

IBM Security QRadar Risk Manager
Version 7.3.1

Guide d'utilisation

IBM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 145.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.1 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*

© Copyright IBM France 2017. Tous droits réservés.

© **Copyright IBM Corporation 2012, 2017.**

Table des matières

Avis aux lecteurs canadiens	vii
Présentation d'IBM Security QRadar Risk Manager	ix
1 Nouveautés de QRadar Risk Manager version 7.3.1	1
2 IBM Security QRadar Risk Manager	3
Navigateurs Web pris en charge	3
Activation du mode document et du mode navigateur dans Internet Explorer	4
Accès à l'interface utilisateur d'IBM Security QRadar Risk Manager	4
Fonctions non prises en charge dans IBM Security QRadar Risk Manager	4
3 Présentation des fonctions de QRadar Risk Manager	5
4 Configuration de l'accès à QRadar Risk Manager	9
Configuration des paramètres système.	9
Mise à jour de l'heure système	10
5 Configuration Source Management.	13
Données d'identification	13
Configuration des données d'identification pour IBM Security QRadar Risk Manager.	14
Reconnaissance d'unité	15
Reconnaissance des unités	16
Importation de périphériques	16
Importation d'un fichier CSV	17
Gestion des unités	18
Affichage des unités	18
Ajout d'un périphérique	18
Modification des unités	19
Suppression d'une unité	19
Filtrage de la liste d'unités	19
Obtention d'une configuration de périphérique	21
Collecte de données voisines	21
Gestion des travaux de sauvegarde	22
Affichage des travaux de sauvegarde.	22
Affichage de l'état et des journaux des travaux de sauvegarde	23
Ajout d'un travail de sauvegarde	23
Modification d'un travail de sauvegarde.	25
Renommage d'un travail de sauvegarde	26
Suppression d'un travail de sauvegarde	26
Configuration de protocoles	27
Configuration des protocoles	27
Configuration de la planification du processus de reconnaissance	30
6 Connexions.	31
Affichage des connexions.	31
Utilisation des graphiques pour afficher les données de connexion	34
Utilisation du graphique de série temporelle	34
Utilisation du graphique de connexion pour afficher les connexions réseau	36
Utilisation des graphiques circulaires, à barres et tabulaires	38
Recherche de connexions	39
Enregistrement des critères de recherche.	40
Effectuer une sous-recherche.	42
Gestion des résultats de recherche.	43

Sauvegarde des résultats de la recherche	44
Annulation d'une recherche	44
Suppression d'une recherche.	44
Exportation des connexions	45
7 Moniteur de configuration	47
Recherche des règles de périphérique.	47
Comparaison de la configuration de vos périphériques réseau	48
Gestion des périphériques	49
Ajout d'un périphérique	49
Sauvegarde d'un périphérique	50
Suppression d'un périphérique	50
Reconnaissance de périphériques	50
Activité récente	51
Mappage de sources de journal.	52
Création ou modification d'un mappage de source de journal	52
8 Filtrage des règles de périphérique par utilisateur ou groupe	55
9 Graphique de topologie de réseau	57
Recherches de diagramme de topologie	57
Indicateurs NAT dans les résultats de recherche	58
Ajout d'un système de prévention contre les intrusions (IPS)	59
Suppression d'un système de prévention contre les intrusions (IPS).	59
Groupes de périphériques de la topologie	59
Cas d'utilisation : Visualisation du chemin d'attaque d'une infraction	60
Visualisation du chemin d'attaque d'une infraction	60
10 Configuration du code couleur des sous-réseaux pour indiquer le statut de vulnérabilité	61
11 Moniteur de politique d'administration	63
Questions du moniteur de politique d'administration	63
Paramètres relatifs à la question du moniteur de politique d'administration	64
Questions de contribution pour les tests de communication réelle	65
Questions de test de contribution dépréciées	68
Questions de restriction pour les tests de communication réelle	68
Questions de contribution pour des tests de communication possible	70
Questions de test de contribution dépréciées	73
Paramètres de questions de restriction pour les tests de communication possible	73
Questions de test relatives aux unités/règles	74
Coefficient d'importance	75
Création d'une question d'actif	75
Recherche des communications externes utilisant des protocoles non sécurisés	76
Recherche d'actifs autorisant la communication par Internet	77
Evaluation des unités autorisant des protocoles à risque	77
Recherche des communications possibles avec les actifs protégés	78
Informations relatives aux questions	78
Création d'une question relative au test des violations de règles.	79
Recherche des unités/règles établissant une communication par Internet	79
Soumission d'une question	80
Résultats d'une question d'actif.	80
Résultats de la question relative aux unités/règles	83
Evaluation des résultats à partir des questions du moniteur de politique d'administration	85
Validation des résultats	86
Surveillance de la question de politique d'administration	86
Surveillance d'une question de moniteur de politique d'administration et génération d'événements	87
Questions de groupe	88
Exportation et importation de questions du moniteur de politique d'administration	88

Exportation de questions de moniteur de politique d'administration	89
Importation des questions de moniteur de politique d'administration	89
Intégration à QRadar Vulnerability Manager	90
Surveillance des comptages d'événements de règle de pare-feu des périphériques Check Point	90
Configuration des applications OPSEC dans SmartDashboard	92
Configuration de la source de journal.	93
Etablissement d'une communication sécurisée entre Check Point et IBM Security QRadar	95
Initialisation du comptage de règles pour Check Point	96
Cas d'utilisation du moniteur de politique d'administration	96
Hiérarchisation des vulnérabilités à haut risque par l'application de politiques de risque	96
Analyses de test de performances CIS	97
Ajout ou édition d'un profil d'actif.	98
Configuration d'un jeu de données d'identification	102
Sauvegarde des critères de recherche d'un actif	102
Edition d'un test de performances de conformité	103
Création d'un profil de test de performances	103
Création d'une question de conformité d'actif.	104
Surveillances des questions de conformité d'actif	105
Affichage des résultats d'analyse	105
12 Gestion des règles.	107
13 Simulations réseau dans IBM Security QRadar Risk Manager	109
Simulations	109
Création d'une simulation	110
Edition d'une simulation	113
Duplication d'une simulation	113
Suppression d'une simulation	113
Exécution manuelle d'une simulation	113
Simulation d'un changement de configuration réseau	114
Création d'un modèle de topologie	114
Simulation d'une attaque	115
Simulation d'une attaque sur un protocole SSH	115
Gestion des résultats de simulations	116
Affichage des résultats de simulations	116
Approbation des résultats de simulations	118
Révocation de l'approbation de simulations	118
Surveillance des simulations	119
Regroupement de simulations	120
14 Modèles de topologie	121
Création d'un modèle de topologie	121
Edition d'un modèle de topologie	124
Duplication d'un modèle de topologie	124
Suppression d'un modèle de topologie	124
Modèles de topologie de groupe	124
Affichage des groupes	125
Création d'un groupe.	125
Edition d'un groupe	125
Copie d'un élément dans un autre groupe.	126
Affectation d'une topologie à un groupe	126
Suppression d'un élément d'un groupe	126
15 Gestion des rapports IBM Security QRadar Risk Manager	127
Production manuelle d'un rapport	127
Utilisez l'assistant du rapport	128
Création d'un rapport	128
Edition d'un rapport	130
Duplication d'un rapport	131
Partage d'un rapport	132

Configuration des graphiques	132
Graphiques de connexion	132
Graphiques Règles du périphérique	135
Graphiques Objets non utilisés du périphérique	139
16 Données de journaux d'audit	141
Actions consignées	141
Affichage de l'activité d'utilisateur	142
Affichage du fichier journal	143
Détails du fichier journal	144
Remarques	145
Marques	146
Dispositions relatives à la documentation du produit	147
Déclaration IBM de confidentialité en ligne	147
Glossaire	149
A	149
C	149
D	149
G	149
I	149
L	150
M	150
N	150
P	150
R	150
T	150
V	150
Index	151

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 être utilisées avec IBM® Security QRadar Risk Manager. QRadar Risk Manager est un dispositif utilisé pour contrôler les configurations de périphérique, simuler les modifications du réseau et hiérarchiser les risques et les vulnérabilités du réseau.

Ce manuel contient des instructions de configuration et d'utilisation d'IBM Security QRadar Risk Manager dans une console IBM Security QRadar SIEM.

Utilisateurs concernés

Les administrateurs système chargés de configurer et d'utiliser QRadar Risk Manager doivent disposer de droits d'accès d'administrateur sur IBM Security QRadar SIEM et sur les périphériques réseau et les pare-feux. L'administrateur système doit connaître les technologies de réseau d'entreprise et de mise en réseau.

Documentation technique

Pour plus d'informations sur l'accès à une documentation plus technique, à des notes techniques et à des notes sur l'édition, voir la note technique Accessing IBM Security Documentation (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

Contactez le service clients

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

Instructions relatives aux bonnes pratiques de sécurité

La sécurité 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. Un accès non autorisé peut se traduire par la modification, la destruction ou le détournement d'informations, ou une utilisation inadéquate ou malveillante de vos systèmes, y compris l'utilisation de ces derniers pour attaquer d'autres systèmes. Aucun système ou produit informatique ne doit être considéré comme étant complètement sécurisé et aucun produit, service ou mesure de sécurité ne peut être entièrement efficace contre une utilisation ou un accès non autorisé. 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'IMMUNITÉ DES SYSTÈMES, PRODUITS OU SERVICES NI L'IMMUNITÉ DE VOTRE ENTREPRISE CONTRE LES CONDUITES MALVEILLANTES OU ILLICITES DE TIERS.**

1 Nouveautés de QRadar Risk Manager version 7.3.1


IBM Security QRadar Risk Manager V7.3.1 migre des fonctions de Configuration Source Management vers le Moniteur de configuration et améliore les vues et recherches topologiques.

QRadar Risk Manager - Migration de Configuration Source Management vers le Moniteur de configuration

Plusieurs fonctions sont migrées de Configuration Source Management vers le Moniteur de configuration : ajout d'un périphérique, suppression d'un périphérique, sauvegarde d'un périphérique et reconnaissance de périphériques dans le Moniteur de configuration. Cette migration est en cours de préparation en vue de la suppression par Google Chrome de la prise en charge complète d'Adobe Flash et constitue la première étape du processus de suppression de la dépendance Flash de QRadar Risk Manager .

 En savoir plus sur les fonctions de QRadar Vulnerability Manager dans le Moniteur de configuration...


 En savoir plus sur la reconnaissance de périphériques dans QRadar Vulnerability Manager...

 En savoir plus sur l'activité récente dans QRadar Vulnerability Manager...

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

Vues et recherches topologiques QRadar Risk Manager améliorées

Chaque recherche topologique ouvre une vue avec onglets et les résultats sont mis en cache pour améliorer la récupération de topologie, ce qui réduit le temps de traitement.

 En savoir plus sur les recherches topologiques de QRadar Risk Manager...

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

2 IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager est un dispositif installé séparément pour surveiller les configurations de périphérique, simuler les modifications dans votre environnement de réseau et hiérarchiser les risques et les vulnérabilités dans votre réseau.

Vous pouvez accéder à QRadar Risk Manager en utilisant l'onglet **Risques** de IBM Security QRadar SIEM Console.

QRadar Risk Manager utilise les données collectées par QRadar. Par exemple, les données de configuration provenant des pare-feux, des routeurs, des commutateurs, des systèmes de prévention des intrusions (IPS), des fils de vulnérabilité et de sources de sécurité tierces. Les sources de données permettent à QRadar Risk Manager d'identifier les risques de sécurité, de règles et de compatibilité dans votre réseau et d'estimer la probabilité de l'exploitation des risques.

QRadar Risk Manager vous avertit des risques détectés en affichant les infractions sur l'onglet **Infractions**. Les données de risque sont analysées et font l'objet d'un rapport dans le contexte de toutes les autres données traitées par QRadar. Dans QRadar Risk Manager, vous pouvez évaluer et gérer les risques à un niveau acceptable dépendant de la tolérance aux risques de votre société.

Vous pouvez également utiliser QRadar Risk Manager pour interroger toutes les connexions réseau, comparer les configurations de périphérique, filtrer la topologie réseau et simuler les effets possibles de la mise à jour des configurations de périphérique.

Vous pouvez utiliser QRadar Risk Manager pour définir un ensemble de règles (ou de questions) pour votre réseau et surveiller les modifications des règles. Par exemple, si vous souhaitez refuser des protocoles non chiffrés dans votre zone démilitarisée à partir d'Internet, vous pouvez définir une question de surveillance des règles pour détecter les protocoles non chiffrés. L'envoi de la question renvoie une liste des protocoles non chiffrés qui communiquent entre Internet et votre zone démilitarisée, et vous pouvez déterminer les protocoles non chiffrés qui représentent des risques de sécurité.

Navigateurs Web pris en charge

Pour que les fonctions des produits IBM Security QRadar fonctionnent correctement, vous devez utiliser un navigateur Web pris en charge.

Le tableau ci-après répertorie les versions de navigateurs web pris en charge.

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

Navigateur Web	Versions prises en charge
Mozilla Firefox	45.8 Extended Support Release
Microsoft Internet Explorer 64 bits avec le mode Microsoft Edge activé.	11.0, Edge 38.14393
Google Chrome	Latest

Activation du mode document et du mode navigateur dans Internet Explorer

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

Procédure

1. Dans votre navigateur Web Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre des Developer Tools.
2. Cliquez sur **Mode navigateur** et sélectionnez la version de votre navigateur Web.
3. Cliquez sur **Mode document** et sélectionnez l'option **Standards Internet Explorer** correspondant à votre version d'Internet Explorer.

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

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

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

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

Informations de connexion	Default
URL	https://<Adresse IP>, où<Adresse IP> est l'adresse IP de QRadar Console.
Nom d'utilisateur	admin
Mot de passe	Mot de passe attribué à QRadar Risk Manager lors du processus d'installation.
Clé de licence	Une clé de licence par défaut offre un accès au système pendant 5 semaines.

Fonctions non prises en charge dans IBM Security QRadar Risk Manager

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

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

- Haute disponibilité(HA)
- Routage dynamique pour protocole BGP
- IPv6
- Masques de réseau non contigus
- Routages à équilibrage de charge

3 Présentation des fonctions de QRadar Risk Manager

Utilisez les fonctions de QRadar Risk Manager pour gérer les risques au sein de votre réseau, surveiller les configurations des unités, afficher les topologies, simuler des modifications apportées à votre environnement de réseau et hiérarchiser les risques et les vulnérabilités dans votre réseau.

La liste suivante est une présentation des fonctions offertes par QRadar Risk Manager à des fins de surveillance et de gestion des risques dans votre réseau.

Connexions

Utilisez la fonction Connexions pour surveiller les connexions réseau de vos hôtes locaux.

Le graphique des connexions fournit une représentation visuelle des connexions dans votre réseau.

A l'aide des graphiques de série temporelle, accédez, naviguez et analysez les connexions de divers points de vue et perspectives.

Exécutez les requêtes et les rapports sur les connexions réseau de vos hôtes locaux en fonction des applications, ports, protocoles et sites Web avec lesquels les hôtes locaux peuvent communiquer.

Moniteur de configuration

Utilisez le moniteur de configuration pour examiner et comparer les configurations, gérer les règles de sécurité et surveiller les modifications apportées aux unités dans votre réseau. Les configurations d'unité peuvent concerner les commutateurs, les routeurs, les pare-feux et les unités IPS de votre réseau. Pour chaque unité, vous pouvez afficher l'historique de configuration d'unité, les interfaces et les règles.

Vous pouvez également comparer les configurations d'une ou de plusieurs unités afin d'identifier les incohérences et les changements de configuration introduisant un risque dans votre réseau.

Topologie

La topologie est une représentation graphique qui illustre l'infrastructure physique et la connectivité de votre topologie réseau à 3 couches. La topologie est issue des informations de configuration importées depuis les unités de votre réseau à l'aide de la gestion source de configuration.

Le graphique est créé à partir des informations de configuration détaillées obtenues auprès des unités réseau, telles que les pare-feu, les routeurs, les commutateurs et les systèmes de prévention d'intrusion.

Utilisez le graphique interactif dans la topologie pour visualiser les connexions entre les unités.

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 le chemin entre une source et une destination, ainsi que les ports, les protocoles et les règles.

Moniteur de politique d'administration

Le moniteur de politique d'administration permet de définir des questions spécifiques sur les risques dans votre réseau, puis d'envoyer une question à IBM Security QRadar Risk Manager.

QRadar Risk Manager évalue les paramètres que vous avez définis dans la question et renvoie les actifs de votre réseau afin de vous aider à évaluer les risques. Les questions sont basées sur une série de tests pouvant être combinés et configurés si nécessaire. QRadar Risk Manager propose un grand nombre de questions prédéfinies. Vous pouvez toutefois créer vos propres questions personnalisées. Vous pouvez créer des questions de moniteur de politique d'administration pour les situations suivantes :

- Communications établies
- Communications possibles basées sur la configuration des pare-feux ou des routeurs
- Règles de pare-feu réelles (tests d'unité)

Le moniteur de politique d'administration utilise les données provenant des données de configuration, des données d'activité de réseau, des événements de réseau et de sécurité et des données d'analyse des vulnérabilités pour déterminer la réponse adéquate. QRadar Risk Manager dispose de modèles de règles pour vous aider à identifier les risques encourus par de nombreux mandats réglementaires et meilleures pratiques de sécurité des informations, tels que PCI, HIPPA et ISO 27001. Vous pouvez mettre à jour les modèles pour les adapter à votre politique de sécurité informatique d'entreprise. Une fois la réponse traitée, vous pouvez accepter la réponse à la question et définir la façon dont vous souhaitez que le système réponde aux résultats non validés.

Vous pouvez surveiller de manière active un nombre illimité de questions dans le moniteur de politique d'administration. Lorsqu'une question est surveillée, QRadar Risk Manager évalue en continu la question en attente de résultats non approuvés. Lorsque des résultats non approuvés sont détectés, QRadar Risk Manager peut être configuré pour envoyer des notifications par e-mail, afficher des notifications, générer un événement syslog ou créer une infraction dans IBM Security QRadar SIEM.

