IBM Security QRadar Risk Manager
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 33.

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 d'IBM Security QRadar Risk Manager

Ces informations sont destinées à un usage avec IBM® Security QRadar Risk Manager. QRadar Risk Manager est un dispositif destiné à la surveillance des configurations d'unité, qui simule des changements apportés à votre environnement réseau et hiérarchise les risques et vulnérabilités sur votre réseau. -

Utilisateurs concernés

Ce guide est destiné aux administrateurs de réseau responsables de l'installation et de la configuration de systèmes QRadar Risk Manager sur votre réseau.

Documentation technique

Pour rechercher la documentation produit IBM Security QRadar sur le Web, y compris toute la documentation traduite, accédez à IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Pour savoir comment accéder à plus de documentation technique dans la bibliothèque produit QRadar, voir Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

Pour contacter le service clients, voir Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

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 réglementaire. 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. Mise en route d'IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager est un dispositif installé séparément. Utilisez QRadar Risk Monitor pour surveiller des configurations d'unité, en simulant des changements dans votre environnement réseau, et pour hiérarchiser les risques et vulnérabilités de votre réseau.

QRadar Risk Manager est accessible depuis l'onglet **Risques** de la console IBM Security QRadar SIEM.

QRadar Risk Manager améliore QRadar SIEM en fournissant à l'administrateur des outils pour exécuter les tâches suivantes :

- Centralisation de la gestion des risques.
- Utilisation d'une topologie pour visualiser votre réseau.
- Configuration et surveillance des unités réseau.
- Visualisation des connexions entre les unités réseau.
- Recherche parmi les règles de pare-feu.
- Visualisation des règles existantes et comptage des événements pour les règles déclenchées.
- Recherche d'unités et de chemins pour vos unités réseau.
- Surveillance et audit de votre réseau afin d'en garantir la conformité.
- Définition, planification et exécution de simulations d'utilisation sur votre réseau.
- Recherche des vulnérabilités.

La gestion centralisée des risques et la mise en conformité pour une intelligence accrue des informations peut impliquer la coopération d'un grand nombre d'équipes en interne. Doté d'un dispositif Risk Management supplémentaire, SIEM nouvelle génération permet de réduire le nombre d'étapes nécessaires comparativement aux produits SIEM première génération. Nous fournissons une topologie de réseau et une évaluation des risques pour des actifs gérés dans QRadar SIEM.

Lors du processus d'évaluation, vous consolidez les informations de votre système, de sécurité, d'analyse des risques et du réseau via l'agrégation et la corrélation, et disposez ainsi d'une visibilité totale de votre environnement réseau. Vous définissez également un portail d'accès à votre environnement, lequel offre une visibilité et une efficacité que vous ne pouvez pas égaler en utilisant des processus manuels et autres technologies produit ponctuelles.

Chapitre 2. Déploiement d'IBM Security QRadar Risk Manager

Votre dispositif QRadar Risk Manager est installé avec la dernière version du logiciel QRadar Risk Manager.

Vous devez installer le dispositif d'évaluation IBM Security QRadar Risk Manager. Le logiciel doit être activé et vous devez affecter une adresse IP au dispositif QRadar Risk Manager.

Si vous avez besoin d'une assistance pour activer le logiciel et affecter une adresse IP, prenez contact avec le support clients.

Le dispositif est prêt à accepter les informations provenant de vos unités réseau.

Pour plus d'informations sur l'utilisation d'IBM Security QRadar Risk Manager, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Pour déployer QRadar Risk Manager dans votre environnement , vous devez :

1. vous assurer que la version la plus récente d'IBM Security QRadar SIEM est installée ;
2. vérifier que toutes les conditions de préinstallation sont satisfaites ;
3. configurer et mettre sous tension votre dispositif QRadar Risk Manager ;
4. installer le plug-in QRadar Risk Manager sur votre console QRadar SIEM ;
5. établir la communication entre QRadar SIEM et le dispositif QRadar Risk Manager ;
6. définir des rôles utilisateur pour vos utilisateurs QRadar Risk Manager.

Avant de procéder à l'installation

Vous devez exécuter le processus d'installation pour une console IBM Security QRadar SIEM avant d'installer IBM Security QRadar Risk Manager. Il est recommandé d'installer QRadar SIEM et QRadar Risk Manager sur le même commutateur réseau.

Passez en revue les informations suivantes :

- Configuration de l'accès aux ports sur les pare-feu
- Identification des paramètres réseau
- Fonctions non prises en charge dans QRadar Risk Manager
- Navigateurs Web pris en charge

Avant d'installer le dispositif d'évaluation IBM Security QRadar Risk Manager, assurez-vous de disposer :

- de suffisamment d'espace pour un dispositif à deux unités
- de rails de guidage et d'étagères montés

Vous avez la possibilité d'utiliser un clavier USB et un moniteur VGA standard pour accéder à la console QRadar SIEM.

Configuration de l'accès aux ports sur les pare-feu

Les pare-feu entre la console IBM Security QRadar et IBM Security QRadar Risk Manager doivent autoriser le trafic sur certains ports.

Assurez-vous que tout pare-feu situé entre la console QRadar SIEM et QRadar Risk Manager autorise le trafic sur les ports suivants :

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (horloge)

Identification des paramètres réseau

Vous devez collecter des informations sur vos paramètres réseau avant de lancer le processus d'installation.

Collectez les informations suivantes pour vos paramètres réseau :

- Nom d'hôte
- Adresse IP
- Adresse du masque de réseau
- Masque de sous-réseau
- Adresse de la passerelle par défaut
- Adresse serveur du système de noms de domaine (DNS) principal
- Adresse serveur du système DNS secondaire (facultatif)
- Adresse IP publique pour les réseaux utilisant un nom de serveur de messagerie NAT
- Nom du serveur de messagerie
- Nom du serveur NTP (console uniquement) ou nom du serveur d'horloge

Fonctions non prises en charge dans QRadar Risk Manager

Il est important de connaître les fonctions qui ne sont pas prises en charge par IBM Security QRadar Risk Manager.

Les fonctions suivantes ne sont pas prises en charge dans QRadar Risk Manager :

- Haute disponibilité (HA)
- Routage dynamique pour les protocoles BGP (Border Gateway Protocol), OSPF (Open Shortest Path First) ou RIP (protocole de routage).
- IPv6
- Masques de réseau non contigus
- Routes à équilibrage de charge
- Mappes de référence
- Stockage et retransmission

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 invité à fournir vos nom d'utilisateur et 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

Activation des modes Document et Navigateur dans Internet Explorer

Si vous utilisez Microsoft Internet Explorer pour accéder aux produits IBM Security QRadar, vous devez activer les modes Document et Navigateur.

