspond à aucun événement de coalescence en cours. A l'intérieur de l'intervalle de coalescence, les trois premiers événements correspondants sont regroupés et envoyés au processeur d'événement.

intervalle de rapport
Intervalle de temps configurable au terme duquel le processeur d'événement doit envoyer la totalité des événements capturés et des données de flux à la console.

IP Voir protocole Internet.

IPS Voir système de prévention contre les intrusions.

ISP Voir fournisseur d'accès à Internet.

J

journal de flux
Collection d'enregistrements de flux.

L

LAN Voir réseau local.

LDAP Voir protocole LDAP (Lightweight Directory Access Protocol).

L2L Voir local à local.

local à distant (L2R)
Concerne le trafic interne d'un réseau local à un autre réseau distant.

local à local (L2L)
Concerne le trafic interne d'un réseau local à un autre réseau local.

L2R Voir local à distant.

M

magasin de clés certifiées
Fichier de la base de données de clés contenant les clés publiques d'une entité de confiance.

magistrat
Composant interne analysant le trafic réseau et les événements de sécurité à l'aide de règles personnalisées définies.

mappe de références
enregistrement de données d'un mappage direct d'une clé à une valeur (un nom d'utilisateur vers un ID global, par exemple).

mappe de références de mappes
enregistrement de données de deux clés mappées à un grand nombre de valeurs (mappage, par exemple, du nombre d'octets total d'une application vers un IP source.

mappe de références d'ensembles
enregistrement de données d'une clé mappée à un grand nombre de valeurs (mappage, par exemple, d'une liste d'utilisateurs privilégiés à un hôte).

mappe QID
Taxonomie identifiant chaque événement unique et mappant les événements à des catégories de bas niveau et de haut

niveau afin de déterminer la façon dont un événement doit être corrélé et organisé.

masque de sous-réseau
Pour la mise en sous-réseau Internet, masque de 32 bits permettant d'identifier les bits d'adresse de sous-réseau de la partie hôte d'une adresse IP.

minuteur d'actualisation
Périphérique interne déclenché manuellement ou automatiquement à des intervalles temporisés, mettant à jour les données d'activité réseau en cours.

module de support de périphérique (DSM)
Fichier de configuration analysant les événements reçus de plusieurs sources de journal et les convertissant à un format de taxonomie standard affichable comme sortie.

multi-diffusion IP
Transmission d'un datagramme IP (Internet Protocol) à une série de systèmes constituant un groupe de multi-diffusion unique.

N

NAT Voir Network Address Translation.

NDQC
Voir nom de domaine qualifié complet.

NetFlow
Protocole de réseau Cisco surveillant les données de flux du trafic réseau. Les données NetFlow contiennent des informations sur le client et le serveur, les ports utilisés et le nombre d'octets et de paquets circulant via les commutateurs et routeurs connectés à un réseau. Les données sont envoyées aux connecteurs NetFlow où l'analyse des données se produit.

Network Address Translation (NAT)
Dans un pare-feu, conversion d'adresses de protocole Internet (IP) sécurisées à des adresses enregistrées externes. Ceci permet la communication avec des réseaux externes mais masque les adresses IP utilisées à l'intérieur du pare-feu.

noeud final
Adresse d'une interface de programme d'application ou d'un service dans un environnement. Une interface de programme d'application expose un noeud final et appelle en même temps les noeuds finaux pour d'autres services.

nom de domaine qualifié complet (NDQC)
Dans les communications Internet, le nom d'un système hôte qui inclut tous les sous-noms du nom de domaine. rchland.vnet.ibm.com est un exemple de nom de domaine complet.

nom de réseau qualifié complet (NDQC)
Dans une hiérarchie de réseau, le nom d'un objet comprenant tous les services. CompanyA.Department.Marketing est un exemple de nom de réseau habilité complet.

NRQC
Voir nom de réseau qualifié complet.

numéro de système autonome (ASN)
Dans TCP/IP, numéro affecté à un système autonome par la même autorité centrale que celle qui affecte les adresses IP. Le numéro de système autonome permet aux algorithmes de routage automatique de distinguer les systèmes autonomes.