Gestion des règles

Vous utilisez les pages de gestion des règles QRadar Risk Manager pour consulter les détails relatifs aux modifications de conformité aux règles et de risques liés aux règles pour les actifs, les règles et les vérifications de règles.

Les pages de gestion des règles QRadar Risk Manager affichent les données de la dernière règle exécutée. Vous pouvez filtrer les données par actif, par règle ou par vérification de règle.

Simulation

Les simulations permettent de créer des simulations réseau.

Vous pouvez créer une simulation d'attaque sur votre topologie en vous basant sur une série de paramètres configurés de manière identique au moniteur de politique d'administration. Vous pouvez créer une attaque simulée sur votre topologie de réseau actuelle ou créer un modèle de topologie.

Simulez une attaque à l'aide d'un modèle de topologie dans lequel vous pouvez apporter des modifications sans aucune répercussion sur le réseau opérationnel.

Vous pouvez simuler la façon dont les modifications apportées aux règles de réseau, aux ports, aux protocoles ou aux connexions autorisées ou refusées peuvent affecter votre réseau. La fonction de simulation permet de déterminer l'impact des risques des changements à apporter à votre configuration réseau avant que vous ne les implémentiez.

Vous pouvez examiner les résultats à l'issue de la simulation.

IBM Security QRadar Risk Manager autorise la surveillance active de 10 simulations au maximum. Lorsqu'une simulation est surveillée, QRadar Risk Manager analyse en continu la topologie en attente de résultats non approuvés. Lorsque des résultats non approuvés sont détectés, QRadar Risk Manager peut

envoyer des e-mails, afficher des notifications, générer un événement syslog ou créer une infraction dans QRadar SIEM.

Configuration Source Management

Configurez **Configuration Source Management** pour extraire des informations de configuration d'unité depuis les unités de votre réseau et fournir à QRadar Risk Manager les données dont il a besoin pour gérer les risques dans votre réseau. Utilisez ces informations de configuration pour générer la topologie associée à la configuration de votre réseau.

Rapports

L'onglet **Rapports** permet de créer des rapports spécifiques d'après les données disponibles dans QRadar Risk Manager, telles que les connexions, les règles d'unités et les objets d'unité inutilisés.

Les rapports détaillés suivants sont également disponibles :

- Connexions entre unités
- Règles de pare-feu sur une unité
- Objets non utilisés sur une unité

4 Configuration de l'accès à QRadar Risk Manager

Vous pouvez configurer les paramètres d'accès pour QRadar Risk Manager dans l'onglet **Admin** de IBM Security QRadar SIEM. Lorsque vous ajoutez QRadar Risk Manager à votre déploiement, vous devez configurer des paramètres, comme le pare-feu local, les interfaces réseau, le serveur de messagerie et ajouter la licence appropriée.

Si vous disposez des droits d'administrateur, vous pouvez configurer plusieurs paramètres de dispositif pour QRadar Risk Manager.

En tant qu'administrateur, vous pouvez effectuer les tâches suivantes :

- Depuis la fenêtre Gestion du système et de la licence, vous pouvez gérer les licences, configurer le pare-feu local et ajouter un serveur de messagerie, puis configurer les interfaces réseau de QRadar Risk Manager.
- Vous pouvez changer le mot de passe d'un hôte.
- Vous pouvez mettre à jour l'heure système.

Configuration des paramètres système

Pour que votre système de sécurité QRadar soit opérationnel ou pour gérer votre système, vous devez configurer QRadar Console et les paramètres système des hôtes gérés depuis la fenêtre Informations système.


Pourquoi et quand exécuter cette tâche

Vous pouvez affecter des rôles pour les interfaces réseau, les interfaces de liaison, la gestion des licences et la configuration du serveur de messagerie associé à QRadar, puis utiliser le pare-feu local pour gérer l'accès des unités externes vers QRadar.

Si vous devez effectuer des modifications de configuration, comme le changement d'une adresse IP sur votre console QRadar Console et les systèmes hôtes gérés après l'installation du déploiement QRadar, utilisez l'utilitaire **qchange_netsetup**. Pour plus d'informations sur les paramètres réseau, voir le manuel *IBM Security QRadar Risk Manager - Guide d'installation*.

Si vous modifiez le paramètre **Port de surveillance de source de flux externe** dans la configuration QFlow, vous devez également mettre à jour la configuration d'accès de votre pare-feu.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Configuration système**.
3. Cliquez sur l'icône **Gestion du système et de la licence**.
4. Dans le menu **Afficher**, sélectionnez **Systèmes**.
5. Sélectionnez l'hôte pour lequel vous souhaitez configurer les paramètres d'accès au pare-feu.
6. Dans le menu **Actions**, cliquez sur **Afficher et gérer le système**.

Remarque : Vous pouvez cliquer avec le bouton droit de la souris sur l'hôte sélectionné afin d'accéder à cette option de menu, ou vous pouvez cliquer deux fois sur l'hôte pour ouvrir la fenêtre Informations système.

7. Pour configurer votre pare-feu local afin qu'il autorise l'accès à cet hôte depuis les appareils spécifiés en dehors de votre déploiement QRadar, cliquez sur l'onglet **Pare-feu**.

- a. Configurez l'accès pour les appareils qui se trouvent à l'extérieur de votre déploiement et qui doivent se connecter à cet hôte.
 - b. Pour ajoutez cette règle d'accès, cliquez sur la flèche.
8. Pour configurer les interfaces réseau sur votre système QRadar, cliquez sur l'onglet **Interfaces réseau**.
- a. Sélectionnez une interface réseau dans la colonne **Périphérique**.
 - b. Pour modifier vos interfaces réseau, cliquez sur **Editer**, puis configurez les paramètres.
 - c. Pour lier les interfaces réseau, cliquez sur l'option de **liaison**, puis configurez les paramètres.
- Pour plus d'informations sur la configuration des interfaces réseau, voir le manuel *IBM Security QRadar Administration Guide*.
- Vous ne pouvez pas éditer une interface réseau ayant un rôle Gestion, Croisé haute disponibilité ou Esclave.
9. Pour configurer un serveur de messagerie qui distribuera les alertes, les rapports, les notifications et les messages d'événement, cliquez sur l'onglet **Serveur de messagerie**.
- a. Dans la zone **Adresse du serveur de messagerie**, entrez le nom d'hôte ou l'adresse IP du serveur de messagerie que vous voulez utiliser.
- Si vous ne disposez pas d'un serveur de messagerie et si vous voulez utiliser le serveur de messagerie fourni par QRadar, entrez localhost pour indiquer le traitement d'e-mail local. Si vous définissez le paramètre de serveur de messagerie sur localhost, les e-mails ne quittent pas la boîte de QRadar. Si vous voulez que la livraison des e-mails externes puisse s'effectuer, vous devez utiliser un serveur relais de messagerie valide.
- Remarque :** Il est recommandé d'utiliser le port 25 pour la connexion au serveur de messagerie.
10. Cliquez sur **Sauvegarder**.


Mise à jour de l'heure système

Configurez l'heure système dans l'interface utilisateur QRadar Console, soit manuellement, soit à l'aides des serveurs NTP. QRadar Console synchronise son heure système avec les hôtes gérés de votre déploiement.

Pourquoi et quand exécuter cette tâche

Configurez le paramétrage de l'heure dans QRadar Console.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
 2. Cliquez sur **Configuration système**.
 3. Cliquez sur l'icône **Gestion du système et de la licence**.
 4. Dans le menu **Afficher**, sélectionnez **Systemes**.
 5. Sélectionnez l'hôte dont vous souhaitez configurer les paramètres d'heure système.
 6. Dans le menu **Actions**, sélectionnez **Afficher et gérer le système**.
 7. Cliquez sur l'onglet **Heure système**.
 8. Sélectionnez un fuseau horaire dans le menu **Fuseau horaire**.
- Le fuseau horaire ne peut être configuré que sur un hôte géré. L'heure système est synchronisée avec QRadar Console, mais si l'hôte géré est dans un autre fuseau horaire, vous pouvez choisir celui-ci.
9. Pour configurer manuellement l'heure système, cliquez sur le bouton d'option **Définir l'heure manuellement** : et définissez une date et une heure.

Exceptions :

Si vous définissez l'heure système sur une date qui est concernée par l'heure d'été, l'heure saisie est modifiée d'une heure. Ainsi, si le 4 juillet 2016, aux Etats-Unis, vous définissez l'heure et la date sur 20:00 le 16 décembre 2016, l'heure d'été n'est pas prise en compte et l'heure devient 19:00.

L'heure définie sur un système VMware peut être perdue lors du redémarrage du système. Pour empêcher la perte de la modification de l'heure système, vous pouvez éditer le fichier .vmx sur le périphérique virtuel et désactiver la synchronisation d'horloge en ajoutant les lignes suivantes aux propriétés de synchronisation :

```
tools.syncTime = "FALSE"
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
```

10. Pour configurer l'heure à l'aide des serveurs NTP, cliquez sur le bouton d'option **Serveurs de temps NTP**.
 - a. Entrez l'adresse IP ou le nom d'hôte du serveur NTP dans la zone **Adresse du serveur 1**.
Les noms d'hôte sont résolus par un serveur DNS.
 - b. Pour ajouter des serveurs NTP, cliquez sur l'icône plus en regard de **Ajouter plus**.
11. Cliquez sur **Sauvegarder**.
12. Cliquez sur **OK** pour accepter le redémarrage des services, ou sur **Annuler** pour annuler les modifications.
Les services redémarrés comprennent hostcontext et tomcat.

5 Configuration Source Management

Vous utilisez Configuration Source Management pour configurer des données d'identification, ajouter ou découvrir des périphériques, afficher des configurations de périphériques et sauvegarder des configurations de périphériques dans IBM Security QRadar Risk Manager.

Les données provenant de périphériques dans votre réseau sont utilisées pour remplir la topologie. Vous devez disposer de privilèges d'administrateur pour accéder aux fonctions de Configuration Source Management à partir de l'onglet **Admin** de IBM Security QRadar SIEM.

Pour configurer les sources de configuration, vous devez :

1. Configurez les données d'identification de votre périphérique.
2. Activez la reconnaissance ou l'importation des périphériques. Il existe deux manières d'ajouter des périphériques réseau à QRadar Risk Manager : utiliser la reconnaissance de périphérique à l'aide de Configuration Source Management ou importer une liste de périphériques à partir d'un fichier CSV à l'aide de la fonction Importation d'unité.
3. Obtenez la configuration de périphérique pour chacun de vos périphériques.
4. Gérez les tâches de sauvegarde pour vous assurer que toutes les mises à jour des configurations de périphériques sont capturées.
5. Configurez la planification de reconnaissance pour vous assurer que les nouveaux périphériques sont automatiquement découverts.

Vous pouvez utiliser Configuration Source Management pour :

- Ajouter, éditer, rechercher et supprimer les sources de configuration. Pour plus d'informations, voir Gestion des périphériques.
- Configurer ou gérer les protocoles de communication pour vos périphériques. Pour plus d'informations, voir Configuration de protocoles.

Si vous utilisez le périphérique Juniper NSM, vous devez également obtenir des informations de configuration.

Pour obtenir des informations détaillées sur les adaptateurs utilisés pour communiquer avec les périphériques de fabricants spécifiques, voir *IBM Security QRadar Risk Manager Adapter - Guide de configuration*.

Données d'identification

Dans IBM Security QRadar Risk Manager, les données d'identification sont utilisées pour accéder à la configuration de périphériques tels que les pare-feux, les routeurs, les commutateurs ou les IPS.

Les administrateurs font appel à la gestion source de configuration pour saisir les données d'identification des périphériques afin que QRadar Risk Manager puisse accéder aux unités spécifiques. Les données de périphérique individuelles peuvent être sauvegardées pour un périphérique de réseau spécifique. Si plusieurs périphériques réseau utilisent les mêmes données d'identification, vous pouvez les affecter à un groupe de périphériques.

Vous pouvez affecter plusieurs unités de votre réseau à des groupes du réseau, afin d'unifier les ensembles de données d'identification et les ensembles d'adresses de vos unités.

Un jeu de données d'identification contient des valeurs telles que le nom d'utilisateur et le mot de passe d'un ensemble d'unités.

Un ensemble d'adresses est une liste d'adresses IP définissant un groupe d'unités qui partagent le même ensemble de données d'identification.

Par exemple, si tous les pare-feux de l'entreprise disposent des mêmes nom d'utilisateur et mot de passe, ces données d'identification associées aux ensembles d'adresses de tous les pare-feux sont utilisées pour sauvegarder les configurations d'unité de tous les pare-feux de l'entreprise.

S'il n'est pas nécessaire d'avoir des données d'identification de réseau pour une unité spécifique, le paramètre peut rester vide dans Configuration Source Management. Pour une liste des informations d'identification requises de l'adaptateur, voir le *IBM Security QRadar Risk Manager Adapter - Guide de configuration*.

Vous pouvez configurer QRadar Risk Manager pour hiérarchiser le mode d'évaluation de chaque groupe réseau.

Le groupe du réseau en haut de la liste possède la priorité la plus élevée. Le premier groupe du réseau correspondant à l'adresse IP configurée est intégré en tant que candidat lors de la sauvegarde d'un périphérique. Un maximum de trois ensembles de données d'identification provenant d'un groupe du réseau est pris en compte.

Par exemple, si la composition de vos groupes du réseau est la suivante :

- Le groupe du réseau 1 comprend deux ensembles de données d'identification
- Le groupe du réseau 2 comprend deux ensembles de données d'identification

QRadar Risk Manager compile trois ensembles de données d'identification au maximum, de sorte que les ensembles suivants soient utilisés :

- Les deux ensembles de données d'identification dans le groupe du réseau 1 sont utilisés, car le groupe du réseau 1 figure plus haut dans la liste.
- Seul le premier ensemble de données d'identification dans le groupe du réseau 2 est utilisé, car trois ensembles de données d'identification maximum sont requis.

Lorsqu'un ensemble de données d'identification est utilisé pour accéder à une unité, QRadar Risk Manager utilise cet ensemble pour les tentatives suivantes d'accès à cette unité. Si les données d'identification associées à cette unité sont modifiées, l'authentification échoue et lors de la prochaine tentative d'authentification, QRadar Risk Manager compile de nouveau les données d'identification afin de garantir le succès de l'opération.


Configuration des données d'identification pour IBM Security QRadar Risk Manager

Les administrateurs doivent configurer les données d'identification pour permettre à IBM Security QRadar Risk Manager de se connecter à des périphériques dans le réseau.

Pourquoi et quand exécuter cette tâche

Vous pouvez entrer une plage d'adresses IP à l'aide d'un tiret ou indiquer une plage à l'aide du caractère générique (*). Par exemple, 10.100.20.0-10.100.20.240 ou 1.1.1.*. Si vous entrez 1.1.1.*, toutes les adresses IP répondant à cette exigence sont incluses.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Dans le menu de navigation, cliquez sur **Credentials**.

5. Dans la sous-fenêtre **Network Groups**, cliquez sur l'icône **Ajouter (+)**.
6. Entrez le nom d'un groupe du réseau, puis cliquez sur **OK**.
7. Déplacez en haut de la liste le groupe du réseau auquel vous souhaitez affecter la première priorité. Vous pouvez utiliser les icônes en forme de flèche **Vers le haut** et **Vers le bas** pour définir la priorité d'un groupe du réseau.
8. Dans la zone **Add Address**, entrez l'adresse IP ou la plage CIDR que vous souhaitez appliquer au groupe du réseau, puis cliquez sur l'icône **Ajouter (+)**.
Répétez cette procédure pour toutes les adresses IP à ajouter à l'ensemble d'adresses de ce groupe du réseau.
9. Dans la sous-fenêtre **Credentials**, cliquez sur l'icône **Ajouter (+)**.
10. Entrez le nom du nouveau jeu de données d'identification, puis cliquez sur **OK**.
11. Entrez les valeurs pour les paramètres :

Option	Description
Username	Entrez le nom d'utilisateur du jeu de données d'identification.
Password	Entrez le mot de passe du jeu de données d'identification.
Enable Username	Entrez le nom d'utilisateur de l'authentification de second niveau du jeu de données d'identification.
Enable Password	Entrez le mot de passe de l'authentification de second niveau du jeu de données d'identification.
SNMP Get Community	Entrez la communauté SNMP Get.
SNMPv3 Authentication Username	Entrez le nom d'utilisateur que vous souhaitez utiliser pour authentifier SNMPv3.
SNMPv3 Authentication Password	Entrez le mot de passe que vous souhaitez utiliser pour authentifier SNMPv3.
SNMPv3 Privacy Password	Entrez le protocole que vous souhaitez utiliser pour déchiffrer les alertes SNMPv3.

12. Déplacez en haut de la liste le jeu de données d'identification auquel vous souhaitez affecter la première priorité. Utilisez les icônes en forme de flèche **Vers le haut** et **Vers le bas** pour définir la priorité d'un jeu de données d'identification.
13. Répétez la procédure pour chaque jeu de données d'identification à ajouter.
14. Cliquez sur **OK**.

Reconnaissance d'unité

Le processus de reconnaissance utilise le protocole SNMP et la ligne de commande (CLI) pour reconnaître les unités réseau.

Une fois que vous avez configuré une adresse IP ou une plage CIDR, le moteur de reconnaissance effectue une analyse TCP en fonction de l'adresse IP afin de déterminer si le port 22, 23 ou 443 surveille les connexions. Si l'analyse TCP aboutit et que la requête SNMP est configurée pour déterminer le type d'unité, la fonction SNMP Get Community String est utilisée en fonction de l'adresse IP.