Procédure

1. Dans votre navigateur web Internet Explorer, appuyez sur la touche F12 pour ouvrir la fenêtre Outils de développement.
2. Cliquez sur **Mode Navigateur** et sélectionnez la version de votre navigateur web.
3. Cliquez sur **Mode Document**.
   - Pour Internet Explorer 9.0, sélectionnez **Normes d'Internet Explorer 9**
   - Pour Internet Explorer 8.0, sélectionnez **Normes d'Internet Explorer 8**

Accès à l'interface utilisateur d'IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager utilise des informations de connexion par défaut pour l'URL, le nom d'utilisateur et le mot de passe.

Vous accédez à IBM Security QRadar Risk Manager via la console QRadar. Utilisez les informations du tableau suivant lorsque vous vous connectez à votre console IBM Security QRadar.

Tableau 2. Informations de connexion par défaut pour QRadar Risk Manager

Informations de connexion	Valeur par défaut
URL	https://<adresse IP>, où <adresse IP> est l'adresse IP de la console QRadar.
Nom d'utilisateur	admin
Mot de passe	Mot de passe affecté à QRadar Risk Manager lors du processus d'installation.
Clé de licence	Une clé de licence par défaut fournit l'accès au système pour 5 semaines.

Configuration d'un dispositif QRadar Risk Manager

Vous devez connecter l'interface de gestion et vous assurer que les branchements d'alimentation sont correctement effectués pour le dispositif QRadar Risk Manager.

Avant de commencer

Lire, maîtriser et obtenir les prérequis

Pourquoi et quand exécuter cette tâche

Le dispositif d'évaluation IBM Security QRadar Risk Manager est un serveur monté en armoire à deux unités. Les rails de guidage et les étagères ne sont pas fournis avec le matériel d'évaluation.

Le dispositif QRadar Risk Manager inclut quatre interfaces réseau. Pour cette évaluation, utilisez comme interface de gestion l'interface réseau libellée ETH0. Les autres interfaces sont des interfaces de surveillance. Toutes les interfaces se trouvent sur le panneau arrière du dispositif QRadar Risk Manager.

Le bouton d'alimentation est situé sur le panneau frontal.

Procédure

1. Connectez l'interface réseau de gestion au port libellé ETH0.
2. Vérifiez que les connexions d'alimentation dédiées sont branchées à l'arrière du dispositif.
3. Facultatif. Pour accéder à la console QRadar SIEM, connectez le clavier USB et un moniteur VGA standard.
4. Si le dispositif est doté d'un volet avant, retirez celui-ci en appuyant sur les taquets situés de chaque côté et tirez sur le volet pour l'ôter du dispositif.
5. Appuyez sur le bouton d'alimentation à l'avant pour mettre le dispositif sous tension.

Résultats

Le dispositif débute le processus d'amorçage.

Ajout de QRadar Risk Manager à QRadar console

Vous devez ajouter IBM Security QRadar Risk Manager en tant qu'hôte géré à la console IBM Security QRadar.

Avant de commencer

Si vous souhaitez activer la compression, la version minimale pour chaque hôte géré doit être QRadar console 7.1 ou QRadar Risk Manager 7.1.

Pour ajouter un hôte géré sans conversion NAT à votre déploiement lorsque la console a subi une conversion NAT, vous devez faire passer la console QRadar en hôte avec conversion NAT. Vous devez changer la console avant d'ajouter l'hôte géré à votre déploiement. Pour plus d'informations, voir le *guide d'administration d'IBM Security QRadar SIEM*.

Procédure

1. Ouvrez votre navigateur Web.
2. Entrez l'URL `https://<Adresse IP>`, où <Adresse IP> correspond à l'adresse IP de la console QRadar.
3. Entrez votre nom d'utilisateur et votre mot de passe.
4. Dans l'onglet **Admin**, cliquez sur l'**éditeur de déploiement**.
5. Depuis le menu, sélectionnez **Actions**, puis **Ajouter un hôte géré**.
6. Cliquez sur **Suivant**.
7. Entrez des valeurs pour les paramètres suivants :

Option	Description
Enter the IP of the server or appliance to add	Adresse IP de QRadar Risk Manager.
Enter the root password of the host	Mot de passe root de l'hôte.
Confirm the root password of the host	Confirmation de votre mot de passe.
Host is NATed	Pour activer la conversion d'adresses réseau (NAT) pour un hôte géré, le réseau converti doit utiliser la conversion NAT statique. Pour plus d'informations, voir le *guide d'administration d'IBM Security QRadar SIEM*.
Enable Encryption	Crée un tunnel de chiffrement SSH pour l'hôte. Pour activer le chiffrement entre deux hôtes gérés, chacun de ces hôtes doit exécuter la console QRadar 7.1 ou QRadar Risk Manager 7.1.
Enable Compression	Active la compression de données entre deux hôtes gérés.

8. Sélectionnez l'une des options suivantes :
   - Si vous avez cochez la case **Host is NATed**, vous devez indiquer des valeurs pour les paramètres NAT.

Option	Description
Enter public IP of the server or appliance to add	Adresse IP publique de l'hôte géré. L'hôte géré utilise cette adresse IP pour communiquer avec d'autres hôtes gérés sur différents réseaux utilisant la conversion NAT.
Select NATed network	Réseau que cet hôte géré doit utiliser. Si l'hôte géré se trouve sur le même sous-réseau que la console QRadar, sélectionnez la console du réseau avec conversion NAT. Si l'hôte géré ne se trouve pas sur le même sous-réseau que la console QRadar, sélectionnez l'hôte géré du réseau avec conversion NAT.

   - Si vous n'avez pas coché la case **Host is NATed**, cliquez sur **Suivant**.
9. Cliquez sur **Terminer**. L'exécution de ce processus peut prendre plusieurs minutes. Si votre déploiement inclut des modifications, vous devez déployer tous ces changements.

10. Cliquez sur **Déployer**.

Que faire ensuite

Videz le cache de votre navigateur Web puis connectez-vous à la console QRadar. L'onglet **Risques** est à présent disponible.

Etablissement des communications

Vous devez établir la communication entre votre dispositif QRadar Risk Manager et votre console QRadar SIEM avant de configurer QRadar Risk Manager.

Pourquoi et quand exécuter cette tâche

L'exécution du processus d'établissement de communications peut prendre plusieurs minutes. Si vous changez l'adresse IP de votre dispositif QRadar Risk Manager, ou si vous avez besoin de connecter QRadar Risk Manager à une autre console QRadar SIEM, vous pouvez utiliser les **paramètres du gestionnaire de risques** de l'onglet **Admin** de QRadar SIEM.