O

objet Noeud terminal de la base de données
Objet de terminal ou noeud dans une hiérarchie de base de données.

objet réseau
Composant d'une hiérarchie réseau.

Open Source Vulnerability Database (OSVDB)
Créée par et pour la communauté de sécurité réseau, cette base de données open source fournit des informations techniques sur les vulnérabilités de la sécurité réseau.

ordre d'analyse syntaxique
Définition de source de journal dans laquelle l'utilisateur peut définir l'ordre d'importance pour les sources de journal qui partagent une adresse IP ou un nom d'hôte communs.

OSI Voir interconnexion de systèmes ouverts.

OSVDB
Voir Open Source Vulnerability Database.

P

partage administratif
Ressource réseau qui est masquée aux utilisateurs ne disposant pas de privilèges d'administration. Les partages administratifs donne accès aux administrateurs à toutes les ressources sur un système réseau.

passerelle
Périphérique ou programme permettant de connecter des réseaux ou des systèmes à des architectures réseau différentes.

pertinence
Mesure de l'impact relatif d'un événement, d'une catégorie ou d'une infraction sur le réseau.

point de données
Valeur calculée d'une mesure à un moment donné.

pondération du réseau
Valeur numérique appliquée à chaque réseau qui témoigne de l'importance du réseau. La pondération du réseau est définie par l'utilisateur.

protocole
Ensemble de règles gérant les communications et le transfert de données entre plusieurs unités ou systèmes, dans un réseau de communication.

protocole de message de gestion inter-réseau (ICMP)
Protocole Internet utilisé par une passerelle pour communiquer avec un hôte source, par exemple, pour signaler une erreur dans un datagramme.

protocole de résolution d'adresse (ARP)
Protocole qui établit une correspondance dynamique entre une adresse IP et une adresse d'adaptateur de réseau dans un réseau local.

protocole DHCP
Voir Dynamic Host Configuration Protocol.

protocole Internet (IP)
Protocole acheminant les données via un réseau ou des réseaux interconnectés. Ce protocole joue le rôle d'intermédiaire entre les couches de protocole de niveau supérieur et le réseau physique. Voir également protocole TCP.

protocole LDAP (Lightweight Directory Access Protocol)
Protocole ouvert utilisant TCP/IP pour fournir l'accès aux annuaires qui prennent en charge un modèle X.500 et pour lequel les ressources exigées par le protocole X.500 DAP (Directory Access Protocol) plus complexe ne sont pas requises. Par exemple, le protocole LDAP peut être utilisé pour localiser des personnes, des organisations et d'autres ressources dans un annuaire Internet ou Intranet.

R

rapport
Dans la gestion des requêtes, données dont la mise en forme résulte de l'exécution d'une requête et de l'application d'un formulaire particulier aux enregistrements renvoyés par cette requête.

recon Voir reconnaissance.

reconnaissance (recon)
Méthode par laquelle les informations appartenant à l'identité des ressources réseau sont collectées. L'analyse réseau et d'autres techniques sont utilisées pour compiler une liste d'événements de ressource réseau auxquels un niveau de sécurité est ensuite affecté.

redirection du protocole de résolution d'adresse
Méthode du protocole ARP permettant de notifier l'hôte en cas de problème sur un réseau.

règle Ensemble d'instructions conditionnelles permettant à des systèmes informatiques d'identifier des relations et d'exécuter les réponses automatisées correspondantes.

règle de routage
Condition qui, lorsque ses critères sont satisfaits par les données d'événement, entraîne une collection de conditions et le routage conséquent.

réseau local
Réseau reliant plusieurs périphériques dans une zone limitée (telle qu'un bâtiment ou un campus) et pouvant être connecté à un réseau plus grand.