Ces informations sont utilisées pour déterminer vers quel adaptateur l'unité doit être mappée lors de l'ajout IBM Security QRadar Risk Manager se connecte à l'unité et collecte une liste d'informations relatives aux interfaces et voisinage, par exemple, les tables CDP, NDP ou ARP. L'unité est ensuite ajoutée à l'inventaire.

L'adresse IP configurée utilisée pour lancer le processus de reconnaissance peut ne pas être l'adresse IP affectée pour la nouvelle unité. QRadar Risk Manager ajoute une unité à l'aide de l'adresse IP de l'interface la plus faiblement numérotée sur l'unité (ou l'adresse de bouclage la plus faible, le cas échéant).

Si vous utilisez la case à cocher **Crawl the network from the addresses defined above**, l'adresse IP des voisins collectée à partir de l'unité est réintroduite dans le processus de reconnaissance et le processus se répète pour chaque adresse IP.


Reconnaissance des unités

Les utilisateurs utilisent la reconnaissance d'unités pour déterminer le type de périphérique.

Pourquoi et quand exécuter cette tâche

Lors d'une reconnaissance de périphérique, tout périphérique non pris en charge, mais répondant au protocole SNMP est ajouté à l'adaptateur SNMP générique. Si vous souhaitez exécuter un filtrage de chemin dans le périphérique avec des routes simulées, vous devez supprimer manuellement le périphérique

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Configurez le protocole SNMP et ajoutez l'adresse IP ou la plage du routage CIDR des unités que vous souhaitez reconnaître.
 - a. Dans le menu de navigation, cliquez sur **Protocols**.
 - b. Dans le panneau Network Groups, cliquez sur le symbole (+) .
 - c. Entrez un nom pour le groupe du réseau.
 - d. Cliquez sur **OK**.
 - e. Dans la zone **Add address (IP, CIDR, Wildcard, or Range)**, entrez l'adresse IP ou la plage du routage CIDR.
 - f. Cliquez sur (+) pour ajouter l'adresse IP ou la plage du routage CIDR.
 - g. Sélectionnez le protocole **SNMP**.
 - h. Cliquez sur **OK**.
5. Dans le menu de navigation, cliquez sur **Discover Devices**.
6. Entrez une adresse IP ou une plage CIDR.

Cette adresse IP ou cette plage CIDR indique l'emplacement des périphériques à reconnaître.
7. Cliquez sur l'icône **Ajouter (+)**.
8. Si vous souhaitez également rechercher des périphériques dans le réseau à partir de l'adresse IP ou de la plage CIDR définie, cochez la case **Crawl the network from the addresses defined above**.
9. Cliquez sur **Run**.

Importation de périphériques

Utilisez Importation d'unité pour ajouter une liste d'adaptateurs et de leurs adresses IP sur le réseau au gestionnaire de sources de configuration. La liste doit être au format .CSV.

La liste d'importation de périphérique peut contenir jusqu'à 5000 périphériques, mais cette liste doit contenir une seule ligne pour chaque adaptateur et son adresse IP associée dans le fichier d'importation.

Par exemple,

<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>

Où :

<Adapter::Name> contient le nom du fabricant et du périphérique tel que Cisco::IOS.

<IP Address> contient l'adresse IP du périphérique telle que 191.168.1.1.

Tableau 3. Exemples d'importation de périphériques

Manufacturer	Nom	Example <Adapter::Name>,<IP Address>
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 maîtresse de périphériques dans l'outil de Gestion de source de configuration à l'aide d'un fichier au format CSV.

Avant de commencer

Si vous importez une liste de périphériques puis modifiez une adresse IP dans le fichier CSV, vous risquez de dupliquer accidentellement un périphérique dans la liste Configuration Source Management. Pour cette raison, supprimez le périphérique dans Configuration Source Management avant de réimporter votre liste maîtresse de périphériques.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Applications**, cliquez sur **Importation d'unité**.
4. Cliquez sur **Parcourir**.
5. Localisez votre fichier CSV, puis cliquez sur **Ouvrir**.
6. Cliquez sur **Importer les unités**.

Résultats

Si une erreur survient, vous devez réviser votre fichier CSV afin de corriger les erreurs puis réimporter le fichier. L'importation d'une liste de périphériques au format CSV peut échouer si elle ne dispose pas d'une structure correcte ou si elle contient des informations incorrectes. Par exemple, des points-virgules ou une commande peuvent manquer dans le fichier CSV, une ligne du fichier peut contenir plusieurs périphériques ou le nom d'un adaptateur peut contenir une erreur.

Si l'importation de périphérique est interrompue, aucun périphérique du fichier CSV n'est ajouté à Configuration Source Management.

Gestion des unités


L'onglet **Devices** de la fenêtre **Configuration Source Management** vous permet de gérer les périphériques de votre réseau.

Dans l'onglet **Devices**, vous pouvez afficher, ajouter, modifier et supprimer des périphériques. Vous pouvez également filtrer la liste des périphériques, obtenir des informations sur leur configuration, collecter des données voisines et reconnaître les périphériques de votre déploiement.

Affichage des unités

Vous pouvez afficher toutes les unités de votre déploiement sous l'onglet **Devices**.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Devices**.
5. Pour afficher des informations détaillées sur une configuration de périphérique, sélectionnez le périphérique à afficher et cliquez sur **Open**.

Ajout d'un périphérique


Permet d'ajouter des périphériques réseau et des adaptateurs individuels à l'aide de **Configuration Source Management**.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter un périphérique individuel à la liste de périphériques de **Configuration Source Management** ou vous pouvez ajouter plusieurs périphériques à l'aide d'un fichier CSV.

Pour plus d'informations sur l'ajout de plusieurs périphériques, voir **Importation de périphériques**.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Dans la sous-fenêtre de navigation, cliquez sur **Add Device**.
5. Configurez les valeurs des paramètres suivants :


Option	Description
IP Address	Entrez l'adresse IP de gestion du périphérique.
Adapter	Dans la liste déroulante Adapter , sélectionnez l'adaptateur que vous souhaitez affecter à ce périphérique.

6. Cliquez sur **Add**.
Le cas échéant, cliquez sur **Go** pour actualiser la liste des adaptateurs.

Modification des unités

Vous pouvez éditer un périphérique pour corriger l'adresse IP ou le type d'adaptateur en cas d'erreur ou si votre réseau a changé et que vous devez réaffecter une adresse IP.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Sélectionnez l'unité que vous souhaitez éditer.
5. Cliquez sur **Edit**.
6. Configurez les valeurs des paramètres suivants :


Option	Description
IP Address	Entrez l'adresse IP de gestion de l'unité.
Adapter	Dans la liste déroulante Adapter , sélectionnez l'adaptateur que vous souhaitez affecter à cette unité.

7. Cliquez sur **Save**.

Suppression d'une unité

Vous pouvez supprimer un périphérique d'IBM Security QRadar Risk Manager. Un périphérique supprimé l'est aussi de Configuration Source Management, du moniteur de configuration et de la topologie.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Devices**.
5. Sélectionnez le périphérique à supprimer.
6. Cliquez sur **Remove**.
7. Cliquez sur **Yes** pour supprimer le périphérique.

Résultats

Une fois le périphérique supprimé, son retrait de la topologie peut prendre quelques minutes.

Filtrage de la liste d'unités

Vous pouvez utiliser des filtres pour rapidement trouver des périphériques dans la liste de périphériques.

Pourquoi et quand exécuter cette tâche

IBM Security QRadar Risk Manager peut gérer 5000 périphériques réseau dans Configuration Source Management. Les grands nombres de périphériques réseau peuvent rendre l'exploration de la liste de périphériques fastidieuse.

Le tableau suivant contient les types de filtres qui peuvent être appliqués à la liste de périphériques pour vous aider à rapidement trouver des périphériques.

Tableau 4. Types de filtres pour la liste d'unités

Option de recherche	Description
Interface IP Address	<p>Filtres des périphériques possédant une interface correspondant soit à une adresse IP, soit à une plage CIDR.</p> <p>Entrez l'adresse IP ou la plage CIDR sur laquelle vous souhaitez rechercher dans la zone IP/CIDR.</p> <p>Par exemple, si vous saisissez un critère de recherche 10.100.22.6, les résultats de la recherche renvoient un périphérique présentant une adresse IP 10.100.22.6. Si vous entrez une plage CIDR 10.100.22.0/24, tous les périphériques de 10.100.22.* sont renvoyés.</p>
Admin IP Address	<p>Filtre la liste de périphériques en fonction de l'adresse IP de l'interface d'administration. Une adresse IP administrative est l'adresse IP qui identifie de manière unique un périphérique.</p> <p>Entrez l'adresse IP ou la plage CIDR sur laquelle vous souhaitez rechercher dans la zone IP/CIDR.</p>
OS Version	<p>Filtre la liste de périphériques en fonction de la version de système d'exploitation sur laquelle les périphériques sont exécutés.</p> <p>Sélectionnez les valeurs pour les paramètres suivants :</p> <p>Adapter - Dans la liste déroulante, sélectionnez le type d'adaptateur que vous souhaitez rechercher.</p> <p>Version - Dans la liste déroulante, sélectionnez les critères de recherche de la version. Par exemple, supérieure à, inférieure à, égale à la valeur spécifiée. Entrez le numéro de version dans la zone dans laquelle vous souhaitez effectuer la recherche. Si vous ne sélectionnez pas d'option de recherche pour la version, les résultats contiennent tous les périphériques configurés avec l'adaptateur sélectionné, quelle que soit la version.</p>
Model	<p>Filtre la liste de périphériques en fonction du fournisseur et du numéro de modèle.</p> <p>Configurez les valeurs des paramètres suivants :</p> <p>Vendor - Dans la liste déroulante, sélectionnez le fournisseur que vous souhaitez rechercher.</p> <p>Model - Entrez le modèle que vous souhaitez rechercher.</p>
Hostname	<p>Filtre la liste de périphériques en fonction du nom d'hôte.</p> <p>Entrez le nom d'hôte sur lequel vous souhaitez effectuer la recherche dans la zone Hostname.</p>

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre Risk Manager, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Devices**.
5. Dans la liste déroulante située à gauche de la liste de périphériques, sélectionnez un filtre.
6. Cliquez sur **Go**.

Résultats

Tous les résultats de la recherche correspondant à vos critères s'affichent dans le tableau.

Que faire ensuite

Pour réinitialiser un filtre, sélectionnez **Interface IP Address**, supprimez l'adresse IP/CIDR, puis cliquez sur **Go**.

Obtention d'une configuration de périphérique

Le processus de sauvegarde d'un périphérique pour obtenir une configuration de périphérique peut être exécuté pour un périphérique unique dans la liste de périphériques. Vous pouvez également sauvegarder tous les périphériques à partir de l'onglet **Devices**.

Pourquoi et quand exécuter cette tâche

Après avoir configuré les ensembles de données d'identification et les ensembles d'adresses pour accéder aux périphériques réseau, vous devez sauvegarder vos périphériques pour télécharger leur configuration. Ainsi, les informations sur les périphériques sont incluses dans la topologie.

Pour plus d'informations sur la planification des sauvegardes automatisées des configurations de périphériques à partir de l'onglet **Jobs**, voir la section Gestion des travaux de sauvegarde.

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Devices**.
5. Pour obtenir la configuration de tous les périphériques, cliquez sur **Backup All (Tout sauvegarder)** dans la sous-fenêtre de navigation, puis cliquez sur **Yes** pour continuer.
6. Pour obtenir la configuration d'un périphérique, sélectionnez le périphérique. Pour sélectionner plusieurs périphériques, maintenez la touche CTRL enfoncée et sélectionnez tous les périphériques nécessaires. Cliquez sur **Backup**.
7. Le cas échéant, cliquez sur l'option permettant d'**afficher les détails d'une erreur**. Après avoir corrigé l'erreur, cliquez sur **Backup All** dans la sous-fenêtre de navigation.


Collecte de données voisines

Utilisez le processus de reconnaissance pour obtenir les données voisines d'un périphérique à l'aide du protocole SNMP et d'une interface de ligne de commande (CLI).

Pourquoi et quand exécuter cette tâche

Les données voisines sont utilisées dans la topologie pour tirer les lignes de connexion afin d'afficher la mappe topologique graphique de vos périphériques réseau. Le bouton Reconnaître vous permet de sélectionner un périphérique unique ou plusieurs périphériques et de mettre à jour les données voisines d'un périphérique. Ces informations permettent de mettre à jour les lignes de connexion pour un ou plusieurs périphériques de la topologie.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Devices**.
5. Sélectionnez le périphérique pour lequel vous souhaitez obtenir des données. Pour sélectionner plusieurs périphériques, maintenez la touche CTRL enfoncée et sélectionnez tous les périphériques nécessaires.
6. Cliquez sur **Discover**.
7. Cliquez sur **Yes** pour poursuivre.

Résultats

Si vous sélectionnez plusieurs périphériques, le processus de reconnaissance peut prendre plusieurs minutes.

Que faire ensuite

Sélectionnez **Run in Background** pour utiliser un autre composant.

Gestion des travaux de sauvegarde

Un travail fait référence à un travail de sauvegarde, ce qui vous permet de sauvegarder automatiquement les informations de configuration de tous les périphériques de l'onglet **Devices** d'un planning.


Sous l'onglet **Jobs** de Configuration Source Management, vous pouvez créer des travaux de sauvegarde pour tous les périphériques ou des groupes individuels de périphériques dans Configuration Source Management.

Tout travail de sauvegarde que vous définissez sur la page Configuration Source Management n'affecte pas votre configuration de sauvegarde IBM Security QRadar SIEM si vous utilisez l'icône **Sauvegarde et récupération** de l'onglet **Admin**. La fonctionnalité de récupération et de sauvegarde permet d'obtenir des informations et des données de configuration pour QRadar SIEM. Le travail de sauvegarde de la page permet d'obtenir des informations pour les périphériques externes.

Affichage des travaux de sauvegarde

Les travaux et leurs détails sont affichés sur l'onglet **Jobs**.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Jobs**.

5. Cliquez deux fois sur un travail dont vous souhaitez afficher des détails supplémentaires.

Affichage de l'état et des journaux des travaux de sauvegarde

Vous pouvez résoudre les problèmes de tâche de sauvegarde en utilisant les informations d'état et des journaux de sauvegarde qui sont disponibles sur la page **Moniteur de configuration**.

Pourquoi et quand exécuter cette tâche

Pour afficher l'état et l'avancement d'une tâche de sauvegarde, utilisez la page Moniteur de configuration. Pour afficher le fichier journal des travaux de sauvegarde, utilisez l'Afficheur de journal de sauvegarde.

Procédure

Allez à **Risques > Moniteur de configuration**. Les colonnes suivantes de la table **Liste des unités** fournissent des informations sur l'état du travail de sauvegarde :

Colonne	Description
Etat de la sauvegarde	Indique l'état d'achèvement du travail de sauvegarde : COLLECTE. Le travail de sauvegarde est en attente de traitement. EN COURS. Le travail de sauvegarde est en cours. SUCCES. Le travail de sauvegarde s'est terminé avec succès. ECHEC. Le travail de sauvegarde n'est pas terminé.
Progrès	Affiche une barre de progression qui permet de suivre le taux d'achèvement du travail de sauvegarde. Pour mettre à jour la barre de progression, cliquez sur l'icône Actualiser dans la page Moniteur de configuration.
Journal de sauvegarde	Pour ouvrir la fenêtre Afficheur de journal de sauvegarde pour le travail de sauvegarde, cliquez sur le lien Afficher le journal dans cette colonne. Pour mettre à jour la barre de progression, cliquez sur le lien Actualiser dans la fenêtre Afficheur de journal de sauvegarde.


Ajout d'un travail de sauvegarde

Vous pouvez créer des travaux de sauvegarde pour tous les périphériques ou des groupes individuels de périphériques dans Configuration Source Management.

Pourquoi et quand exécuter cette tâche

Après avoir défini les critères de recherche, vous devez définir la planification de travail. La configuration de planification s'affiche dans la colonne Triggers. Les déclencheurs d'un travail représentent la planification des travaux. Vous pouvez avoir plusieurs planifications qui sont configurées. Par exemple, vous pouvez configurer deux options de planification pour qu'un travail soit exécuté chaque lundi et le premier jour de chaque mois.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.

4. Cliquez sur l'onglet **Jobs**.
5. Sélectionnez **New Job > Backup**.
6. Configurez les valeurs des paramètres suivants :

Option	Description
Job Name	Entrez le nom que vous souhaitez affecter à ce travail.
Group	Dans la liste Group, sélectionnez le groupe auquel vous souhaitez effectuer ce travail. S'il n'apparaît aucun groupe dans la liste, vous pouvez entrer un nom de groupe. Vous pouvez trier les travaux après qu'ils sont affectés à un groupe.
Comment	Entrez tous les commentaires à associer à ce travail de sauvegarde. Vous pouvez entrer jusqu'à 255 caractères dans votre description du travail de sauvegarde.

7. Cliquez sur **OK**.
8. Sélectionnez une des méthodes de recherche suivantes :

Option	Description
Static list	Vous pouvez utiliser une liste statique pour rechercher les périphériques à l'aide de plusieurs options. Grâce à cette option de liste statique, vous pouvez définir les périphériques spécifiques sur lesquels vous souhaitez exécuter le travail.
Search	Entrez une adresse IP ou une plage CIDR à inclure dans le travail. Une fois que vous avez défini les critères de recherche, la recherche de périphériques est effectuée une fois le travail exécuté. Cela vous permet de vous assurer que tous les nouveaux périphériques sont inclus dans le travail.