Procédure

1. Ouvrez votre navigateur Web et videz le cache.
2. Connectez-vous à QRadar SIEM. Pour des informations sur l'adresse IP, le nom d'utilisateur ou le mot de passe root, voir Accès à l'interface utilisateur d'IBM Security QRadar Risk Manager.
3. Cliquez sur l'onglet **Risques**.
4. Entrez des valeurs pour les paramètres suivants :

Option	Description
IP/Hôte	Adresse IP ou nom d'hôte du dispositif QRadar Risk Manager.
Mot de passe root	Mot de passe root du dispositif QRadar Risk Manager.

5. Cliquez sur **Sauvegarder**.

Que faire ensuite

Définissez des rôles utilisateur.

Ajout du rôle utilisateur de gestionnaire de risques

Vous devez affecter le rôle utilisateur de gestionnaire de risques (Risk manager) afin de fournir un accès à QRadar Risk Manager.

Pourquoi et quand exécuter cette tâche

Par défaut, QRadar SIEM fournit un rôle d'administration par défaut qui donne accès à la totalité du contenu de QRadar Risk Manager. Un utilisateur doté des privilèges d'administration, y compris du rôle d'administration par défaut, ne peut pas éditer son propre compte. Un autre administrateur doit procéder aux changements requis.

Pour plus d'informations sur la création et la gestion des rôles utilisateur, voir le *guide d'administration d'IBM Security QRadar SIEM*.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Configuration système**.
3. Dans le panneau **Gestion des utilisateurs**, cliquez sur **Rôles utilisateur**.
4. Dans le volet de gauche, sélectionnez le rôle utilisateur à éditer.
5. Sélectionnez la case à cocher **Risk Manager**.
6. Cliquez sur **Sauvegarder**
7. Cliquez sur **Fermer**.
8. Dans l'onglet **Fermer**, cliquez sur **Déployer les changements**.

Chapitre 3. Collecte des données réseau

Vous devez configurer QRadar Risk Manager pour pouvoir consulter les informations de configuration provenant des unités de votre réseau.

Les informations de configuration collectées depuis vos unités réseau génèrent la topologie de votre réseau et permettent à QRadar Risk Manager de comprendre votre configuration de réseau.

Les données collectées dans QRadar Risk Manager sont utilisées pour renseigner la topologie avec des informations clé sur votre environnement réseau.

La collecte de données est un processus en trois étapes :

- Fourniture à QRadar Risk Manager des données d'identification pour télécharger des configurations d'unité réseau.
- Détection des unités pour créer une liste des unités dans la gestion de sources de configuration.
- Sauvegarde de la liste des unités pour obtenir les configurations d'unité et remplir la topologie avec les données relatives à votre réseau.

Données d'identification

QRadar Risk Manager doit être configuré avec les données d'identification pour l'accès et le téléchargement des configurations d'unité. Les données d'identification permettent à QRadar Risk Manager de se connecter aux pare-feu, routeurs, commutateurs ou dispositifs IPS (Intrusion Prevention System, système de prévention des intrusions).

Les administrateurs utilisent la **gestion de sources de configuration** pour entrer des données d'identification d'unité, lesquelles fournissent à QRadar Risk Manager l'accès à une unité spécifique. QRadar Risk Manager peut sauvegarder des données d'identification d'unité individuelle pour une unité réseau spécifique. Si plusieurs unités réseau utilisent les mêmes données d'identification, vous pouvez affecter ces données à un groupe. Vous pouvez, par exemple, affecter des données d'identification à un groupe si tous les pare-feu de l'organisation ont les mêmes nom d'utilisateur et mot de passe. Les données d'identification sont associées à l'ensemble d'adresses pour tous les pare-feu et sont utilisées pour sauvegarder les configurations d'unité de tous les pare-feu de votre organisation.

Remarque : Si des données d'identification réseau ne sont pas nécessaires pour une unité spécifique, le paramètre peut être laissé à blanc dans la **gestion de sources de configuration**.

Configuration des données d'identification

Vous configurez des unités réseau pour fournir à QRadar Risk Manager l'accès aux unités.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Plug-ins**.
3. Dans le volet **Risk Manager**, cliquez sur **Gestion de sources de configuration**.

4. Dans le menu de navigation, cliquez sur **Données d'identification**.
5. Dans le volet **Groupes réseau**, cliquez sur **Ajouter un nouveau groupe réseau**.
6. Indiquez un nom pour le groupe de réseau et cliquez sur **OK**.
7. Dans la zone **Ajouter une adresse**, entrez l'adresse IP de votre unité et cliquez sur **Ajouter**. Répétez cette étape pour chaque adresse à ajouter.

   Remarque : Assurez-vous que les adresses que vous ajoutez s'affichent dans la section des adresses réseau, sous la zone **Ajouter une adresse**. Ne répliquez pas des adresses d'unité qui existent déjà dans d'autres groupes de réseau de **Gestion de sources de configuration**.
   Vous pouvez taper une adresse IP, une plage d'adresses IP, un sous-réseau CIDR ou un caractère générique. Ainsi, pour utiliser un caractère générique, tapez 10.1.*.*, ou pour utiliser un routage CIDR, tapez 10.2.1.0/24.
8. Dans le volet **Données d'identification**, cliquez sur **Ajouter un nouveau jeu de données d'identification**.
9. Indiquez un nom pour l'ensemble de données d'identification et cliquez sur **OK**.
10. Sélectionnez le nom de l'ensemble de données d'identification que vous avez créé, puis configurez des valeurs pour les paramètres suivants :

Option	Description
Username	Nom d'utilisateur valide permettant de se connecter à l'adaptateur. Pour les adaptateurs, le nom d'utilisateur et le mot de passe nécessitent l'accès à plusieurs fichiers tels que rule.C, objects.C, implied_rules.C et Standard.PF.
Password	Mot de passe de l'unité.
Enable Password	Indiquez le mot de passe pour l'authentification de second niveau. Ce mot de passe est obligatoire pour l'invite de saisie des données d'identification nécessaires à l'utilisateur pour le mode expert.
SNMP Get Community	Facultatif
SNMPv3 Authentication Username	Paramètre facultatif.
SNMPv3 Authentication Password	Paramètre facultatif.
SNMPv3 Privacy Password	Paramètre facultatif. Protocole à utiliser pour déchiffrer les messages d'alerte SNMPv3.

11. Cliquez sur **OK**.

Reconnaissance d'unités

Le processus de reconnaissance ajoute des unités réseau à l'interface de topologie en utilisant les données d'identification que vous avez ajoutées.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Plug-ins**.
3. Dans la section **Risk Manager**, cliquez sur **Gestion de sources de configuration**.
4. Dans le menu de navigation, cliquez sur **Reconnaître les unités**.
5. Entrez une adresse IP ou une plage CIDR pour indiquer l'emplacement des unités à reconnaître.
6. Cliquez sur l'icône **Ajouter (+)**.
7. Si vous souhaitez rechercher des unités sur le réseau à partir de l'adresse IP ou de la plage CIDR définie, sélectionnez la case **Crawl the network from the addresses defined above**.
8. Cliquez sur **Exécuter**.