R2L Voir local à local.

routage CIDR
Méthode d'ajout d'adresses IP (Internet

Protocol) de classe C. Les adresses sont fournies aux fournisseurs de services Internet (ISP) pour une utilisation par leurs clients. Les adresses CIDR réduisent la taille des tables de routage et augmentent le nombre d'adresses IP disponibles au sein des organisations.

R2R Voir distant à distant.

S

scanner
Programme de sécurité automatisée qui recherche les vulnérabilités logicielles au sein d'applications Web.

serveur whois
Serveur utilisé pour récupérer les informations sur des ressources Internet enregistrées, telles que les allocations de noms de domaine et adresses IP.

signature d'application
Ensemble unique de caractéristiques dérivées de l'examen de contenus de paquets puis utilisées pour identifier une application spécifique.

Simple Network Management Protocol (SNMP)
Ensemble de protocoles permettant de surveiller les systèmes et les périphériques dans des réseaux complexes. Les informations sur les périphériques gérés sont définies et stockées dans une base d'informations de gestion.

SNMP
Voir Simple Network Management Protocol.

SOAP Protocole simple reposant sur XML pour l'échange d'informations dans un environnement réparti décentralisé. Le protocole SOAP peut être utilisé pour rechercher et renvoyer des informations et pour appeler des services via Internet.

source de journal
Equipement de sécurité ou équipement réseau duquel un journal d'événement provient.

source hors site
Périphérique situé en dehors du site principal renvoyant les données normalisées à un collecteur d'événements.

sources de flux
Origine du flux capturé. Une source de flux est classée comme interne lorsque le flux provient d'un matériel installé sur un hôte géré et comme externe lorsque le flux est envoyé à un collecteur de flux.

sous-recherche
Fonction permettant d'effectuer une requête de recherche sur un ensemble de résultats de recherche terminés.

sous-réseau
Réseau divisé en plusieurs sous-groupes indépendants de plus petite taille, connectés entre eux.

structure hiérarchique du réseau
Type de conteneur représentant une collection hiérarchique d'objets réseau.

subnet
Voir sous-réseau.

super-flux
Flux unique composé de plusieurs flux aux propriétés similaires permettant d'améliorer la capacité de traitement en réduisant les contraintes de stockage.

système actif
Dans un cluster haute disponibilité, système ayant tous ses services en cours d'exécution.

système de détection d'intrusion (IDS)
Logiciel détectant les tentatives d'attaques ou attaques réussies sur les ressources surveillées d'un réseau ou d'un système hôte.

système de noms de domaine (DNS)
Système de base de données répartie qui mappe des noms de domaine à des adresses IP.

système de notation de vulnérabilité commune (CVSS)
Système d'évaluation permettant de mesurer la gravité d'une vulnérabilité.

système de prévention contre les intrusions (IPS) Système essayant de refuser les activités potentiellement malveillantes. Les mécanismes de refus peuvent impliquer le filtrage, le suivi ou la définition de limites de débit.

système de secours
Système s'activant automatiquement en cas de défaillance du système actif. Si la

réplication de disque est activée, il réplique les données du système actif.

T

table de référence
tableau dans lequel l'enregistrement de données mappe les clés qui ont un type affecté à d'autres clés, qui sont ensuite mappées à une valeur unique.

TCP Voir Transmission Control Protocol.

Transmission Control Protocol (TCP)
Protocole de communication utilisé sur Internet et dans tout réseau respectant les normes IETF (Internet Engineering Task Force) relatives au protocole inter-réseau. TCP constitue un protocole hôte à hôte fiable dans les réseaux à commutation de paquets et dans les systèmes interconnectés de ces réseaux. Voir également Protocole Internet.

V

violation
Acte visant à détourner ou contourner les règles de l'entreprise.

violation
Message envoyé ou événement généré en réponse à une condition contrôlée. Par exemple, une infraction indiquera si une règle a été violée ou si le réseau se trouve en état d'attaque.

vue système
Représentation visuelle de l'hôte principal et de l'hôte géré composant un système.

vulnérabilité
Exposition de la sécurité dans un système d'exploitation, un logiciel système ou un composant de logiciel d'application.

Index