9. Si vous sélectionnez Liste statique, définissez les critères de recherche :
 - a. Cliquez sur l'onglet **Devices**.
 - b. Dans la liste de l'onglet **Devices**, sélectionnez les critères de recherche. Pour plus d'informations, voir Critères de recherche pour une liste statique ou une recherche.
 - c. Cliquez sur **Go**.
 - d. Sous l'onglet **Devices**, sélectionnez les périphériques que vous souhaitez inclure dans le travail.
 - e. Dans la sous-fenêtre Job Details, cliquez sur **Add selected from device view search**.
10. Si vous sélectionnez Search, définissez les critères de recherche :
 - a. Cliquez sur l'onglet **Devices**.
 - b. Dans la liste de l'onglet **Devices**, sélectionnez les critères de recherche. Pour plus d'informations, voir Critères de recherche pour une liste statique ou une recherche.
 - c. Cliquez sur **Go**.
 - d. Dans la sous-fenêtre Job Details, cliquez sur **Use search from devices view**. Ces critères de recherche permettent de déterminer les périphériques associés à ce travail.
11. Cliquez sur **Schedule** et configurez les valeurs des paramètres suivants :

Option	Description
Name	Entrez un nom pour la configuration de planification.


Option	Description
Start time	Sélectionnez une heure et une date de départ du processus de sauvegarde. L'heure doit être indiquée en heure militaire.
Frequency	Sélectionnez la fréquence à associer à cette planification.
Cron	Entrez une expression cron, interprétée en temps moyen de Greenwich (GMT). Pour obtenir de l'aide, contactez votre administrateur.
Specify End Date	Facultatif. Sélectionnez une date de fin de la planification de travaux.

12. Cliquez sur **Save** dans la sous-fenêtre Trigger.
13. Répétez les étapes 11 et 12 pour créer plusieurs planifications.
14. Si vous souhaitez exécuter le travail immédiatement, cliquez sur **Run Now**.
15. Cliquez sur **Yes** pour poursuivre.

Modification d'un travail de sauvegarde

Vous pouvez modifier les travaux de sauvegarde.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Jobs**.
5. Cliquez deux fois sur le travail que vous souhaitez modifier.
6. Sélectionnez une des options suivantes à partir du **type de sélection** :

Option	Description
Static list	Une liste statique vous permet de rechercher les périphériques à l'aide de plusieurs options. Grâce à cette option de liste statique, vous pouvez définir les périphériques spécifiques sur lesquels vous souhaitez exécuter le travail.
Search	Entrez une adresse IP ou une plage CIDR à inclure dans le travail. Une fois que vous avez défini les critères de recherche, la recherche de périphériques se produit une fois le travail exécuté. Cela vous permet de vous assurer que tous les nouveaux périphériques sont inclus dans le travail.

7. Si vous sélectionnez Static List, définissez les critères de recherche :
 - a. Cliquez sur l'onglet **Devices**.
 - b. Dans la liste de l'onglet **Devices**, sélectionnez les critères de recherche.
 - c. Cliquez sur **Go**.
 - d. Sous l'onglet **Devices**, sélectionnez les périphériques que vous souhaitez inclure dans le travail.
 - e. Dans la sous-fenêtre **Job Details**, cliquez sur **Add selected from device view search**.
8. Si vous sélectionnez Search, définissez les critères :
 - a. Cliquez sur l'onglet **Devices**.
 - b. Dans la liste de l'onglet **Devices**, sélectionnez les critères de recherche.

- c. Cliquez sur **Go**.
 - d. Dans la sous-fenêtre Job Details, cliquez sur **Use search from devices view**. Ces critères de recherche permettent de déterminer les périphériques associés à ce travail.
9. Cliquez sur **Schedule** et configurez les valeurs des paramètres suivants :


Option	Description
Name	Entrez un nom pour la configuration de planification.
Start time	Sélectionnez une heure et une date de départ du processus de sauvegarde. L'heure doit être indiquée en heure militaire.
Frequency	Sélectionnez la fréquence à associer à cette planification.
Cron	Entrez une expression cron, interprétée en temps moyen de Greenwich (GMT). Pour obtenir de l'aide, contactez votre administrateur.
Specify End Date	Facultatif. Sélectionnez une date de fin de la planification de travaux.

10. Cliquez sur **Save**.
11. Cliquez sur **Run Now**.
12. Répétez les étapes 9 et 10, comme indiqué.
13. Cliquez sur **Yes** pour poursuivre.

Renommage d'un travail de sauvegarde

Vous pouvez renommer un travail de sauvegarde

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Jobs**.
5. Sélectionnez le travail de sauvegarde que vous souhaitez renommer.
6. Cliquez sur **Rename**.
7. Configurez les valeurs des paramètres suivants :


Option	Description
Job Name	Entrez le nom que vous souhaitez affecter à ce travail.
Group	Dans la liste Group , sélectionnez le groupe auquel vous souhaitez affecter ce travail. Vous pouvez également spécifier un nouveau nom de groupe.
Comment	Facultatif. Entrez tous les commentaires à associer à ce travail de sauvegarde. Vous pouvez entrer jusqu'à 255 caractères dans votre description du travail de sauvegarde.

8. Cliquez sur **OK**.

Suppression d'un travail de sauvegarde

Vous pouvez supprimer un travail de sauvegarde.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Cliquez sur l'onglet **Jobs**.
5. Sélectionnez le travail de sauvegarde que vous souhaitez supprimer.
6. Cliquez sur **Delete**.

Configuration de protocoles

Pour que le composant IBM Security QRadar Risk Manager communique avec les périphériques, vous devez définir la méthode de communication (protocole) requise pour la communication avec vos périphériques réseau.

QRadar Risk Manager comprend la configuration de protocole par défaut pour votre système. Si vous devez définir les protocoles, vous pouvez les définir afin de permettre à QRadar Risk Manager d'obtenir une configuration de périphérique et de la mettre à jour. De nombreux environnements réseau possèdent différents protocoles de communication de différents types ou de différentes fonctions de périphérique. Par exemple, un routeur peut utiliser un protocole différent de celui des pare-feux dans le réseau. Pour obtenir une liste des protocoles pris en charge par le fabricant de périphériques, consultez le *IBM Security QRadar Risk Manager Adapter - Guide de configuration*.

QRadar Risk Manager utilise des ensembles de protocoles pour définir des groupes de protocoles pour un ensemble de périphériques nécessitant un protocole de communication spécifique. Vous pouvez affecter des périphériques à des groupes du réseau. Cette opération vous permet d'unifier les ensembles de protocoles et les ensembles d'adresses de vos périphériques.

Les ensembles de protocoles disposent d'un nom et concernent les ensembles de périphériques nécessitant des données d'identification de protocole spécifiques.

Les ensembles d'adresses sont des adresses IP définissant un groupe du réseau.

Configuration des protocoles

Vous définissez les protocoles pour obtenir et mettre à jour une configuration de périphérique.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer les valeurs suivantes pour les paramètres de protocole.


Tableau 5. Paramètres du protocole

Protocole	Paramètre
SSH	<p>Configurez les paramètres suivants :</p> <p>Port - Entrez le port que le protocole SSH doit utiliser lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Le port de protocole SSH par défaut est 22.</p> <p>Version - Sélectionnez la version de SSH que vous souhaitez que ce groupe du réseau utilise lors de la communication avec les périphériques réseau. Les options possibles sont les suivantes :</p> <p>Auto - Cette option détecte automatiquement la version SSH à utiliser lors de la communication avec les périphériques réseau.</p> <p>1 - Utilisez SSH-1 lors de la communication avec les périphériques réseau.</p> <p>2 - Utilisez SSH-2 lors de la communication avec les périphériques réseau.</p>
Telnet	<p>Entrez le numéro de port que vous souhaitez que le protocole Telnet utilise lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Le port de protocole Telnet par défaut est 23.</p>
HTTPS	<p>Entrez le numéro de port que vous souhaitez que le protocole HTTPS utilise lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Le port de protocole HTTPS par défaut est 443.</p>
HTTP	<p>Entrez le numéro de port que vous souhaitez que le protocole HTTP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Le port de protocole HTTP par défaut est 80.</p>
SCP	<p>Entrez le numéro de port que vous souhaitez que le protocole SCP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Le port de protocole SCP par défaut est 22.</p>
SFTP	<p>Entrez le numéro de port que vous souhaitez que le protocole SFTP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Le port de protocole SFTP par défaut est 22.</p>
FTP	<p>Entrez le numéro de port que vous souhaitez que le protocole FTP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Le port de protocole SFTP par défaut est 22.</p>

Tableau 5. Paramètres du protocole (suite)

Protocole	Paramètre
TFTP	Le protocole TFTP ne possède aucune option configurable.
SNMP	<p>Configurez les paramètres suivants :</p> <p>Port - Entrez le numéro de port que vous souhaitez que le protocole SNMP utilise lors de la communication avec les périphériques réseau et de leur sauvegarde.</p> <p>Délai d'attente (ms) - Sélectionnez la durée, en millisecondes, que vous souhaitez utiliser pour déterminer un délai d'attente de communication.</p> <p>Réessayer - Sélectionnez le nombre de fois que vous souhaitez tenter de rétablir des communications avec un périphérique.</p> <p>Version - Sélectionnez la version du protocole SNMP à utiliser pour les communications. Les options sont v1, v2 ou v3.</p> <p>Authentification V3 - Sélectionnez l'algorithme à utiliser pour déchiffrer les alertes SNMP.</p> <p>Chiffrement V3 - Sélectionnez le protocole à utiliser pour déchiffrer les alertes SNMP.</p>

Procédure


1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. On the navigation menu, click **Protocols**.
5. Configurer un nouveau groupe du réseau :
 - a. Dans la sous-fenêtre **Network Groups**, cliquez sur l'icône **Ajouter (+)**.
 - b. Entrez un nom pour un groupe du réseau.
 - c. Cliquez sur **OK**.
 - d. Utilisez les icônes **Vers le haut** et **Vers le bas** pour définir les priorités pour les groupes du réseau. Déplacez en haut de la liste le groupe du réseau auquel vous souhaitez affecter la première priorité.
6. Configurer l'ensemble d'adresses :
 - a. Dans la zone **Add Address**, entrez l'adresse IP ou la plage CIDR que vous souhaitez appliquer au groupe du réseau, puis cliquez sur l'icône **Ajouter (+)**. Par exemple, tapez une plage d'adresses IP en utilisant un tiret ou un caractère générique (*). Par exemple, 10.100.20.0-10.100.20.240 ou 1.1.1.*. Si vous entrez 1.1.1.*, toutes les adresses IP répondant à cette exigence sont incluses.
 - b. Répétez cette procédure pour toutes les adresses IP à ajouter à l'ensemble d'adresses de ce groupe du réseau.
7. Configurer l'ensemble des protocoles :
 - a. Dans la sous-fenêtre **Network Groups**, vérifiez que le groupe du réseau pour lequel vous souhaitez configurer des protocoles est sélectionné.
 - b. Cochez les cases pour appliquer un protocole à la plage d'adresses IP affectée au groupe du réseau créé. Le fait de désélectionner la case désactive l'option de communication du protocole lors de la tentative de sauvegarde d'un périphérique réseau.

- c. Pour chaque protocole sélectionné, configurez les valeurs pour les paramètres.
 - d. Utilisez les icônes **Vers le haut** et **Vers le bas** pour définir les priorités pour les protocoles. Déplacez en haut de la liste le protocole auquel vous souhaitez affecter la première priorité.
8. Cliquez sur **OK**.

Configuration de la planification du processus de reconnaissance

Vous pouvez configurer une planification des reconnaissances pour renseigner les tables ARP et MAC et les informations voisines pour vous périphériques. La planification des reconnaissances permet également d'ajouter automatiquement de nouveaux périphériques à l'inventaire.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Applications**.
3. Dans la sous-fenêtre **Risk Manager**, cliquez sur **Configuration Source Management**.
4. Dans le menu de navigation, cliquez sur **Schedule Discovery**.
5. Cochez la case **Enable periodic discovery** pour activer la planification des reconnaissances.
6. Configurez les valeurs des paramètres suivants :

Option	Description
Nom	Entrez un nom pour la configuration de planification.
Date de début	Sélectionnez une heure et une date de départ du processus de sauvegarde. L'heure doit être indiquée en heure militaire.
Fréquence	Sélectionnez la fréquence à associer à cette planification.
Tâche périodique	Entrez une expression cron, interprétée en temps moyen de Greenwich (GMT). Pour obtenir de l'aide, contactez votre administrateur.
Indiquer Date de fin	Facultatif. Sélectionnez une date de fin de la planification de travaux.
Crawl and discover new devices	Cochez cette case si vous souhaitez que le processus de reconnaissance reconnaisse de nouveaux périphériques. Décochez cette case si vous ne souhaitez pas ajouter de périphérique à l'inventaire.

7. Cliquez sur **OK**.

6 Connexions

Une connexion désigne l'enregistrement d'une communication, y compris une communication refusée, entre deux adresses IP uniques vers un port de destination spécifique, tel qu'il est détecté sur un intervalle de temps spécifique.

Si deux adresses IP communiquent plusieurs fois sur un même port au cours de l'intervalle de temps spécifié, une seule communication est enregistrée. Le nombre total d'octets envoyés et le nombre de flux sont inclus dans les informations de connexion. Celles-ci sont stockées dans la base de données pour chaque intervalle de temps.

Trafic de flux bidirectionnel

Les données de connexion issues de flux unidirectionnels ne sont pas enregistrées. Celles issues d'un trafic de flux bidirectionnel associé à une source de flux et à un événement de refus de routeur ou de pare-feu sont enregistrées dans les cas suivants :

- La destination est distante, ce qui signifie qu'elle se trouve à l'extérieur de la hiérarchie du réseau, la connexion est de type "local à distant" et non pas de type "distant à distant".
- La destination est locale, ce qui signifie qu'elle se trouve à l'intérieur de la hiérarchie du réseau, et l'adresse IP et le port de destination qui figurent dans l'enregistrement de flux se trouvent dans la base de données d'actifs et le port de destination est ouvert.

Recherche des connexions réseau

Vous pouvez surveiller et analyser les connexions de l'unité réseau ou effectuer des recherches avancées. Effectuez les tâches suivantes sur la page Connexions :

- Recherchez des connexions.
- Recherchez un sous-ensemble de connexions.
- Marquez les résultats de la recherche comme faux positifs pour empêcher les événements de faux positifs de créer des infractions.
- Affichez les informations de connexion regroupées par diverses options.
- Exportez les connexions au format XML ou CSV.
- Utilisez le graphique interactif pour afficher les connexions au sein de votre réseau.

Affichage des connexions

Vous pouvez afficher les informations de connexion regroupées par diverses options.

Pourquoi et quand exécuter cette tâche

Par défaut, la fenêtre Connexions affiche les graphiques suivants :

- Le graphique **Enregistrements correspondants par intervalle de temps** fournit des informations de série temporelle indiquant le nombre de connexions basées sur le temps.
- Le **Graphique de connexion** fournit une représentation visuelle des connexions récupérées.

Remarque : Si vous avez déjà sauvegardé une recherche par défaut, les résultats de cette recherche s'affichent.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Connexions**.
3. Pour sélectionner un intervalle de temps, choisissez les paramètres **Heure de début** et **Heure de fin**, ou utilisez la liste **Vue**.

Dans le tableau, cliquez avec le bouton droit de la souris sur une cellule (à l'exception des cellules de la colonne **Heure du dernier paquet**) d'un menu, pour appliquer un filtrage supplémentaire, ou pour **Afficher les événements de connexion**.

Exemple

La fenêtre Connexions affiche les informations suivantes :

Tableau 6. Fenêtre Connexions par défaut

Paramètre	Description
Filtres en cours	<p>Ce paramètre s'affiche uniquement après avoir appliqué un filtre.</p> <p>Les détails du filtre qui sont appliqués au résultat de la recherche s'affichent dans la partie supérieure de l'écran. Pour effacer ces valeurs de filtres, cliquez sur Effacer le filtre.</p>
Afficher	<p>Dans la liste, sélectionnez l'intervalle de temps que vous souhaitez filtrer. Utilisez l'option Développer pour régler l'intervalle de temps.</p>
Statistiques en cours	<p>Les statistiques en cours incluent les paramètres suivants :</p> <p>Résultats totaux - Nombre total de résultats correspondant à vos critères de recherche.</p> <p>Fichiers de données recherchés - Nombre total de fichiers de données recherchés pendant l'intervalle de temps spécifié.</p> <p>Fichiers de données compressés recherchés - Nombre total de fichiers de données compressées recherchées au cours de l'intervalle de temps spécifié.</p> <p>Nombre de fichiers d'index - Nombre total de fichiers d'indexation recherchés pendant l'intervalle de temps spécifié.</p> <p>Durée - Durée de la recherche.</p> <p>Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre un problème, vous pouvez être invité à fournir des informations statistiques actuelles. Cliquez sur la flèche à côté de Statistiques en cours pour afficher ou masquer les statistiques.</p>

Tableau 6. Fenêtre Connexions par défaut (suite)

Paramètre	Description
Graphiques	Affiche les graphiques représentant les enregistrements correspondants par intervalle de temps et/ou option de regroupement. Cliquez sur Masquer les graphiques si vous souhaitez retirer les graphiques de votre affichage. Remarque : Retirez la fonction <i>Adblock Plus</i> de Firefox si elle empêche l'affichage des graphiques dans le navigateur.
Heure du dernier paquet	Date et heure du dernier paquet traité pour cette connexion.
Type de source	Type de source pour cette connexion : Hôte ou Distant .
Source	Les options possibles pour la Source sont les suivantes : Adresse IP - Adresse IP pour la source de cette connexion. Si le Type de source est Hôte , l'adresse IP est affichée. Pays - Pays source (avec le drapeau du pays) de cette connexion. Le drapeau du pays s'affiche si le type de source est distant.
Type de destination	Les options possibles pour Type de destination sont les suivantes : Hôte ou Distant .
Destination	Les options possibles pour Destination sont les suivantes : Adresse IP - Si Type de destination est Hôte, l'adresse IP est affichée. Pays - Pays de destination (avec le drapeau du pays) de cette connexion. Le drapeau du pays s'affiche uniquement si le Type de destination est Distant.
Protocole	Protocole utilisé pour cette connexion.
Port de destination	Port de destination de cette connexion.
Application de flux	Application de flux ayant généré la connexion.
Source de flux	Source de flux associés à cette connexion. Ce paramètre s'applique uniquement aux connexions validées.
Nombre de flux	Nombre total de flux associés à cette connexion.
Octets source du flux	Nombre total d'octets de source de flux associés à cette connexion.
Octets de destination du flux	Nombre total d'octets de destination associés à cette connexion.
Source de journal	Source des événements qui contribuent à cette connexion.
Nombre d'événements	Nombre total d'événements détectés pour la connexion.
Type de connexion	Les options possibles pour le type de connexion sont les suivantes : Autoriser ou Refuser .