Obtention de la configuration d'unité

Vous sauvegardez vos unités pour télécharger la configuration d'unité afin que QRadar Risk Manager puisse inclure les informations d'unité dans la topologie.

Avant de commencer

Vous devez configurer des ensembles de données d'identification avant de pouvoir télécharger des configurations d'unité.

Pourquoi et quand exécuter cette tâche

Vous pouvez sauvegarder une unité unique ou toutes les unités.

Pour des informations sur la planification des sauvegardes automatiques des configurations d'unité depuis l'onglet des **travaux**, voir le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Plug-ins**.
3. Dans le volet **Risk Manager**, cliquez sur **Gestion de sources de configuration**.
4. Cliquez sur l'onglet **Unités**.
5. Pour obtenir la configuration pour toutes les unités, cliquez sur **Tout sauvergarder** dans le panneau de navigation. Cliquez sur **Oui** pour continuer.
6. Pour obtenir la configuration d'une unité spécifique, sélectionnez l'unité concernée. Pour sélectionner plusieurs unités à sauvegarder, maintenez la touche Ctrl enfoncée. Cliquez sur **Sauvegarder**.

Importation d'unités

Utilisez l'importation d'unité pour ajouter une liste d'adaptateurs et leurs adresses IP réseau au gestionnaire de sources de configuration via un fichier au format CSV.

La liste d'importation d'unités peut comporter jusqu'à 5000 unités, mais chaque adaptateur et son adresse IP associée doit figurer sur une seule ligne dans le fichier d'importation.

Par exemple,

```
<Adaptateur::Nom 1>,<Adresse IP>
<Adaptateur::Nom 2>,<Adresse IP>
<Adaptateur::Nom 3>,<Adresse IP>
```

Où :

`<Adaptateur::Nom>` contient le fabricant et le nom d'unité, par exemple Cisco::IOS.

`<Adresse IP>` contient l'adresse IP de l'unité, par exemple 191.168.1.1.

Tableau 3. Exemples d'importation d'unité

Fabricant	**Nom**	**Exemple de type <Adaptateur::Nom>,<Adresse IP>**
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Importation d'un fichier CSV

Vous pouvez importer une liste maître des unités dans la gestion de sources de configuration via un fichier au format CSV.

Avant de commencer

Si vous importez une liste de unités puis modifiez une adresse IP dans le fichier CSV, vous risquez de dupliquer accidentellement une unité dans la liste de gestion de sources de configuration. Pour cette raison, supprimez l'unité de la gestion de sources de configuration avant de réimporter votre liste maître.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Plug-ins**.
3. Dans le volet **Plug-Ins**, cliquez sur **Importation d'unité**.
4. Cliquez sur **Parcourir**.
5. Localisez votre fichier CSV et cliquez sur **Ouvrir**.
6. Cliquez sur **Importer les unités**.

Résultats

Si un message d'erreur s'affiche, vous devez examiner votre fichier CSV afin de corriger les erreurs, puis réimporter le fichier. Une importation du fichier CSV peut échouer si la liste des unités est structurée incorrectement ou si la liste comporte des informations inexactes. Il se peut, par exemple, qu'il manque des virgules ou une commande dans votre fichier CSV, que plusieurs unités figurent sur une ligne unique, ou qu'un nom d'adaptateur comporte une faute de frappe.

Si l'importation d'unité est abandonnée, aucune des unités du fichier CSV n'est ajoutée à la gestion de sources de configuration.

Traitement des incidents d'importation d'unité

Si vous recevez un message d'erreur après une tentative d'importation de votre unité, il peut être lié à l'échec de l'importation du fichier CSV.

L'importation d'une unité peut échouer si la liste des unités n'est pas correctement structurée. Ainsi, certaines colonnes ou une commande peuvent être absentes du fichier CSV, ou bien plusieurs unités peuvent figurer sur une seule ligne.

Autre possibilité : l'importation peut échouer si la liste des unités comporte des informations incorrectes. Par exemple, une erreur typographique dans un nom d'adaptateur.

Si l'importation d'unité est abandonnée, aucune des unités du fichier CSV n'est ajoutée à la gestion de sources de configuration. La liste des noms d'adaptateur valides pour vos adaptateurs installés est fournie dans le message. Si une erreur est affichée, vous devez vérifier votre fichier CSV afin de corriger toute erreur éventuelle. Vous pouvez réimporter le fichier une fois les erreurs corrigées.

Chapitre 4. Gestion des audits

IBM Security QRadar Risk Manager permet de simplifier l'évaluation des politiques de sécurité des réseaux et les exigences de conformité en vous aidant à répondre aux questions.

L'audit de conformité est une tâche nécessaire et complexe pour les administrateurs de sécurité. QRadar Risk Manager vous aide à répondre aux questions suivantes :

- Comment sont configurées mes unités réseau ?
- Comment communiquent mes ressources réseau ?
- Où mon réseau est-il vulnérable ?

Cas d'utilisation : Audit de configuration

Vous pouvez utiliser les informations de configuration relatives aux appareils réseau, informations capturées par QRadar Risk Manager, pour faire un audit de conformité et planifier des sauvegardes de configuration.

Les sauvegardes de configuration offrent une méthode centralisée et automatique d'enregistrer les modifications d'unité pour la conformité d'audit. Les sauvegardes de configuration archivent les changements de configuration et fournissent une référence historique ; vous pouvez capturer un enregistrement historique ou comparer une configuration par rapport à une autre unité réseau.

L'audit de configuration dans QRadar Risk Manager propose les options suivantes :

- Enregistrement historique de vos configurations d'unité réseau.
- Vue normalisée, qui affiche les changements lors de la comparaison de configurations.
- Outil de recherche de règles sur votre unité.

Les informations de configuration de votre unité sont collectées à partir des sauvegardes d'unité dans la gestion des sources de configuration. Chaque fois que QRadar Risk Manager sauvegarde votre liste des unités, il archive une copie de votre configuration d'unité afin de fournir une référence historique. Plus vous programmez fréquemment la gestion des sources de configuration, plus vous disposez d'enregistrements de configuration pour comparaison et référence historique.

Visualisation de l'historique de configuration d'unité

Vous pouvez afficher l'historique de configuration d'une unité réseau.

Pourquoi et quand exécuter cette tâche

Vous pouvez afficher les informations d'historique des unités réseau qui ont été sauvegardées. Ces informations sont accessibles depuis le panneau **History** à la page **Configuration Monitor**. Le panneau d'historique fournit des informations sur une configuration d'unité réseau ainsi que la date à laquelle la configuration d'unité a été sauvegardée pour la dernière fois à l'aide de la gestion de sources de configuration.

La configuration indique le type des fichiers stockés pour votre unité réseau dans QRadar Risk Manager. Types de configuration communs :

- **Standard-Element-Document** (SED), qui correspond aux fichiers de données XML contenant les informations sur votre unité réseau. Les fichiers SED individuels sont affichés au format XML brut. Si un fichier SED est comparé à un autre fichier SED, la vue est normalisée afin d'afficher les différences de règle.
- **Config**, qui correspond aux fichiers de configuration fournis par certaines unités réseau. Ces fichiers dépendent du fabricant d'unité. Un fichier de configuration peut être visualisé en cliquant deux fois dessus.

Remarque : Selon votre unité, plusieurs autres fichiers de configuration peuvent être affichés. Cliquez deux fois sur ces fichiers pour afficher leur contenu en texte normal. La vue en texte normal prend en charge les fonctions de recherche (Ctrl +f), coller (Ctrl+v) et copier (Ctrl+C) de la fenêtre du navigateur Web.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Configuration Monitor**.
3. Cliquez deux fois sur une configuration pour afficher les informations détaillées de l'unité.
4. Cliquez sur **History**.
5. Dans le panneau **History**, sélectionnez une configuration.
6. Cliquez sur **View Selected**.

Comparaison de configurations d'unité pour une unité unique

Vous pouvez comparer des configurations d'unité pour une unité unique.

Pourquoi et quand exécuter cette tâche

Si les fichiers que vous comparez sont de type SED (Standard-Element-Documents), vous pouvez afficher les différences de règle entre les fichiers de configuration.

Lorsque vous comparez des configurations normalisées, la couleur du texte suit les règles suivantes :

- Un contour en pointillés vert indique une règle ou une configuration ajoutée à l'unité.
- Un contour en tirets rouge indique une règle ou une configuration supprimée de l'unité.
- Un contour plein en jaune indique une règle ou une configuration modifiée sur l'unité.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Configuration Monitor**.
3. Cliquez deux fois sur une unité pour afficher les informations détaillées de configuration.
4. Cliquez sur **History** pour afficher l'historique de l'unité.
5. Sélectionnez une configuration principale.
6. Appuyez sur la touche Ctrl et sélectionnez une deuxième configuration pour comparaison.

7. Dans le panneau **History**, cliquez sur **Compare Selected**.
8. Facultatif. Pour afficher les différences de configuration brutes, cliquez sur **View Raw Comparison**. Si la comparaison concerne un fichier de configuration ou un autre type de sauvegarde, la comparaison brute s'affiche.

Comparaison de configurations d'unité pour différentes unités

Vous pouvez comparer deux configurations pour différentes unités

Pourquoi et quand exécuter cette tâche

Si les fichiers que vous comparez sont de type SED (Standard-Element-Documents), vous pouvez afficher les différences de règle entre les fichiers de configuration.

Lorsque vous comparez des configurations normalisées, la couleur du texte suit les règles suivantes :

- Un contour en pointillés vert indique une règle ou une configuration ajoutée à l'unité.
- Un contour en tirets rouge indique une règle ou une configuration supprimée de l'unité.
- Un contour plein en jaune indique une règle ou une configuration modifiée sur l'unité.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Configuration Monitor**.
3. Cliquez deux fois sur une unité pour afficher les informations détaillées de configuration.
4. Cliquez sur **History** pour afficher l'historique de l'unité.
5. Sélectionnez une configuration principale.
6. Cliquez sur **Mark for Comparison**.
7. Dans le menu de navigation, sélectionnez **All Devices** pour revenir à la liste des unités.
8. Cliquez deux fois sur l'unité à comparer puis cliquez sur **History**.
9. Sélectionnez une autre sauvegarde de configuration à comparer à la configuration marquée.
10. Cliquez sur **Compare with Marked**.
11. Facultatif. Pour afficher les différences de configuration brutes, cliquez sur **View Raw Comparison**. Si la comparaison concerne un fichier de configuration ou un autre type de sauvegarde, la comparaison brute s'affiche.

Cas d'utilisation : Visualisation des chemins réseau dans la topologie

La topologie dans QRadar Risk Manager affiche une représentation graphique de vos unités réseau.

Une recherche de chemin topologique permet de déterminer la façon dont les unités réseau communiquent et le chemin réseau qu'elles utilisent pour communiquer. La recherche de chemin permet à QRadar Risk Manager d'afficher de manière visible le chemin entre une source et une destination, ainsi que les ports, protocoles et règles.

Vous pouvez visualiser la façon dont les unités communiquent, ce qui est essentiel sur des actifs à accès sécurisé ou restreint.

Fonctions principales :

- Possibilité de visualiser les communications entre unités sur le réseau.
- Utilisation de filtres pour rechercher des unités réseau dans la topologie.
- Accès rapide pour consulter les règles et la configuration d'unité.
- Possibilité de visualiser les événements qui sont générés à partir d'une recherche de chemin.

Recherche sur la topologie

Vous pouvez visualiser la communication d'unités en effectuant une recherche sur la topologie.

Pourquoi et quand exécuter cette tâche

Une recherche de chemin est utilisée pour filtrer le modèle de topologie. Une recherche de chemin inclut tous les sous-réseaux comportant les adresses IP ou plages de routage CIDR source et tous les sous-réseaux comportant les adresses IP ou plages de routage CIDR de destination pour le réseau et qui sont autorisés à communiquer via le protocole et le port configurés. La recherche examine votre modèle de topologie existant et inclut les unités impliquées dans le chemin de communication entre la source et la destination, ainsi que les informations de connexion détaillées.

Vous pouvez utiliser des vulnérabilités pour filtrer la recherche si votre topologie inclut un système de prévention des intrusions (IPS). Pour plus d'informations, reportez-vous au manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Topologie**.
3. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche**.
4. Dans le volet **Critères de recherche**, sélectionnez **Chemin**.
5. Dans la zone **Source IP/CIDR**, entrez l'adresse IP ou la plage de routage CIDR sur laquelle vous souhaitez filtrer le modèle de topologie. Séparez les entrées multiples par des virgules.
6. Dans la zone **Destination IP/CIDR**, entrez l'adresse IP ou la plage de routage CIDR de destination sur laquelle vous souhaitez filtrer le modèle de topologie. Séparez les entrées multiples par des virgules.
7. Facultatif. Dans la liste **Protocole**, sélectionnez le protocole à utiliser pour filtrer le modèle de topologie.
8. Facultatif. Dans la zone **Port de destination**, indiquez le port de destination sur lequel filtrer le modèle de topologie. Séparez les entrées multiples par des virgules.
9. Cliquez sur **OK**.
10. Passez le curseur sur une ligne de connexion pour afficher les détails relatifs à cette connexion. Si la recherche se connecte à une unité comportant des règles, un lien vers les règles de l'unité s'affiche dans la boîte de dialogue.