Utilisation des graphiques pour afficher les données de connexion

Vous pouvez afficher les données de connexion via diverses options de graphiques. Par défaut, vous affichez les données à l'aide des enregistrements correspondants par intervalle de temps et d'un graphique des connexions.

Le graphique **Enregistrements correspondants par intervalle de temps** indique le nombre de connexions basées sur le temps.

Le **Graphique de connexion** fournit une représentation visuelle de la connexion récupérée.

Les options de graphiques disponibles pour les connexions groupées sont les graphiques circulaires, à barres ou tabulaires.

Si vous utilisez une extension de navigateur Adblock Plus avec un navigateur Web Mozilla Firefox, il est possible que les graphiques ne s'affichent pas correctement. Pour que les graphiques s'affichent, vous devez supprimer l'extension de navigateur Adblock Plus. Pour plus d'informations sur la suppression des ajouts, consultez la documentation de votre navigateur Web.

Utilisation du graphique de série temporelle

Les graphiques de série temporelle sont des représentations graphiques de vos connexions au fil du temps, les pics et creux qui s'affichent représentent l'activité haute et basse des connexions.

Avant de commencer

Si vous avez déjà sauvegardé une recherche en tant que recherche par défaut, les résultats de cette recherche s'affichent sur la page Connexions. Si cette recherche comprend les options Grouper par sélectionnées dans la zone Définition de vue avancée, le graphique de série temporelle n'est pas disponible. Vous devez supprimer les critères de recherche avant de poursuivre.

Pourquoi et quand exécuter cette tâche

Les graphiques de série temporelle sont utiles pour l'analyse des tendances de données à court et à long terme. À l'aide des graphiques de série temporelle, vous pouvez accéder, naviguer et analyser les connexions de divers points de vue et perspectives.

Le tableau suivant fournit des fonctions vous permettant d'afficher les graphiques de séries temporelles.

Tableau 7. Fonctions des graphiques de série temporelle

Si vous souhaitez	Alors
Afficher les connexions plus en détail	<p>Le fait d'augmenter les données d'un graphique de série temporelle vous permet d'analyser des segments temporels plus petits des connexions. Vous pouvez agrandir le graphique de séries temporelles à l'aide des options suivantes :</p> <p>Appuyez sur le bouton Maj et cliquez sur le graphique sur le temps que vous souhaitez étudier.</p> <p>Appuyez sur les boutons Maj et Ctrl lorsque vous cliquez et vous glissez le pointeur de la souris sur l'intervalle que vous souhaitez afficher.</p> <p>Placez le pointeur de votre souris sur le graphique, puis appuyez sur la flèche vers le bas de votre clavier.</p> <p>Placez le pointeur de votre souris sur le graphique et ensuite utilisez la molette de votre souris pour effectuer un zoom avant (roulez la molette de la souris vers le haut).</p> <p>Une fois que vous avez agrandi un graphique de série temporelle, le graphique s'actualise pour afficher un plus petit segment de temps.</p>
Afficher une plus grande plage de temps des connexions	<p>Le fait d'intégrer des intervalles de temps supplémentaires dans le graphique des séries temporelles vous permet d'étudier les plus grands segments temporels ou de revenir à la plage horaire maximale. Vous pouvez afficher un intervalle de temps en utilisant l'une des options suivantes :</p> <p>Cliquez sur Max à gauche du graphique ou appuyez sur la touche Accueil pour renvoyer à l'intervalle de temps maximal.</p> <p>Placez le pointeur de votre souris sur le graphique, puis appuyez sur la flèche vers le bas sur votre clavier.</p> <p>Placez le pointeur de votre souris sur le graphique du tracé et ensuite utilisez la molette de votre souris pour effectuer un zoom arrière (roulez la molette de la souris vers le bas).</p>

Tableau 7. Fonctions des graphiques de série temporelle (suite)

Si vous souhaitez	Alors
Analyser le graphique	<p>Pour afficher le graphique afin de déterminer les informations sur chaque point de données, procédez comme suit :</p> <p>Cliquez et glissez le graphique pour analyser la ligne de temps.</p> <p>Appuyez sur le bouton Page Up pour que la ligne de temps supprime une page complète vers la gauche.</p> <p>Appuyez sur la touche de déplacement vers la gauche pour déplacer la page de la moitié de ligne de temps vers la gauche.</p> <p>Appuyez sur le bouton Page Down pour que la ligne de temps déplace toute la page vers la droite.</p> <p>Appuyez sur la touche de déplacement vers la droite pour déplacer la page de la moitié de ligne de temps vers la droite</p>

Procédure

Procédure

1. Cliquez sur l'onglet Risques.
2. Dans le menu de navigation, cliquez sur **Connexions**.
3. Dans le panneau Graphiques, cliquez sur l'icône permettant de **configurer**.
4. Dans la liste déroulante **Type de graphique**, sélectionnez Série temporelle.
5. A l'aide des graphiques de série temporelle interactifs, vous pouvez parcourir une ligne temporelle pour analyser les connexions.
6. Pour actualiser les informations dans le graphique, cliquez sur Mettre à jour les détails.

Utilisation du graphique de connexion pour afficher les connexions réseau

Le graphique des connexions fournit une représentation visuelle des connexions dans votre réseau.

Le graphique qui s'affiche dans la fenêtre Connexions n'est pas interactif. Si vous cliquez sur le graphique, la fenêtre Visualiseur de données radiales s'affiche. La fenêtre Visualiseur de données radiales permet de manipuler le graphique si nécessaire.

Par défaut, le graphique affiche vos connexions réseau comme suit :

- Seules les connexions autorisées s'affichent.
- Toutes les adresses IP locales sont réduites pour afficher uniquement les réseaux en feuilles.
- Tous les noeuds de pays sont réduits en un noeud appelé Pays distants.
- Tous les noeuds distants sont réduits en un noeud appelé Réseaux distants.
- La prévisualisation de la vue miniature du graphique affiche une partie du graphique principal. Cette option est utile pour les graphiques de grande taille.

Visualiseur de données radiales comprend plusieurs options de menu.

Tableau 8. Options du menu Visualiseur de données radiales

Option de menu	Description
Type de connexion	Par défaut, le graphique radial affiche les connexions validées. Si vous souhaitez afficher les connexions refusées, sélectionnez Refuser dans la liste déroulante Type de connexion .
Annuler	Permet de réduire le développement du dernier noeud. Si vous souhaitez annuler plusieurs développements, cliquez sur le bouton Annuler pour chaque développement.
Télécharger	Cliquez sur Télécharger pour enregistrer la topologie en cours sous un fichier image JPEG ou un fichier de dessin Visio (VDX). Pour télécharger et enregistrer la topologie actuelle en tant que fichier dessin Visio (VDX), votre version logicielle minimale requise est Microsoft Visio Standard 2010.

Le tableau suivant contient des fonctions supplémentaires pour afficher les connexions.

Tableau 9. Fonctions Visualiseur de données radiales

Si vous souhaitez	Alors
Effectuer un zoom avant ou arrière	Utilisez le curseur en haut à droite du graphique pour changer l'échelle.
Répartir les noeuds sur le graphique pour afficher plus de détails	Faites glisser le noeud vers l'emplacement souhaité pour distribuer les noeuds sur le diagramme.
Développer un noeud réseau	Cliquez deux fois sur le noeud pour détailler et voir les actifs pour ce noeud. Le noeud se développe pour inclure les actifs spécifiques avec lesquels ce noeud communiquait. Par défaut, ce développement est limité aux 100 premiers actifs du réseau.
Afficher des détails supplémentaires concernant une connexion	Placez le pointeur de votre souris sur la ligne de connexion pour afficher des détails supplémentaires. Si la connexion est établie entre un noeud réseau et un réseau distant ou un pays distant, cliquez sur le bouton droit de la souris pour afficher les menus Source et Affichage des flux suivants : Si la connexion est établie entre deux adresses IP, les informations de source, de destination et de port s'affichent lorsque vous cliquez sur la ligne de connexion.
Déterminer le nombre de données impliquées dans la connexion	L'épaisseur de la ligne du graphique détermine le nombre de données impliquées dans la connexion. Une ligne plus épaisse indique un nombre de données plus important. Ces informations sont basées sur le nombre d'octets impliqués dans la communication
Sélectionner un chemin de connexion	Placez le pointeur de votre souris sur la ligne de connexion. Si la connexion est autorisée, le chemin est surligné en vert. Si la connexion est refusée, le chemin est surligné en rouge.

Tableau 9. Fonctions Visualiseur de données radiales (suite)

Si vous souhaitez	Alors
Déterminer le chemin de connexion pour un noeud particulier	Placez le pointeur de votre souris sur le noeud. Si le noeud est autorisé, le chemin d'accès au noeud et le noeud sont surlignés en vert. Si le noeud est refusé, le chemin d'accès au noeud et le noeud sont surlignés en rouge.
Changer la vue graphique	A l'aide de la miniature de prévisualisation, placez la miniature sur la partie de graphique que vous souhaitez afficher.

Utilisation des graphiques circulaires, à barres et tabulaires

Vous pouvez afficher les données de connexion dans un graphique circulaire, à barres ou tabulaire.

Pourquoi et quand exécuter cette tâche

Les options des graphiques circulaires, à barres et tabulaires s'affichent uniquement si la recherche comprend les options Grouper par sélectionnées dans Définition de vue avancée.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Connexions**.

Remarque : Les résultats de recherches sauvegardées s'affichent.

3. Effectuez une recherche.
4. Dans la sous-fenêtre Graphiques, cliquez sur l'icône **Configuration**.
5. Configurez les paramètres suivants:

Option	Description
Valeur à représenter	Dans la liste Valeur à représenter , sélectionnez le type d'objet que vous souhaitez faire apparaître sur le graphique. Les options comprennent tous les paramètres du flux uniformisés et personnalisés inclus dans vos paramètres de recherche.
Type de graphique	Dans la liste Type de graphique , sélectionnez le type de graphique que vous souhaitez afficher. Les options comprennent : Table - Affiche les données dans un tableau. Barres - Affiche les données dans un graphique à barres. Secteurs - Affiche les données dans un graphique circulaire.

6. Cliquez sur **Sauvegarder**.
Les données ne s'actualisent pas automatiquement, sauf si vos critères de recherche s'affichent pour afficher automatiquement les détails.
7. Pour actualiser les données, cliquez sur **Mettre à jour les détails**.

Recherche de connexions

Vous pouvez rechercher des connexions à l'aide de critères spécifiques et afficher les connexions qui correspondent aux mêmes critères dans une liste de résultats. Vous pouvez créer une nouvelle recherche ou charger un ensemble de critères de recherche précédemment enregistré.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Connexions**.
Le cas échéant, les résultats de recherches sauvegardées par défaut sauvegardé recherche s'affichent.
3. Dans la liste **Rechercher**, sélectionnez **Nouvelle recherche**.
4. Si vous souhaitez charger une recherche précédemment sauvegardée, utilisez l'une des options suivantes :
 - a. Dans la liste **Groupe**, sélectionnez le groupe auquel la recherche sauvegardée est associée.
 - b. A partir de la liste **Recherches sauvegardées disponibles**, sélectionnez la recherche sauvegardée que vous voulez charger.
 - c. Dans la zone **Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste**, saisissez le nom de la recherche que vous voulez charger. A partir de la liste Recherches sauvegardées disponibles, sélectionnez la recherche enregistrée que vous voulez charger.
 - d. Cliquez sur **Charger**.
 - e. Dans le volet **Editer la recherche**, sélectionnez les options souhaitées pour cette recherche.

Option	Description
Inclure dans mes recherches rapides	Incluez cette recherche dans vos éléments Recherche rapide.
Inclure dans mon tableau de bord	Incluez les données de votre recherche sauvegardée dans votre tableau de bord. Ce paramètre ne s'affiche que si la recherche est regroupée.
Définir par défaut	Définissez cette recherche en tant que recherche par défaut.
Partager avec tout le monde	Partagez ces exigences de recherche avec tous les autres utilisateurs IBM Security QRadar Risk Manager.

5. Dans la sous-fenêtre Intervalle, sélectionnez une option pour l'intervalle de temps que vous voulez capturer pour cette recherche.

Option	Description
Récent	Dans la liste, indiquez l'intervalle de temps que vous souhaitez filtrer.
Intervalle spécifique	A l'aide de l'agenda, indiquez la plage de dates et heures que vous souhaitez filtrer.

6. Si vous avez fini de configurer la recherche et que vous souhaitez afficher les résultats, cliquez sur **Rechercher**.
7. Dans la sous-fenêtre Paramètres de recherche, définissez vos critères de recherche spécifiques :
 - a. Dans la première liste, sélectionnez un attribut de recherche. Par exemple, Type de connexion, Réseau source ou Direction.
 - b. Dans la deuxième liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. La liste des modificateurs qui s'affichent dépend de l'attribut sélectionné dans la première liste.
 - c. Dans la zone de texte, entrez les informations spécifiques associées à votre recherche.
 - d. Cliquez sur **Ajouter un filtre**.

- e. Répétez les étapes a à d pour chaque filtre que vous souhaitez ajouter aux critères de recherche.
- f. Si vous avez fini de configurer la recherche et que vous souhaitez afficher les résultats, cliquez sur **Rechercher**. Sinon, passez à l'étape suivante.
8. Si vous souhaitez enregistrer automatiquement les résultats de recherche lorsque la recherche est terminée, cochez la case Enregistrer les résultats une fois la recherche terminée et entrez un nom.
9. Si vous avez fini de configurer la recherche et que vous souhaitez afficher les résultats, cliquez sur **Rechercher**. Sinon, passez à l'étape suivante.
10. A l'aide du volet Définition de colonne, définissez les colonnes et l'agencement de colonne que vous souhaitez utiliser pour afficher les résultats :
 - a. Dans la liste **Afficher**, sélectionnez la vue que vous souhaitez associer à cette recherche.
 - b. Cliquez sur la flèche située en regard de **Définition de vue avancée** afin d'afficher les paramètres de recherche avancée. Cliquez à nouveau sur la flèche pour masquer les paramètres.
11. Cliquez sur **Rechercher**.

Enregistrement des critères de recherche

Vous pouvez créer une recherche en spécifiant des critères de recherche et vous pouvez également sauvegarder la recherche pour une utilisation ultérieure.

Pourquoi et quand exécuter cette tâche

Vous pouvez personnaliser les colonnes qui s'affichent dans les résultats de la recherche. Ces options sont disponibles dans la section Définition de colonne et s'appellent options Définition de vue avancée.

Tableau 10. Options Définition de vue avancée

Paramètre	Description
Saisir une colonne ou effectuer votre sélection dans la liste	<p>Filtre les colonnes dans la liste Colonnes disponibles.</p> <p>Saisissez le nom de la colonne que vous souhaitez localiser ou saisissez un mot-clé pour afficher une liste de noms de colonnes qui incluent ce mot-clé.</p> <p>Par exemple, saisissez Source pour afficher la liste des colonnes qui comprend Source dans le nom de la colonne.</p>
Colonnes disponibles	Répertorie les colonnes disponibles associées à la vue sélectionnée. Les colonnes qui sont actuellement en usage pour cette recherche enregistrée sont soulignées et affichées dans la liste Colonnes .
Ajouter et retirer des boutons de colonne (premier ensemble)	<p>Le premier ensemble de boutons vous permet de personnaliser la liste Grouper par.</p> <p>Ajouter une colonne - Sélectionnez une ou plusieurs colonnes dans la liste Colonnes disponibles et cliquez sur le bouton Ajouter une colonne.</p> <p>Retirer la colonne - Sélectionnez une ou plusieurs colonnes dans la liste Grouper par et cliquez sur le bouton Retirer la colonne.</p>

Tableau 10. Options Définition de vue avancée (suite)

Paramètre	Description
Ajouter et retirer des boutons de colonne (dernier ensemble)	<p>Le dernier ensemble de boutons vous permet de personnaliser la liste Colonnes.</p> <p>Ajouter une colonne - Sélectionnez une ou plusieurs colonnes dans la liste Colonnes disponibles et cliquez sur le bouton Ajouter une colonne.</p> <p>Retirer la colonne - Sélectionnez une ou plusieurs colonnes dans la liste Colonnes et cliquez sur le bouton Retirer la colonne.</p>
Grouper par	<p>Indique les colonnes dans lesquelles la recherche enregistrée regroupe les résultats. Vous pouvez personnaliser davantage la liste Grouper par en utilisant les options suivantes :</p> <p>Vers le haut - Sélectionnez une colonne et déplacez-la vers la liste prioritaire en utilisant l'icône Vers le haut.</p> <p>Vers le bas - Sélectionnez une colonne et déplacez-le vers le bas liste prioritaire en utilisant l'icône Vers le bas.</p> <p>La liste de priorité indique l'ordre dans lequel les résultats sont regroupés. Les résultats de la recherche se regrouperont selon la première colonne de la liste Grouper par, puis selon la colonne suivante sur la liste.</p>
Colonnes	<p>Indique les colonnes choisies pour la recherche. Les colonnes sont chargées depuis une recherche enregistrée. Vous pouvez personnaliser la liste Colonnes en sélectionnant des colonnes à partir de la liste Colonnes disponibles. Vous pouvez personnaliser davantage la liste Colonnes en utilisant les options suivantes :</p> <p>Vers le haut - Sélectionnez une colonne et déplacez-la vers la liste prioritaire en utilisant le bouton de déplacement vers le haut.</p> <p>Vers le bas - Sélectionnez une colonne et déplacez-la vers la liste prioritaire en utilisant le bouton de déplacement vers le bas.</p> <p>Si le type de colonne est numérique ou temporel et qu'il existe une entrée dans la liste Grouper par, la colonne contient une liste déroulante qui vous permet de choisir la façon dont vous souhaitez regrouper la colonne.</p>
Trier par	<p>A partir de la première liste, indiquez la colonne par laquelle vous voulez trier les résultats de la recherche. Puis, à partir de la deuxième liste, indiquez la commande que vous souhaitez afficher pour les résultats de la recherche : Décroissant ou Croissant.</p>

Procédure

1. Cliquez sur l'onglet **Risque**.
2. Dans le menu de navigation, cliquez sur **Connexions**.
3. Effectuez une recherche.
4. Cliquez sur **Sauvegarder les critères**.