Cas d'utilisation : Visualisation du chemin d'attaque d'une infraction

Dans QRadar Risk Manager, les infractions sont des événements générés par le système afin de vous alerter au sujet d'une condition ou d'un événement sur le réseau.

La visualisation de chemin d'attaque lie les infractions aux recherches topologiques. Cette visualisation permet aux opérateurs de sécurité de visualiser les détails de l'infraction et le chemin emprunté par l'infraction à travers le réseau. Le chemin d'attaque fournit une représentation visuelle. Cette représentation montre les actifs du réseau qui communiquent pour autoriser une infraction à passer par le réseau. Ces données sont essentielles lors de l'audit afin de prouver que vous surveillez les infractions, mais elles prouvent également que l'infraction ne dispose pas d'un chemin de remplacement sur votre réseau pour accéder à un actif critique.

Fonctions principales pour la visualisation :

- Optimisation du système de règles et d'infractions existant à partir de QRadar SIEM.
- Affichage d'un chemin visuel pour toutes les unités entre la source et la destination de l'infraction.
- Accès rapide aux configurations d'unité et aux règles qui autorisent l'infraction.

Visualisation du chemin d'attaque d'une infraction

Vous pouvez visualiser le chemin d'attaque d'une infraction. Le chemin d'attaque indique la source, la destination et les unités associées.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans le menu de navigation, cliquez sur **Toutes les infractions**. La page **Toutes les infractions** affiche la liste des infractions existant sur votre réseau. Les infractions sont répertoriées en commençant par celle avec la plus grande ampleur.
3. Cliquez deux fois sur une infraction pour ouvrir le récapitulatif correspondant.
4. Dans la barre d'outils **Infractions**, cliquez sur **Visualiser le chemin d'attaque**.

Chapitre 5. Cas d'utilisation : Surveillance des politiques d'administration

L'audit des politiques d'administration et le contrôle des changements constituent des processus fondamentaux permettant aux administrateurs et aux professionnels de la sécurité de contrôler l'accès et les communications entre des actifs métier critiques.

Les critères de surveillance des politiques d'administration peuvent inclure la surveillance des actifs et des communications pour les scénarios suivants :

- Mon réseau comporte-t-il des actifs avec des configurations à risque pour les audits PCI Section 1 ?
- Mes actifs autorisent-ils des communications utilisant des protocoles à risque pour les audits PCI Section 10 ?
- Comment savoir quand un changement de politique d'administration place mon réseau en situation de violation ?
- Comment visualiser les vulnérabilités d'actifs à haut risque ou sécurisés ?
- Comment visualiser les actifs du réseau présentant des vulnérabilités et un accès à Internet ?

Utilisez le moniteur de politique d'administration pour définir des tests basés sur les indicateurs de risque, puis limitez les résultats de test afin de filtrer la requête en fonction de résultats, violations, protocoles ou vulnérabilités spécifiques.

IBM Security QRadar Risk Manager inclut plusieurs questions du moniteur de politique d'administration qui sont regroupées par catégorie PCI (Payment Card Industry). Par exemple, les questions PCI 1, PCI 6 et PCI 10. Vous pouvez créer des questions pour des actifs ou des unités et des règles pour exposer un risque de sécurité pour le réseau. Après qu'une question relative à un actif ou une unité/règle a été soumise au moniteur de politique d'administration, les résultats renvoyés spécifient le niveau de risque. Vous pouvez approuver les résultats renvoyés par les actifs, ou définir la façon dont vous souhaitez que le système réponde aux résultats non approuvés.

Le moniteur de politique d'administration fournit les fonctions principales suivantes :

- Poser des questions prédéfinies au moniteur de politique d'administration pour assister le flux de travaux.
- Déterminer si des utilisateurs ont utilisé des protocoles interdits pour communiquer.
- Evaluer si des utilisateurs sur des réseaux spécifiques peuvent communiquer avec des réseaux ou des actifs interdits.
- Evaluer si des règles de pare-feu satisfont la politique de l'entreprise.
- Surveiller en continu les politiques d'administration qui génèrent des infractions ou des alertes envoyées aux administrateurs.
- Donner un ordre de priorité aux vulnérabilités en évaluant les systèmes qui peuvent être compromis suite à la configuration d'unité.
- Aider à identifier les problèmes de conformité.

Cas d'utilisation : Evaluation d'actifs ayant des configurations suspectes

Les organisations utilisent des politiques de sécurité d'entreprise pour définir des risques et les communications autorisées entre actifs et réseaux. Pour les aider à être conformes à la politique de l'entreprise et prévenir les violations, les organisations utilisent le moniteur de politique d'administration (Policy Monitor) afin d'évaluer et de contrôler les risques potentiels inconnus.

Selon les règles édictées par l'industrie des cartes de paiement (PCI, Payment Card Industry), vous devez identifier les unités comportant des données sur les titulaires de carte, établir un diagramme, vérifier les communications, et surveiller les configurations de pare-feu afin de protéger les actifs comportant des données sensibles. Le moniteur de politique d'administration (Policy Monitor) fournit des méthodes pour rapidement satisfaire ces exigences et permet aux administrateurs d'adhérer aux politiques de l'entreprise. Les méthodes communes permettant de réduire les risques incluent l'identification et la surveillance des actifs qui communiquent avec des protocoles non sécurisés. Ces protocoles incluent les routeurs, pare-feu ou commutateurs autorisant des connexions FTP ou telnet. Utilisez le moniteur de politique d'administration pour identifier les actifs de votre topologie qui présentent des configurations à risque.

Les questions PCI section 1 peuvent inclure les critères suivants :

- Actifs autorisant des protocoles interdits.
- Actifs autorisant des protocoles à risque.
- Actifs autorisant des applications contrevenant à la politique d'administration sur le réseau.
- Actifs autorisant des applications contrevenant à la politique d'administration sur des réseaux comportant des actifs protégés.

Evaluation des unités autorisant des protocoles à risque

Utilisez le moniteur de politique d'administration (Policy Monitor) pour évaluer des unités autorisant des protocoles à risque.

Pourquoi et quand exécuter cette tâche

QRadar Risk Manager évalue la question et affiche les résultats de tout actif dans votre topologie qui correspond à la question test. Les spécialistes de la sécurité, les administrateurs ou les auditeurs de votre réseau peuvent approuver des communications qui ne présentent pas de risque pour des actifs spécifiques. Ils peuvent également créer des infractions correspondant au comportement.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans la zone de liste Groupe, sélectionnez **PCI 1**.
4. Séletionnez la question de test pour **Assess any devices (i.e. firewalls) that allow risky protocols (i.e telnet and FTP traffic - port 21 & 23 respectively) from the internet to the DMZ**.
5. Cliquez sur **Soumettre la question**.

Cas d'utilisation : Evaluation d'actifs avec communication suspecte

Utilisez le moniteur de politique d'administration (Policy Monitor) pour identifier la conformité PCI section 10 en effectuant le suivi, la consignation et l'affichage des accès aux actifs réseau.

QRadar Risk Manager peut vous aider à identifier la conformité aux règles PCI section 10 en identifiant les actifs de la topologie qui autorisent des communications douteuses ou à risque. QRadar Risk Manager peut examiner ces actifs et identifier les communications réelles ou potentielles. Les communications réelles affichent des actifs qui ont utilisé les critères définis dans vos questions pour communiquer. Les communications potentielles affichent des actifs pouvant utiliser les critères définis dans vos questions pour communiquer.

Les questions PCI section 10 peuvent inclure les critères suivants :

- Actifs autorisant les questions entrantes adressées à des réseaux internes.
- Actifs communiquant depuis des emplacements non sécurisés vers des emplacements sécurisés.
- Actifs communiquant depuis un réseau privé virtuel vers des emplacements sécurisés.
- Actifs autorisant des protocoles contrevenant à la politique d'administration et non chiffrés au sein d'un emplacement sécurisé.

Recherche d'actifs autorisant la communication

Vous pouvez rechercher des actifs autorisant la communication depuis Internet.

Pourquoi et quand exécuter cette tâche

QRadar Risk Manager évalue la question et affiche les résultats de tout actif interne autorisant des connexions entrantes provenant d'Internet. Les spécialistes de la sécurité, les administrateurs ou les auditeurs de votre réseau peuvent approuver des communications avec des actifs qui ne sont pas considérés comme sécurisés ou comportant des données client. Lorsque d'autres événements sont générés, vous pouvez créer des infractions dans QRadar SIEM afin de surveiller ce type de communication à risque.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans la zone de liste Groupe, sélectionnez **PCI 10**.
4. Sélectionnez la question de test **Assess any inbound connections from the internet to anywhere on the internal network**.
5. Cliquez sur **Soumettre la question**.

Cas d'utilisation : Surveillance des politiques d'administration pour les violations

QRadar Risk Manager peut surveiller en continu toute question prédéfinie ou générée par l'utilisateur via le moniteur de politique d'administration (Policy Monitor). Vous pouvez utiliser le mode moniteur pour générer des événements dans QRadar Risk Manager.

Lorsque vous sélectionnez une question à surveiller, QRadar Risk Manager analyse à chaque heure la question en fonction de votre topologie, ce afin de déterminer si un changement au niveau d'un actif ou d'une règle génère un résultat non approuvé. Si QRadar Risk Manager détecte un résultat non approuvé, une infraction peut être générée afin de vous alerter sur une déviation de la politique d'administration définie. En mode moniteur, QRadar Risk Manager peut surveiller simultanément les résultats de 10 questions.

La surveillance des questions fournit les fonctions principales suivantes :

- Surveillance horaire des modifications de règle ou d'actif pour des résultats non approuvés.
- Utilisation de vos catégories d'événement de haut et bas niveaux afin de classer les résultats non approuvés.
- Génération d'infractions, de courriers électroniques, de messages syslog ou de notifications de tableau de bord portant sur les résultats non approuvés.
- Utilisation de la visualisation des événements, corrélation, rapport d'événement, règles personnalisées et tableaux de bord dans QRadar SIEM.

Configuration d'une question

Vous pouvez utiliser le moniteur de politique d'administration (Policy Monitor) pour configurer une question à surveiller.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Sélectionnez la question à surveiller.
4. Cliquez sur **Moniteur**.
5. Configurez les options nécessaires pour surveiller votre question.
6. Cliquez sur **Sauvegarder le moniteur**.

Résultats

La surveillance est activée pour la question et des événements ou des infractions sont générés en fonction de vos critères de surveillance.

Cas d'utilisation : Utilisation de vulnérabilités pour hiérarchiser les risques

Les vulnérabilités exposées constituent un facteur de risque significatif pour les actifs réseau.

QRadar Risk Manager exploite les informations relatives aux actifs et aux vulnérabilités dans le moniteur de politique d'administration (Policy Monitor). Ces informations sont utilisées pour déterminer si vos actifs sont sensibles aux attaques de type entrée telles que les injections SQL, les champs masqués ou le clickjacking (détournement de clic).

Les vulnérabilités détectées sur vos actifs peuvent être classées par ordre de priorité (hiérarchisées) en fonction de leur emplacement ou d'une connexion à une autre unité elle-même vulnérable.

Les questions d'actifs vulnérables peuvent inclure les critères suivants :

- Actifs avec de nouvelles vulnérabilités signalées à compter d'une date spécifique.
- Actifs avec des vulnérabilités ou un score CVSS spécifiques.
- Actifs avec une classification spécifique de vulnérabilité, comme la manipulation d'entrées, le refus de service, l'OSVDB vérifié.

Recherche d'actifs présentant des vulnérabilités

Vous pouvez rechercher les actifs présentant des vulnérabilités.

Pourquoi et quand exécuter cette tâche

QRadar Risk Manager évalue une question et affiche les résultats pour les actifs comportant la vulnérabilité que vous recherchez. Les spécialistes de la sécurité, les administrateurs ou les auditeurs peuvent identifier des actifs de votre réseau qui contiennent des vulnérabilités connues d'injection SQL. Ils peuvent immédiatement corriger tout actif connecté à un réseau protégé. Lorsque d'autres événements sont générés, vous pouvez créer des infractions dans QRadar SIEM afin de surveiller les actifs qui présentent des vulnérabilités d'injection SQL.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans la liste **Groupe**, sélectionnez **Vulnérabilité**.
4. Sélectionnez la question de test **Assess assets with SQL injection vulnerabilities on specific localnet(s) (i.e. protected server network)**.
5. Cliquez sur **Soumettre la question**.

Cas d'utilisation : Hiérarchisation des vulnérabilités d'actif par zone ou communication réseau

Les systèmes présentant des vulnérabilités sur un même réseau que des actifs protégés représentent un risque plus élevé de perte de données.

La détection des vulnérabilités sur des actifs par zone ou réseau constitue une mesure clé pour empêcher les exploitations avant qu'elles ne surviennent sur votre réseau. Les normes PCI section 6.1 et 6.2 stipulent que vous devez réviser et corriger vos systèmes sous un mois à compter de la publication d'un correctif de vulnérabilité. QRadar Risk Manager vous aide à automatiser et gérer les priorités du processus d'application de correctif. Lorsque des vulnérabilités sont détectées sur vos actifs, vous pouvez les classer en fonction de l'emplacement réseau ou d'une connexion à une autre unité elle-même vulnérable. La hiérarchisation est importante pour les réseaux sécurisés qui peuvent être connectés à des régions suspectes, ou pour des actifs affichant un score CVSS supérieur à celui autorisé par votre politique d'administration interne.