5. Configurez les valeurs des paramètres suivants :

Option	Description
Nom de la recherche	Tapez un nom que vous souhaitez attribuer à ces critères de recherche.
Affecter la recherche au(x) groupe(s)	Le groupe que vous souhaitez affecter à cette recherche sauvegardée. Si vous ne sélectionnez pas un groupe, cette recherche enregistrée est attribuée à l'autre groupe par défaut.
Options d'intervalle	Sélectionnez une des options suivantes : Récent - Dans la liste déroulante, indiquez l'intervalle de temps que vous souhaitez filtrer. Intervalle spécifique - A l'aide de l'agenda, indiquez la plage de dates et heures que vous souhaitez filtrer.
Inclure dans mes recherches rapides	Cochez cette case si vous souhaitez inclure cette recherche dans vos éléments Recherche rapide qui sont disponibles dans la liste déroulante Recherche .
Inclure dans mon tableau de bord	Cochez cette case si vous voulez inclure les données de votre recherche enregistrée dans votre tableau de bord. Ce paramètre ne s'affiche que si la recherche est regroupée.
Définir par défaut	Cochez cette case si vous souhaitez définir cette recherche en tant que votre recherche par défaut.
Partager avec tout le monde	Sélectionnez cette case pour partager ces exigences de recherche avec tous les autres utilisateurs IBM Security QRadar Risk Manager.

6. Cliquez sur **OK**.

Effectuer une sous-recherche

Chaque fois que vous effectuez une recherche, la base de données entière est interrogée pour des connexions qui correspondent à vos critères. En fonction de la taille de la base de données, ce processus peut prendre beaucoup de temps.

Pourquoi et quand exécuter cette tâche

Une fonction de sous-recherche vous permet d'effectuer des recherches dans un ensemble de résultats de recherche réalisée. Vous pouvez raffiner vos résultats de recherche sans rechercher à nouveau la base de données. Une fonction de sous-recherche n'est pas disponible pour les recherches regroupées ou les recherches en cours.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Connexions**.
3. Effectuez une recherche. Les résultats de la recherche sont affichés. Les recherches supplémentaires utilisent le jeu de données provenant de la recherche précédente lorsque des sous-recherches sont effectuées.
4. Pour ajouter un filtre, procédez comme suit :
 - a. Cliquez sur **Ajouter un filtre**.
 - b. Dans la première liste, sélectionnez un attribut de recherche.

- c. Dans la deuxième liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. La liste des modificateurs qui s'affichent dépend de l'attribut sélectionné dans la première liste.
- d. Dans la zone de texte, entrez les informations spécifiques associées à votre recherche.
- e. Cliquez sur **Ajouter un filtre**.

Remarque : Si la recherche est toujours en cours, les résultats partiels sont affichés. La sous-fenêtre dédiée au filtre d'origine indique le filtre sur lequel la recherche d'origine est basée. La sous-fenêtre Filtre en cours indique le filtre appliqué à la sous-recherche.

Conseil : Vous pouvez effacer les filtres de sous-recherche sans avoir à redémarrer la recherche d'origine. Cliquez sur le lien Effacer le filtre à côté du filtre que vous souhaitez effacer. Si vous désactivez un filtre dans le volet dédié au filtre d'origine, la recherche initiale est relancée.

5. Cliquez sur **Sauvegarder les critères** pour enregistrer la sous-recherche.

Résultats

Si vous supprimez la recherche d'origine, vous pouvez accéder à la sous-recherche enregistrée. Si vous ajoutez un filtre, la sous-recherche explore toute la base de données puisqu'elle n'est plus fondée un ensemble de données précédemment recherchées.

Gestion des résultats de recherche

Vous pouvez effectuer plusieurs recherches de connexion tout en naviguant sur d'autres interfaces.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer la fonction de recherche pour vous envoyer une notification par courrier électronique lorsqu'une recherche est terminée. A tout moment pendant qu'une recherche est en cours, vous pouvez consulter les résultats partiels d'une recherche en cours.

La barre d'outils des résultats de la recherche fournit les options suivantes :

Paramètre	Description
Nouvelle recherche	Cliquez sur Nouvelle recherche afin de créer une recherche. Lorsque vous cliquez sur ce bouton, la fenêtre de recherche s'affiche.
Sauvegarder les résultats	Cliquez sur Sauvegarder les résultats afin de sauvegarder les résultats de recherche. Cette option est activée uniquement lorsque vous avez sélectionné une ligne dans la liste Gérer les résultats de la recherche.
Annuler	Cliquez sur Annuler afin d'annuler les recherches qui sont en cours ou qui sont en attente pour démarrer.
Supprimer	Cliquez sur Supprimer afin de supprimer un résultat de recherche.
Envoyer une notification	Sélectionnez la ou les recherches pour lesquelles vous souhaitez recevoir une notification, puis cliquez sur Envoyer une notification pour activer la notification par courrier électronique lorsque la recherche est terminée.

Paramètre	Description
Afficher	<p>Dans la liste déroulante, indiquez les résultats de la recherche que vous voulez lister dans la fenêtre correspondante. Les options sont :</p> <p>Résultats de recherche sauvegardée</p> <p>Tous les résultats de la recherche</p> <p>Recherches annulées/erronées</p> <p>Recherches en cours</p>

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Connexions**.
3. Dans le menu, sélectionnez **Rechercher > Gérer les résultats de la recherche**.

Sauvegarde des résultats de la recherche

Vous pouvez sauvegarder les résultats de la recherche.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Connexions**.
3. Effectuez une recherche ou sous-recherche de connexion.
4. Dans la fenêtre Résultats de la recherche, sélectionnez **Rechercher > Gérer les résultats de la recherche** et sélectionnez un résultat de recherche.
5. Cliquez sur **Sauvegarder les résultats**.
6. Saisissez un nom pour les résultats de la recherche.
7. Cliquez sur **OK**.

Annulation d'une recherche

Vous pouvez annuler une ou plusieurs recherches.

Pourquoi et quand exécuter cette tâche

Si une recherche est en cours lors de l'annulation, les résultats accumulés jusqu'à l'annulation de la recherche, sont maintenus.

Procédure

1. A partir de la fenêtre Gérer les résultats de la recherche, sélectionnez les résultats de recherche en attente ou en cours que vous souhaitez annuler. Vous pouvez sélectionner plusieurs recherches pour annuler.
2. Cliquez sur **Annuler la recherche**.
3. Cliquez sur **Oui**.

Suppression d'une recherche

Vous pouvez supprimer une recherche.

Procédure

1. Dans la fenêtre Gérer les résultats de la recherche, sélectionnez les résultats de recherche que vous souhaitez supprimer.

2. Cliquez sur **Supprimer**.
3. Cliquez sur **Oui**.

Exportation des connexions

Vous pouvez exporter des connexions au format XML ou CSV.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Connexions**.
3. Si vous souhaitez exporter la connexion au format XML, sélectionnez **Actions > Exporter au format XML**.
4. Si vous souhaitez exporter la connexion au format CSV, sélectionnez **Actions > Exporter au format CSV**.
5. Si vous souhaitez reprendre vos activités, cliquez sur **Aviser à la fin de l'opération**.

7 Moniteur de configuration

Dans IBM Security QRadar Risk Manager, vous pouvez gérer l'efficacité de vos unités réseau, rechercher les règles de pare-feu et identifier les risques de sécurité résultant de règles de pare-feu non valides.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le volet de navigation, cliquez sur **Moniteur de configuration**.
3. Pour rechercher vos périphériques réseau, entrez une adresse IP ou un nom d'hôte dans la zone **Adresse IP ou nom d'hôte**.

4. Double-cliquez sur le dispositif à examiner.

La colonne **Nombre d'événements** de la règle affiche la fréquence de déclenchement des règles de pare-feu. Une règle de nombre d'événement nul 'affiche pour l'une des raisons suivantes :

- Une règle n'est pas déclenchée et peut entraîner un risque de sécurité. Vous pouvez examiner votre dispositif réseau et supprimer les règles qui ne sont pas déclenchées.
- Il n'y a pas de mappage de source de journal QRadar configuré.

5. Pour rechercher les règles, dans la barre d'outils **Règles**, cliquez sur **Rechercher > Nouvelle recherche**.

Si une icône s'affiche dans la colonne **Etat**, vous pouvez passer la souris sur l'icône de statut pour afficher des informations supplémentaires.

6. Pour examiner les interfaces d'unité, cliquez sur **Interfaces** dans la barre d'outils.
7. Pour examiner les règles des dispositifs de liste de contrôle d'accès, cliquez sur **ACLs**.

Chaque liste de contrôle d'accès définit les interfaces sur lesquelles les dispositifs de votre réseau communique. Lorsque les conditions d'une liste de contrôle d'accès sont remplies, les règles associées à une liste de contrôle d'accès sont déclenchées. Chaque règle est testée pour autoriser ou refuser la communication entre les dispositifs.

8. Pour examiner les règles des dispositifs de conversion d'adresses réseau (NAT), dans la barre d'outils, cliquez sur **NAT**.

La colonne **Phase** spécifie le moment auquel la règle NAT doit être déclenchée, par exemple, avant ou après le routage.

9. Pour examiner l'historique ou comparer les configurations des dispositifs, dans la barre d'outils, cliquez sur **Historique**.

Vous pouvez afficher les règles des dispositifs dans une vue uniformisée ou la configuration des dispositifs en mode brut. La configuration uniformisée des dispositifs est une comparaison graphique qui affiche les règles ajoutées, supprimées ou modifiées entre les dispositifs. La configuration des dispositifs en mode brut est une vue XML ou en texte simple du fichier de dispositif.

Recherche des règles de périphérique

Dans IBM Security QRadar Risk Manager, vous pouvez rechercher les règles qui ont été modifiées dans votre topologie. Vous pouvez également découvrir les changements de règles qui se produisent entre les sauvegardes de configuration de périphérique.

Les résultats renvoyés pour une recherche de règles dépendent de la sauvegarde de gestion des sources de configuration de votre périphérique. Pour s'assurer que les recherches de règles fournissent des informations à jour, vous pouvez planifier vos sauvegardes de périphérique dans la page de mise à jour des règles de pare-feu.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le volet de navigation, cliquez sur **Moniteur de configuration**.
3. Double-cliquez sur un périphérique dans la page Moniteur de configuration.
4. Dans la barre d'outils du volet Règles, cliquez sur **Rechercher > Nouvelle recherche**.
5. Dans le volet **Critères de recherche**, cliquez sur une plage horaire.
6. Pour rechercher les règles de votre périphérique, sélectionnez l'une des options suivantes :
 - Pour rechercher des règles **fictives, supprimées** ou **autres**, cliquez sur une option de statut. Par défaut, toutes les options de statut sont activées. Pour rechercher des règles fictives uniquement, désélectionnez les options **Supprimé** et **Autre**.
 - Pour rechercher une liste de contrôle d'accès, renseignez la zone **Liste**.
 - Pour rechercher le numéro d'ordre de l'entrée de règle, entrez une valeur numérique dans la zone **Entrée**.
 - Pour rechercher une source ou une cible, entrez une adresse IP, une adresse CIDR, un nom d'hôte ou une référence de groupe d'objets.
 - Pour rechercher des ports ou des références de groupe d'objets, renseignez la zone **Service**. Le service peut inclure des plages de ports, comme 100-200, ou des expressions de port, comme 80 (TCP). Si le port est annulé, les informations associées contiennent également un point d'exclamation et peuvent être mises entre parenthèses, par exemple, !(100-200) ou !80(TCP).
 - Pour rechercher les informations de règles de vulnérabilité définies par le périphérique IPS, renseignez la zone **Signature**.
 - Pour rechercher des applications par adaptateur, cliquez sur **Sélectionner des applications**, puis entrez un adaptateur ou un nom d'application.
7. Cliquez sur **Rechercher**.

Comparaison de la configuration de vos périphériques réseau

Dans IBM Security QRadar Risk Manager, les configurations de périphérique peuvent être comparées entre elles en comparant différentes sauvegardes sur un périphérique ou en comparant une sauvegarde de périphérique réseau à une autre.

Les types de configuration courants peuvent inclure les éléments suivants :

- **Document d'élément standard** - Les fichiers de document d'élément standard (SED) sont des fichiers de données XML qui contiennent des informations sur votre périphérique réseau. Les fichiers SED individuels s'affichent dans leur format XML brut. Si un fichier SED est comparé à un autre fichier SED, la vue est uniformisée de manière à afficher les différences entre les règles.
- **Config** - Certains périphériques réseau fournissent des fichiers de configuration en fonction du fabricant des périphériques. Vous pouvez afficher un fichier de configuration en cliquant deux fois dessus.

En fonction des informations collectées par l'adaptateur pour votre périphérique, différents autres types de configuration peuvent s'afficher. Ces fichiers s'affichent en texte brut lorsque vous cliquez deux fois dessus.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur le **Moniteur de configuration**.
3. Cliquez deux fois sur un périphérique pour afficher les informations de configuration détaillées.
4. Cliquez sur **History** pour afficher l'historique de ce périphérique.
5. Pour comparer deux configurations sur un périphérique unique, procédez comme suit :

- a. Sélectionnez une configuration primaire.
 - b. Appuyez sur la touche Ctrl et sélectionnez une seconde configuration pour la comparaison.
 - c. Dans le volet History, cliquez sur **Compare Selected**.
Si les fichiers de comparaison sont des documents d'élément standard (SED), la fenêtre Normalized Device Configuration Comparison affiche les différences de règles entre les sauvegardes.
Lorsque vous comparez les configurations uniformisées, la couleur du texte indique les mises à jour de périphérique suivantes :
 - Un contour pointillé vert indique une règle ou une configuration ajoutée au périphérique.
 - Un contour à tirets rouges indique une règle ou une configuration supprimée sur le périphérique.
 - Un contour plein jaune indique une règle ou une configuration modifiée sur le périphérique.
 - d. Pour afficher les différences brutes de configuration, cliquez sur **View Raw Comparison**.
Si la comparaison porte sur un fichier de configuration ou un autre type de sauvegarde, la comparaison brute s'affiche.
6. Pour comparer deux configurations sur différents périphériques :
- a. Sélectionnez une configuration primaire dans un périphérique.
 - b. Cliquez sur **Mark for Comparison**.
 - c. Dans le menu de navigation, sélectionnez **Toutes les unités** pour retourner à la liste de périphériques.
 - d. Cliquez deux fois sur le périphérique pour comparer et cliquez sur **History**.
 - e. Sélectionnez une configuration à comparer à la configuration marquée.
 - f. Cliquez sur **Compare with Marked**.
 - g. Pour afficher les différences brutes de configuration, cliquez sur **View Raw Comparison**.

Gestion des périphériques

Dans IBM Security QRadar Risk Manager, utilisez le **Moniteur de configuration** pour ajouter ou supprimer des périphériques réseau et pour sauvegarder des configurations de périphérique.

Ajout d'un périphérique

Vous pouvez ajouter des périphériques réseau et des adaptateurs individuels à l'aide du Moniteur de configuration.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Configuration Monitor**.
3. Dans la barre d'outils, cliquez sur **Add device**. Vous pouvez également accéder au menu **Actions**, puis cliquer sur **Device Management > Add Device**.
4. Configurez les valeurs des paramètres suivants :

Option	Description
IP Address	Entrez l'adresse IP de gestion du périphérique.
Adapter	Sélectionnez l'adaptateur à affecter à ce périphérique.
Back up now	Extrait des adaptateurs les informations relatives au périphérique et ajoute ce dernier au travail de sauvegarde. Inclut le périphérique dans la topologie.

5. Cliquez sur **OK**.

Sauvegarde d'un périphérique

Le processus de sauvegarde d'un périphérique pour obtenir une configuration de périphérique peut être exécuté pour un périphérique unique dans la liste de périphériques ou pour sauvegarder tous les périphériques en même temps. Après avoir configuré les ensembles de données d'identification et les ensembles d'adresses pour accéder aux périphériques réseau, vous devez sauvegarder vos périphériques pour télécharger leur configuration. Ainsi, les informations sur les périphériques sont incluses dans la topologie.

Procédure

1. Cliquez sur l'onglet **Risks**.
2. Dans le menu de navigation, cliquez sur **Configuration Monitor**.
3. Sélectionnez le périphérique à sauvegarder.
4. Dans la barre d'outils, cliquez sur **Backup Device** pour sauvegarder le périphérique sélectionné. Vous pouvez également accéder au menu **Actions** et cliquer sur **Device Management > Backup Device**. Pour sélectionner plusieurs périphériques, maintenez la touche CTRL enfoncée et sélectionnez tous les périphériques nécessaires.
5. Pour obtenir la configuration de tous les périphériques, cliquez sur **Backup All** dans la sous-fenêtre de navigation. Vous pouvez également accéder au menu **Actions** et cliquer sur **Device Management > Backup All Devices**.
6. Cliquez sur **Yes**.
7. Le cas échéant, cliquez sur l'option permettant d'**afficher les détails d'une erreur**. Après avoir corrigé l'erreur, cliquez sur **Backup All** dans la sous-fenêtre de navigation.