Les questions portant sur les actifs vulnérables peuvent inclure les critères suivants :

- Actifs présentant une vulnérabilité côté client, qui communiquent avec des régions géographiques suspectes et comportent des actifs protégés.
- Actifs présentant des vulnérabilités de refus de service sur un réseau spécifique.
- Actifs présentant des vulnérabilités de messagerie sur un réseau spécifique.

- Actifs présentant des vulnérabilités et un score CVSS (Common Vulnerability Scoring System) spécifique.

Recherche sur un réseau d'actifs présentant des vulnérabilités

Vous pouvez rechercher sur un réseau particulier les actifs présentant des vulnérabilités.

Pourquoi et quand exécuter cette tâche

QRadar Risk Manager évalue la question et affiche les résultats pour l'emplacement spécifique qui comporte des vulnérabilités spécifiques au système d'exploitation. Les spécialistes de la sécurité, les administrateurs ou les auditeurs de votre réseau peuvent approuver des communications avec des actifs qui ne sont pas considérés comme sécurisés ou comportant des données client. Lorsque d'autres événements sont générés, vous pouvez créer des infractions afin de surveiller ce type de communication à risque.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans la zone de liste **Groupe**, sélectionnez **Vulnérabilité**.
4. Sélectionnez la question de test **Assess assets with OS specific vulnerabilities on a specific localnet(s)**.
5. Cliquez sur **Soumettre la question**.

Chapitre 6. Cas d'utilisation pour les simulations

Cas d'utilisation : Simulation d'attaques sur des actifs réseau

Vous pouvez utiliser une simulation pour tester la vulnérabilité de votre réseau à partir de différentes sources.

Vous pouvez utiliser des simulations d'attaque pour effectuer l'audit des configurations d'unité de votre réseau.

Les simulations offrent les fonctions principales suivantes :

- Elles affichent les permutations de chemin théoriques qu'une attaque peut exécuter sur votre réseau.
- Elles montrent la façon dont des attaques peuvent se propager via vos unités réseau et atteindre d'autres actifs.
- Elles permettent à la surveillance de détecter de nouveaux sites d'exposition.

Création d'une simulation

Vous pouvez créer une simulation pour une attaque du réseau via un protocole Secure Shell (SSH).

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, sélectionnez **Simulation** > **Simulations**.
3. Dans la liste **Actions**, sélectionnez **Nouveau**.
4. Indiquez un nom pour la simulation.
5. Sélectionnez **Topologie en cours**.
6. Cochez la case **Utiliser les données de connexion**.
7. Dans la liste **Where do you want the simulation to begin**, sélectionnez l'origine de la simulation.
8. Ajoutez la simulation d'attaque dans **Attack targets one of the following open ports using protocols**.
9. Pour cette simulation, cliquez sur **Ports ouverts** puis ajoutez le port 22.
10. Cliquez sur **protocoles** puis sélectionnez **TCP**. SSH utilise TCP.
11. Cliquez sur **OK**.
12. Cliquez sur **Sauvegarder la simulation**.
13. Dans la liste **Actions**, sélectionnez **Exécuter la simulation**. La colonne des résultats comporte une liste avec la date d'exécution de la simulation et un lien pour afficher les résultats.
14. Cliquez sur **Afficher les résultats**.

Résultats

Une liste d'actifs comportant des vulnérabilités SSH s'affiche dans les résultats, permettant ainsi aux administrateurs réseau d'approuver les connexions SSH qui sont autorisées ou prévues sur votre réseau. Les communications qui ne sont pas approuvées peuvent être surveillées pour les événements ou les infractions.

Les résultats affichés fournissent aux administrateurs réseau ou aux spécialistes de la sécurité une représentation visuelle du chemin d'attaque et des connexions que l'attaque pourrait emprunter sur votre réseau. Par exemple, la première étape fournit la liste des actifs directement connectés qui sont affectés par la simulation. La deuxième étape répertorie les actifs du réseau qui peuvent communiquer avec des actifs de premier niveau de votre simulation.

Les informations fournies dans l'attaque permettent de renforcer et de tester votre réseau face aux milliers de scénarios d'attaque possibles.

Cas d'utilisation : Simulation des risques liés aux modifications de configuration de réseau

Vous pouvez utiliser un modèle de topologie afin de définir des modèles de réseau virtuel basés sur votre réseau existant. Vous pouvez créer un modèle de réseau basé sur une série de modifications pouvant être combinées et configurées.

Vous pouvez utiliser un modèle de topologie pour déterminer l'effet de modifications de configuration sur votre réseau en utilisant une simulation.

les modèles de topologie fournissent les fonctionnalités clés suivantes :

- Création de topologies virtuelles pour tester les modifications du réseau.
- Simulation d'attaques sur des réseaux virtuels.
- Risque et exposition plus faibles des actifs protégés via le test.
- Segments de réseau virtuel permettant de confiner et de tester des parties sensibles de votre réseau ou de vos actifs.

Pour simuler une modification de configuration de réseau, procédez comme suit :

1. Créez un modèle de topologie.
2. Simulez une attaque du modèle de topologie.

Création d'un modèle de topologie

Vous pouvez créer un modèle de topologie afin de tester des modifications de réseau et simuler des attaques.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, sélectionnez **Simulations** > **Modèle de topologie**.
3. Dans la liste **Actions**, sélectionnez **Nouveau**.
4. Entrez un nom pour le modèle.
5. Sélectionnez les modifications à appliquer à la topologie.
6. Configurez les tests ajoutés au panneau **Configurer le modèle comme suit**.
7. Cliquez sur **Sauvegarder le modèle**.

Que faire ensuite

Créez une simulation pour votre nouveau modèle de topologie.

Simulation d'une attaque

Vous pouvez simuler une attaque sur des ports et des protocoles.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, sélectionnez **Simulation** > **Simulations**.
3. Dans la zone de liste **Actions**, sélectionnez **Nouveau**.
4. Indiquez un nom pour la simulation.
5. Sélectionnez un modèle de topologie que vous avez créé.
6. Dans la liste **Where do you want the simulation to begin**, sélectionnez l'origine de la simulation.
7. Ajoutez la simulation d'attaque dans **Attack targets one of the following open ports using protocols**.
8. Pour cette simulation, cliquez sur **Ports ouverts** puis ajoutez le port 22.
9. Cliquez sur **protocoles** et sélectionnez TCP. SSH utilise TCP.
10. Cliquez sur **OK**.
11. Cliquez sur **Sauvegarder la simulation**.
12. Dans la liste **Actions**, sélectionnez **Exécuter la simulation**. La colonne des résultats comporte une zone de liste avec la date d'exécution de la simulation et un lien pour afficher les résultats.
13. Cliquez sur **Afficher les résultats**.

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 d'International Business Machines Corporation aux Etats-Unis et/ou dans certains 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 exister et éventuellement avoir été enregistrées 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).

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).

Index