Tâches associées:

Affichage de l'état et des journaux des travaux de sauvegarde

Vous pouvez résoudre les problèmes de tâche de sauvegarde en utilisant les informations d'état et des journaux de sauvegarde qui sont disponibles sur la page **Moniteur de configuration**.

Suppression d'un périphérique

Vous pouvez supprimer un ou plusieurs périphériques de IBM Security QRadar Risk Manager afin de nettoyer la vue dans la liste de périphériques. Le périphérique supprimé l'est aussi du Moniteur de configuration, de Configuration Source Management et de la topologie.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Configuration Monitor**.
3. Accédez au menu **Actions**, puis cliquez sur **Device Management** pour supprimer un seul ou plusieurs périphériques.
 - Pour supprimer un seul périphérique, sélectionnez-le, puis cliquez sur **Delete Device**.
 - Pour supprimer plusieurs périphériques, maintenez la touche CTRL enfoncée et sélectionnez tous les périphériques à supprimer, puis cliquez sur **Delete Device**.
 - Pour supprimer tous les périphériques de la **liste de périphériques**, cliquez sur **Delete All Devices**.
4. Cliquez sur **Yes**.

Résultats

Le processus de suppression du périphérique de la topologie peut prendre plusieurs minutes.

Reconnaissance de périphériques

Dans IBM Security QRadar Risk Manager, utilisez l'écran Device Discovery du Moniteur de configuration pour ajouter, éditer et exécuter une reconnaissance définie.

Pourquoi et quand exécuter cette tâche

Lorsque vous exécutez une reconnaissance de périphérique de type Discover with SNMP, tout périphérique non pris en charge, mais répondant au protocole SNMP est ajouté via l'adaptateur SNMP générique.

Procédure

1. Accédez à l'écran Device Discovery comme suit :
 - a. Cliquez sur l'onglet Risques.
 - b. Cliquez sur **Configuration Monitor** > **Device Discovery** dans la sous-fenêtre Risk Manager.
2. Ajoutez un périphérique à QRadar Risk Manager comme suit :
 - a. Dans la sous-fenêtre de navigation, cliquez sur **Add**.
 - b. Sélectionnez un type **Discovery Type** dans l'écran Discovery Profile Configuration. Les méthodes permettant d'ajouter un périphérique réseau sont les suivantes :
 - Discover with SNMP
 - Discover from Check Point OPSEC
 - Discover from Defense Center
 - Discover from NSM
 - Discover from SiteProtector™
 - Discover from Check Point HTTPS
 - c. Renseignez les zones **Device IP**, **Username** et **Password** pour le périphérique.
 - d. Vous pouvez également rechercher des périphériques dans le réseau à partir de l'adresse IP définie avec l'option Discover with SNMP. Cochez la case **Crawl the network from the addresses defined above**.
 - e. Pour lancer la reconnaissance immédiatement, cliquez sur **Run Discovery Now**. Vous pouvez aussi sauvegarder la configuration de profil et exécuter la reconnaissance ultérieurement.
 - f. Cliquez sur **Save**.
3. Editez un périphérique répertorié dans la liste de reconnaissances comme suit :
 - a. Sélectionnez un périphérique dans la liste de reconnaissances, puis cliquez sur **Edit** dans la sous-fenêtre de navigation.
 - b. Editez les détails de la reconnaissance, puis sélectionnez **Run Discovery Now** pour lancer immédiatement la reconnaissance. Vous pouvez aussi sauvegarder la configuration de profil et exécuter la reconnaissance ultérieurement.
4. Pour rechercher un périphérique, entrez son adresse IP/nom dans la zone **Device IP**, puis cliquez sur l'icône **Rechercher**.
5. Vous pouvez supprimer un travail de reconnaissance de périphérique en sélectionnant un périphérique dans la **liste de reconnaissances**, puis en cliquant sur **Delete** dans la sous-fenêtre de navigation.

Activité récente

Dans IBM Security QRadar Risk Manager, utilisez l'écran Activité récente de QRadar Risk Manager pour vous aider à gérer les activités des périphériques et identifier et résoudre les problèmes liés à la gestion des périphériques.

Vous pouvez afficher toutes les informations relatives à une activité, y compris son **Type**, son **Etat** et un indicateur de **Progression**. Vous pouvez également afficher et examiner le **Journal**.

Toutes les reconnaissances consignent une entrée dans l'écran Activité récente. Les types d'activité qui s'affichent dans l'écran Activité récente sont les suivants :

- **Adapter Backup**
- **Add Device**
- **Delete Device**
- **Device Backup**
- **Run Discovery**

Le tableau suivant répertorie tous les états affichés dans l'écran Activité récente :

Tableau 11. Etats dans Activité récente.

Etat	Description
Collected	La configuration de périphérique est collectée, mais elle n'a pas encore été fusionnée dans QRadar Risk Manager.
Failure	La sauvegarde du périphérique a échoué et celui-ci n'a jamais été sauvegardé avec succès dans QRadar Risk Manager.
Processing	Le périphérique est en cours de traitement.
Staged	QRadar Risk Manager a reconnu le périphérique et l'extraction de sa configuration est en cours.
Success	La sauvegarde du périphérique dans QRadar Risk Manager a réussi.
Warning	La dernière tentative de traitement de ce périphérique a échoué. QRadar Risk Manager utilise une configuration précédemment réussie.

Mappage de sources de journal

Pour contrôler la fréquence de déclenchement des règles de pare-feu et permettre les recherches d'événements de topologie, IBM Security QRadar Risk Manager identifie les sources de journal QRadar.

En maîtrisant les règles de pare-feu, vous pouvez préserver l'efficacité du pare-feu et empêcher les risques de sécurité.

Un maximum de 255 périphériques peut être mappé à une source de journal dans QRadar Risk Manager, mais les périphériques peuvent comporter plusieurs sources de journal.

Options d'affichage du mappage de sources de journal

Si vous avez configuré le périphérique réseau comme source de journal QRadar, la page du moniteur de configuration affiche l'une des entrées suivantes dans la colonne **Source de journal** :

- **Mappage automatique** - Si QRadar Risk Manager identifie et mappe automatiquement la source de journal au périphérique.
- **Nom d'utilisateur** - Si un administrateur a ajouté ou modifié manuellement une source de journal.
- **Vide** - Si QRadar Risk Manager n'est pas en mesure d'identifier une source de journal pour le périphérique, la colonne **Source de journal** n'affiche aucune valeur. Vous pouvez créer manuellement un mappage de source de journal.

Pour plus d'informations sur la configuration des sources de journal, voir *IBM Security QRadar Log Sources - Guide d'utilisation*.

Création ou modification d'un mappage de source de journal

Si IBM Security QRadar Risk Manager ne peut pas identifier une source de journal dans QRadar, vous pouvez configurer un mappage de source de journal.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le volet de navigation, cliquez sur le **moniteur de configuration**.
3. Cliquez sur le périphérique sans mappage de source de journal.
4. Sur la barre d'outils, cliquez sur **Action > Mappage de source de journal > Créer/éditer le mappage de source de journal**.
5. Dans la liste **Groupes de sources de journal**, sélectionnez un groupe.
6. Dans la liste **Sources de journal**, sélectionnez une source de journal et cliquez sur (>).
7. Cliquez sur **OK**.

8 Filtrage des règles de périphérique par utilisateur ou groupe

Dans QRadar Risk Manager, vous pouvez afficher et filtrer vos règles de périphérique par utilisateur ou par groupe.

Pourquoi et quand exécuter cette tâche

Effectuez des recherches par interaction des règles d'utilisateur ou de groupe, et comprenez le mode d'interaction des utilisateurs et des groupes de votre réseau. Il est utile de connaître les interactions de règle de vos utilisateurs au sein du réseau afin de détecter tout comportement déviant. Vous pouvez ainsi formuler des règles efficaces dans votre réseau.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur le **Moniteur de configuration**.
3. Depuis le tableau **Liste de périphériques**, cliquez deux fois sur la ligne correspondant à votre périphérique.
Dans la colonne **Utilisateur(s)/Groupe(s)** dans le tableau de règles, vous pouvez voir vos utilisateurs et vos groupes.
Les résultats de groupes s'affichent sous forme de liens hypertexte, sur lesquels vous pouvez cliquer pour afficher les utilisateurs dans le groupe sélectionné.
4. Dans le panneau Règles, cliquez sur **Rechercher > Nouvelle recherche**.
5. Cliquez sur **Sélectionner les utilisateurs/groupe(s)**.
6. Entrez un terme de recherche partiel ou complet, ou laissez la zone relative au **nom d'utilisateur/de groupe** vide, puis cliquez sur **Rechercher**.
7. Sélectionnez le nom d'utilisateur ou de groupe dans la zone **Résultats de la recherche**, puis cliquez sur **Ajouter** pour les ajouter à la zone des **éléments sélectionnés**.
8. Cliquez sur **OK**, puis sur **Rechercher**.
Utilisez les informations de règle pour établir des tests de performances ou de profils pour l'interaction de règle utilisateur, ce qui peut ensuite vous permettre d'optimiser les règles de votre réseau.

9 Graphique de topologie de réseau

Dans IBM Security QRadar Risk Manager, vous pouvez utiliser le graphique de modèle de topologie pour afficher, filtrer et examiner la connectivité physique de votre réseau.

Le graphique de topologie de réseau est généré à partir des informations de configuration obtenues auprès de périphériques, comme les pare-feux, les routeurs, les commutateurs et les systèmes de prévention des intrusions (IPS). Vous pouvez survoler les lignes de connexion pour afficher les informations de connexion réseau. Vous pouvez filtrer la topologie en recherchant les chemins d'accès d'attaque potentiels sur les protocoles autorisés, les ports ou les vulnérabilités. Vous pouvez afficher le flux du trafic entre les périphériques et les sous-réseaux, ainsi que les règles de périphérique.

Vous pouvez utiliser le graphique de topologie pour effectuer les tâches suivantes :

- Visualiser les chemins réseau spécifiques et le sens du trafic pour une analyse avancée des menaces.
- Intégrer les mappes de sécurité IPS passives dans le graphique de topologie.
- Regrouper les périphériques pour organiser et simplifier la vue.
- Ajouter des périphériques aux groupes, et retirer des périphériques des groupes.
- Repositionner les icônes dans le graphique à l'aide de la souris.
- Sauvegarder les présentations de graphique de topologie.
- Renommer les périphériques et les groupes.
- Créer et sauvegarder des filtres de recherche pour votre topologie de réseau en fonction des protocoles, des ports ou des vulnérabilités.
- Afficher des informations de connexion détaillées entre les périphériques et les sous-réseaux.
- Afficher des règles de périphérique sur les connexions de noeud de topologie avec les ports et les protocoles agréés.
- Afficher des périphériques de conversion d'adresses réseau, des indicateurs NAT et des informations sur les mappages NAT.
- Afficher les périphériques de sécurité des réseaux virtuels disposant de plusieurs contextes.
- Configurez un code couleur pour les sous-réseaux pour indiquer le statut de vulnérabilité des actifs dans les sous-réseaux sur votre graphique de topologie.

Lorsque vous recherchez et affichez les ports et protocoles autorisés entre les périphériques, vous pouvez voir uniquement les connexions qui utilisent les protocoles TCP, UDP et ICMP dans le graphique de topologie.

Recherches de diagramme de topologie

Utilisez la fonction de recherche de topologie pour afficher et étudier différents éléments de votre infrastructure réseau.

Les recherches topologiques s'affichent dans une vue avec onglets et chaque recherche topologique ouvre son propre onglet. Les résultats de recherche topologique sont mis en cache afin d'améliorer la récupération de topologie, ce qui réduit le temps de traitement. Les recherches continuent de s'exécuter en arrière-plan, de sorte que vous pouvez utiliser d'autres fonctions de QRadar Risk Manager.

Vous pouvez utiliser la fonction de recherche pour filtrer la vue de topologie, et zoomer sur les chemins réseau, les hôtes, les sous-réseaux et d'autres éléments réseau. Vous pouvez ainsi affiner votre recherche jusqu'au niveau port ou protocole, par exemple vous pouvez effectuer une recherche des formes d'attaque possibles sur les ports ou protocoles autorisés.

Vous pouvez rechercher des événements en cliquant avec le bouton droit sur les périphériques et les sous-réseaux, ou rechercher des flux en cliquant avec le bouton droit sur les sous-réseaux.

Cliquez sur **Actions** pour afficher le menu **Rechercher**. Entrez vos critères de recherche dans le panneau Critères de recherche. Voici quelques exemples d'options de recherche que vous pouvez utiliser :

Recherches d'hôtes

Si vous recherchez un hôte, tous les périphériques qui communiquent avec l'hôte s'affichent. Si l'hôte ne correspond pas à une interface sur un périphérique, mais qu'il ne se trouve pas dans le sous-réseau, le sous-réseau et tous les périphériques connectés s'affichent.

Recherche de réseaux

Vous pouvez rechercher un CIDR unique, par exemple, 10.3.51.200/24.

Si vous recherchez plusieurs CIDR, assurez-vous qu'ils sont valides et séparés par une virgule, par exemple, 10.51.0.0/24,10.51.01/24.

Recherches de chemins

Une recherche de chemin d'accès affiche la direction du trafic, les protocoles autorisés partiellement ou totalement et les règles de périphérique. Un récapitulatif du chemin s'affiche si vous sélectionnez des critères de recherche autres que les adresses IP de destination et source obligatoires.

Affinez votre recherche en recherchant des applications, des vulnérabilités et des utilisateurs/groupes.

Indicateurs NAT dans les résultats de recherche

Un indicateur NAT, représenté par un point vert fixe, s'affiche dans le graphique de topologie si votre recherche trouve un chemin qui contient des conversions source ou de destination.

Pourquoi et quand exécuter cette tâche

Un indicateur NAT indique que l'adresse IP de destination spécifiée dans le filtre de chemin peut ne pas être la destination finale. Survolez l'indicateur avec votre curseur pour afficher les informations suivantes concernant les conversions.

Tableau 12. Informations disponibles dans l'indicateur NAT

Paramètre	Description
Source	IP ou CIDR source converti.
Port(s) source	Ports source convertis, le cas échéant.
Source convertie	Résultat de la conversion qui a été appliquée à la source.
Port(s) source converti(s)	Résultat de la conversion qui a été appliquée au(x) port(s) source, le cas échéant.
Destination	IP ou CIDR de destination converti.
Port(s) de destination	Ports de destination convertis, le cas échéant.
Destination convertie	Résultat de la conversion qui a été appliquée à la destination.
Port(s) de destination converti(s)	Résultat de la conversion qui a été appliquée au(x) port(s) de destination, le cas échéant.
Phase	Phase de routage lorsque la conversion a été appliquée. Les conversions sont appliquées avant ou après le routage.

Ajout d'un système de prévention contre les intrusions (IPS)

Si votre liste **Configuration Source Management** contient un périphérique Intrusion prevention system (IPS), vous pouvez ajouter un IPS à une connexion entre des noeuds d'unité-à-sous-réseau et entre des noeuds d'unité-à-unité.

Pourquoi et quand exécuter cette tâche

L'ajout d'une connexion IPS est utile pour déterminer l'emplacement du système IPS si le périphérique est passif.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Topologie**.
3. Placez le pointeur de votre souris sur la ligne de connexion reliant un noeud de périphérique à un noeud de sous-réseau.
4. Cliquez avec le bouton droit de la souris sur la ligne de connexion puis sélectionnez **Ajouter IPS**.
5. Sélectionnez le périphérique et les interfaces à ajouter à partir des listes suivantes :

Option	Description
Place IPS	Sélectionnez un placement dans la liste.
Connect IPS interface	Sélectionnez une interface à connecter à l'unité. Lorsqu'il existe plusieurs unités de choix alors vous devez sélectionner une unité (voir l'option suivante).
to device	Sélectionnez l'unité que vous souhaitez connecter à l'IPS. Cette option est disponible lorsqu'il existe plusieurs unités.
Connect IPS interface	Sélectionnez une interface à connecter au sous-réseau.

6. En utilisant les listes, sélectionnez le périphérique et les interfaces pour ajouter la connexion IPS à votre topologie.
7. Cliquez sur **OK**. Si vous voulez ajouter un IPS à un périphérique qui figure dans un groupe, développez le groupe pour ajouter le périphérique.

Suppression d'un système de prévention contre les intrusions (IPS)

Vous pouvez supprimer une connexion IPS.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Topologie**.
3. Placez le pointeur de votre souris sur la ligne de connexion reliant un noeud de périphérique à un noeud de sous-réseau.
4. Cliquez avec le bouton droit de la souris sur la ligne de connexion, sélectionnez l'option Retirer IPS idp.
5. Cliquez sur **OK**.

Groupes de périphériques de la topologie

Regroupez des périphériques dans l'onglet Topologie en cours afin d'organiser et de simplifier les graphiques de topologie complexes.

Sélectionnez un périphérique dans la fenêtre Topologie en cours et cliquez sur le menu **Actions** dans la barre d'outils, ou affichez le menu avec un clic droit de la souris afin d'accéder à la fonction **Groupes** des périphériques. Vous ne pouvez actuellement pas utiliser la fonction **Groupes** dans les onglets Topology Search.

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

Dans IBM Security QRadar Risk Manager, les infractions sont des événements générés par le système pour vous avertir d'une condition ou d'un événement 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 depuis IBM Security 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**.

10 Configuration du code couleur des sous-réseaux pour indiquer le statut de vulnérabilité

Utilisez des couleurs pour afficher le statut de vulnérabilité des sous-réseaux affichés sur votre graphique de topologie.

Pourquoi et quand exécuter cette tâche

Utilisez un code couleur pour les sous-réseaux afin de mettre en évidence les informations liées à la vulnérabilité concernant les actifs sur les sous-réseaux sur votre graphique de topologie.

Procédure

1. Cliquez sur l'onglet **Risques**.
 2. Dans le menu de navigation, cliquez sur **Topologie**.
 3. Sélectionnez **Actions > Propriétés > Editer** pour configurer le code couleur des sous-réseaux.
 4. Sélectionnez l'une des options de code couleur suivantes :
 - **Pas de code couleur pour les sous-réseaux**

Si vous ne souhaitez pas utiliser de code couleur, cliquez sur **Pas de code couleur pour les sous-réseaux**. Lorsque vous sélectionnez cette option, toutes les icônes de sous-réseau sont grisées.
 - **Score CVSS agrégé le plus élevé (score de risque) d'un actif dans un sous-réseau**

Entrez une valeur pour chaque couleur. Lorsque le score de risque d'un actif d'un sous-réseau dépasse la valeur **Supérieur à** correspondante la plus élevée, la couleur de l'icône de sous-réseau adopte cette couleur.

Par exemple, si vous configurez la valeur 14 pour la couleur rouge, l'icône de sous-réseau devient rouge lorsqu'un actif de ce sous-réseau présente un score de risque supérieur à 14.

Seule la couleur de la valeur correspondante la plus élevée s'affiche. Le score de risque est calculé en utilisant le système CVSS (Common Vulnerability Scoring System) et inclut les ajustements de risque apportés par QRadar Risk Manager. Vous pouvez afficher le score **CVSS agrégé** d'un actif sous l'onglet **Actif**.
 - **Nombre de vulnérabilités d'un actif dans un sous-réseau**

Entrez une valeur pour chaque couleur. Lorsque le nombre total de vulnérabilités d'un actif dans un sous-réseau dépasse la valeur **Supérieur à** correspondante la plus élevée, la couleur de l'icône de sous-réseau adopte la couleur représentant cette valeur.
 - **Impact des vulnérabilités d'un actif dans un sous-réseau**

Pour chaque couleur, sélectionnez un impact sur les vulnérabilités. Lorsqu'un actif dans un sous-réseau correspond à l'impact répertorié le plus élevé, la couleur de l'icône de sous-réseau adopte cette couleur.

Par exemple, si vous sélectionnez le rouge pour représenter une perte système, la couleur de l'icône de sous-réseau devient rouge lorsqu'un actif est concerné par une perte système en raison d'une vulnérabilité.

Si vous sélectionnez le même impact sur les vulnérabilités pour deux couleurs différentes, la couleur de la position la plus élevée est appliquée à l'icône de sous-réseau lorsqu'un actif est concerné par l'impact sur les vulnérabilités.
- Pour mettre à jour le statut de vulnérabilité des actifs dans votre topologie lorsqu'une analyse se termine ou que d'autres modifications liées aux vulnérabilités ont lieu, vous pouvez suivre l'une de ces procédures :
- Réinitialisez votre topologie en sélectionnant **Actions > Présentation > Réinitialiser la présentation**.

- Effacez le cache du navigateur, puis actualisez le navigateur.

Remarque : La couleur du sous-réseau sur le graphique de topologie s'affiche avec une ombre plus claire.

11 Moniteur de politique d'administration

Utilisez les questions du moniteur de politique d'administration pour évaluer et gérer les risques au sein de votre réseau. Créez et définissez des questions de risque spécifiques à propos du réseau afin d'évaluer ou de contrôler les risques en fonction de l'analyse des indicateurs de risque.

Dans le moniteur de politique d'administration, vous pouvez définir des politiques, jauger l'adhésion à une politique, évaluer les résultats des questions et surveiller les nouveaux risques.

Des modèles de questions par défaut mis à votre disposition pour vous aider à évaluer et surveiller le risque sur votre réseau. Vous pouvez utiliser l'un des modèles de questions par défaut comme base pour vos propres questions ou créer une nouvelle question. Les modèles de questions par défaut sont disponibles dans le menu **Groupe** de la page Moniteur de politique d'administration.

Vous pouvez choisir l'un des indicateurs de risque de la liste suivante :

- **Activité réseau** - mesure le risque en fonction des communications réseau établies par le passé.
- **Configuration et Topologie** - mesurent le risque en fonction de la communication possible et des connexions réseau.
- **Vulnérabilités** - mesure le risque en fonction de votre configuration réseau et des données d'analyse de vulnérabilité collectées à partir des actifs de réseau.
- **Règles de pare-feu** - mesure le risque en fonction de la mise en application ou de l'absence de règles de pare-feu appliquées au réseau.

Vous pouvez définir des tests en fonction des indicateurs de risque, puis restreindre les résultats de test pour filtrer la requête afin d'obtenir des résultats ou des infractions spécifiques.

Les professionnels de la sécurité créent des questions pour les actifs ou les unités/règles afin d'indiquer les risques dans leurs réseaux. Le niveau de risque pour un actif ou une unité/règle est reporté lorsqu'une question est soumise au moniteur de politique d'administration. Vous pouvez approuver les résultats renvoyés à partir des actifs ou définir la manière dont vous souhaitez que le système réponde aux résultats non validés.

Utilisez les résultats de la question du moniteur de politique d'administration pour évaluer différents scénarios de risques de sécurité, par exemple :

- Utilisation de protocoles de communication interdits.
- Communication avec des réseaux ou actifs interdits.
- Non respect des règles de pare-feu avec la politique de l'entreprise.
- Systèmes exposés à des vulnérabilités à haut risque du fait de leur configuration réseau.

Questions du moniteur de politique d'administration

Vous pouvez définir des questions dans le moniteur de politique d'administration afin d'évaluer et de surveiller les risques d'après l'activité réseau, les vulnérabilités et les règles de pare-feu.

Lorsque vous soumettez une question, la recherche de topologie est basée sur le type de données que vous avez sélectionné :

- Pour les questions basées sur les actifs, la recherche repose sur des actifs réseau ayant violé une règle définie ou sur des actifs ayant introduit un risque sur le réseau.
- Pour les questions basées sur des unités/règles, la recherche identifie les règles sur une unité ayant violé une règle définie ou ayant introduit un risque sur le réseau.

- Si une question est basée sur la conformité d'actif, la recherche identifie si un actif est conforme à un test de performances CIS.

Remarque : Si vous avez configuré IBM Security QRadar pour plusieurs domaines, les questions d'actifs se limitent à contrôler les actifs dans votre domaine par défaut. Les questions de conformité des actifs surveillent des actifs dans votre domaine par défaut sauf si vous avez configuré un autre domaine dans la fenêtre **Admin > Gestion des domaines**. Pour plus d'informations sur la gestion de domaine, consultez le manuel *IBM Security QRadar Administration Guide*.

Les questions relatives aux unités/règles recherchent les infractions de règles et de politique et ne comptent pas de composant de test de restriction. Vous pouvez également poser des questions de périphériques/règles pour les applications.

Les tests d'actif se répartissent dans les catégories suivantes :

- Un *test de contribution* utilise les paramètres de question pour examiner les indicateurs de risque qui sont spécifiés dans la question. Des résultats de données de risque sont générés, lesquels peuvent aussi être filtrés avec un *test restrictif*. Les tests de contribution sont affichés dans la zone **Which tests do you want to include in your question**. Ils retournent des données d'après les actifs détectés qui correspondent à la question de test.
- Un *test restrictif* permet d'affiner les résultats qui sont retournés par un *test de contribution*. Les tests restrictifs s'affichent uniquement dans la zone **Which tests do you want to include in your question** après l'ajout d'un test de contribution. Vous pouvez ajouter des tests restrictifs uniquement après avoir inclus un test de contribution dans la question. Si vous retirez ou supprimez une question de test de contribution, la question de test de restriction ne peut pas être sauvegardée.

Les questions de conformité d'actif permettent de rechercher les actifs qui ne sont pas en conformité avec les tests de performances CIS. Les tests qui sont inclus dans le test de performances CIS sont configurés avec l'éditeur de test de performances de conformité.

Paramètres relatifs à la question du moniteur de politique d'administration

Vous pouvez définir des questions de test pour identifier les risques dans les unités réseau ou dans les règles qu'ils contiennent.

Paramètres génériques et spécifiques au test pour les tests du moniteur de politique d'administration

Vous configurez les paramètres pour chaque test du moniteur de politique d'administration. Les paramètres configurables sont en gras et soulignés. Vous cliquez sur un paramètre pour afficher les options disponibles pour chaque question.

Le moniteur de politique d'administration teste l'utilisation de deux types de paramètres : générique et spécifique au test. Les paramètres génériques offrent 2 options ou plus pour personnaliser un test. Cliquer sur un paramètre générique bascule les choix disponibles. Les paramètres spécifiques au test nécessitent une entrée de l'utilisateur. Vous cliquez sur les paramètres spécifiques au test pour indiquer les informations.

Par exemple, le test d'actif appelé **have accepted communication to destination remote network locations** comprend deux paramètres génériques et un paramètre spécifique au test. Cliquez sur le paramètre générique, **have accepted**, pour sélectionner **have accepted** ou **have rejected**. Cliquez sur le paramètre générique, **to destination**, pour sélectionner **to destination** ou **from source**. Cliquez sur le paramètre spécifique au test, **remote network locations**, pour ajouter un emplacement distant pour le test d'actif.

Questions de test d'actifs

Les questions d'actifs sont utilisées pour identifier les actifs du réseau qui violent une règle définie ou qui introduisent des risques dans l'environnement.

Les questions de tests d'actifs sont classées par type de communication ; réel ou éventuel. Ces deux types de communication utilisent des tests de contribution et des tests de restriction.

Une communication actuelle inclut tous les actifs sur lesquels des communications ont été détectées à l'aide de connexions. Les questions de communication possible vous permettent de voir si des communications spécifiques sont possibles sur les actifs, qu'une communication ait été ou non détectée.

Une question de test de contribution est une question de test de base qui définit le type de communication réelle que vous essayez de tester.

Une question de test de restriction restreint les résultats d'un test de contribution afin de filtrer davantage les infractions caractéristiques dans une communication réelle.

Lorsque vous utilisez un test de restriction, la direction de test de restriction doit être la même que le test de contribution. Il est possible d'utiliser des tests de restriction mélangeant les directions entrantes et sortantes lorsque vous essayez de localiser des actifs entre deux points, tels que deux réseaux ou deux adresses IP.

Inbound fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une destination. Outbound, quant à lui, fait référence à un test qui filtre les connexions pour lesquelles l'actif en question est une source.

Questions de test relatives aux unités/règles

Les unités et les règles sont utilisées pour identifier les règles d'une unité qui violent une règle qui peut introduire des risques dans l'environnement.

Pour une liste détaillée des questions sur les règles de périphériques, voir Questions de test relatives aux unités/règles.

Questions de contribution pour les tests de communication réelle

Les tests de communication réelle pour les actifs incluent des questions et paramètres de contribution que vous pouvez choisir lorsque vous créez un test du moniteur de politique d'administration.

Lorsque vous appliquez la condition `have not` à ce test, la condition `not` s'applique au paramètre que vous testez.

Par exemple, si vous configurez un test avec la condition **have not accepted communication to destination networks**, le test détecte les actifs qui ont accepté des communications vers des réseaux autres que celui configuré. Un autre exemple, si vous configurez un test avec la condition `not accepted communication to the Internet`, le test détecte les actifs qui ont accepté des communications depuis ou vers des réseaux autres que Internet.

Le tableau suivant répertorie et décrit les paramètres de questions pour les tests de communication actuelle.

Tableau 13. Paramètres de questions de contribution pour les tests de communication réelle

Intitulé du test	Description
have accepted communication to any destination	<p>Détecte les actifs disposant de communications vers ou depuis un réseau configuré.</p> <p>Ce test vous permet de définir un point de départ ou d'arrivée pour votre question.</p> <p>Par exemple, pour identifier les actifs qui ont accepté une communication en provenance d'une zone démilitarisée (DMZ), configurez le test comme suit :</p> <p>have accepted communication from any source</p> <p>Vous pouvez utiliser ce test pour détecter les communications non conformes aux règles.</p>
have accepted communication to destination networks	<p>Détecte les actifs disposant de communications vers ou depuis les réseaux que vous indiquez.</p> <p>Ce test vous permet de définir un point de départ ou d'arrivée pour votre question.</p> <p>Par exemple, pour identifier les actifs qui communiquent avec une DMZ, configurez le test comme suit :</p> <p>have accepted communication from source <networks></p> <p>Vous pouvez utiliser ce test pour détecter les communications non conformes aux règles.</p>
have accepted communication to destination IP addresses	<p>Détecte les actifs disposant de communications vers ou depuis l'adresse IP que vous indiquez.</p> <p>Ce test vous permet d'indiquer une adresse IP ou CIDR.</p> <p>Par exemple, si vous souhaitez identifier tous les actifs qui ont communiqué avec un serveur de conformité spécifique, configurez le test comme suit :</p> <p>have accepted communications to destination <compliance server IP address></p>
have accepted communication to destination asset building blocks	<p>Détecte les actifs disposant de communications vers ou depuis les éléments structurants que vous indiquez. Ce test vous permet de réutiliser des blocs de construction définis dans l'Assistant Règles QRadar dans votre règle.</p> <p>Pour plus d'informations sur les règles, actifs et blocs de construction, voir <i>IBM Security QRadar Administration Guide</i>.</p>
have accepted communication to destination asset saved searches	<p>Détecte les actifs ayant des communications vers ou depuis les actifs renvoyés par la recherche sauvegardée que vous spécifiez.</p> <p>Pour plus d'informations sur la création et la sauvegarde d'un actif, consultez le <i>IBM Security QRadar - Guide d'utilisation</i></p>
have accepted communication to destination reference sets	<p>Détecte les actifs qui ont communiqué vers ou depuis les ensembles de référence définis.</p>

Tableau 13. Paramètres de questions de contribution pour les tests de communication réelle (suite)

Intitulé du test	Description
have accepted communication to destination remote network locations	Détecte les actifs qui ont communiqué avec des réseaux définis comme distants. Par exemple, ce test peut identifier les hôtes qui ont communiqué avec des botnets ou des espaces adresse Internet suspects.
have accepted communication to destination geographic network locations	Détecte les actifs qui ont communiqué avec des réseaux définis comme géographiques. Par exemple, ce test peut détecter les actifs qui ont tenté de communiquer avec des pays où vous n'avez aucune opération métier.
have accepted communication to the Internet	Détecte les communications source ou de destination vers ou depuis Internet.
are susceptible to one of the following vulnerabilities	Détecte les vulnérabilités spécifiques. Si vous souhaitez détecter les vulnérabilités d'un type en particulier, utilisez le test, are susceptible to vulnerabilities with one of the following classifications . Vous pouvez chercher les vulnérabilités à l'aide des options OSVDB ID, CVE ID, Bugtraq ID ou du titre.
are susceptible to vulnerabilities with one of the following classifications	Une vulnérabilité peut être associée à au moins une classification de vulnérabilité. Ce test filtre tous les actifs qui comprennent des vulnérabilités correspondant aux classifications spécifiées. Configurez le paramètre classifications afin d'identifier les classifications de vulnérabilité que vous souhaitez que le test applique. Par exemple, une classification de vulnérabilité peut être Input Manipulation ou Denial of Service.
are susceptible to vulnerabilities with CVSS score greater than 5	Une valeur CVSS (Common Vulnerability Scoring System) est une norme de l'industrie permettant d'évaluer la gravité des vulnérabilités. La valeur CVSS est composée de 3 groupes d'indicateurs : de base, temporels et environnementaux. Ces indicateurs permettent à CVSS de définir et de communiquer les caractéristiques fondamentales d'une vulnérabilité. Ce test filtre les actifs de votre réseau qui comprennent les vulnérabilités avec la valeur CVSS que vous indiquez.
are susceptible to vulnerabilities disclosed after specified date	Détecte les actifs de votre réseau ayant une vulnérabilité divulguée après, avant ou à la date configurée.
are susceptible to vulnerabilities on one of the following ports	Détecte les actifs de votre réseau ayant une vulnérabilité associée aux ports configurés. Configurez le paramètre ports afin d'identifier les ports que vous souhaitez que le test prenne en compte.

Tableau 13. Paramètres de questions de contribution pour les tests de communication réelle (suite)

Intitulé du test	Description
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une saisie concernant le nom de l'actif, le fournisseur, la version ou le service. Configurez le paramètre text entries afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une expression régulière concernant le nom de l'actif, le fournisseur, la version ou le service. Configure le paramètre regular expressions afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.
are susceptible to vulnerabilities contained in vulnerability saved searches	Détecte les risques associés aux recherches sauvegardées qui sont créées dans IBM Security QRadar Vulnerability Manager.

Questions de test de contribution dépréciées

Les questions de contribution qui sont remplacées par un autre test sont cachées dans le moniteur de politique d'administration.

Les test suivants sont cachés dans le moniteur de politique d'administration :

- assets that are susceptible to vulnerabilities
- assets that are susceptible to vulnerabilities from the following services

Ces tests de contributions ont été remplacés par d'autres tests.

Questions de restriction pour les tests de communication réelle

Les tests de communication réelle pour les actifs incluent des questions et paramètres de restriction que vous pouvez choisir lorsque vous créez un test du moniteur de politique d'administration.

Lorsque vous appliquez la condition à ce test, la condition *exclude* s'applique au paramètre *protocols*.

Par exemple, si vous configurez ce test sur la condition **exclude the following protocols**, il renvoie uniquement les actifs qui n'utilisent pas les protocoles exclus.

Le tableau suivant répertorie et décrit les paramètres de questions de restriction pour les tests de communications réelles.

Tableau 14. Paramètres de questions de restriction pour les tests de communication réelle

Intitulé du test	Description
include only the following protocols	Filtre les actifs du test de contribution qui incluent ou excluent les protocoles spécifiés. Ce test ne peut être sélectionné que lorsqu'un test de contribution concernant un actif est ajouté à la question.
include only the following inbound ports	Filtre les actifs du test de contribution qui incluent uniquement ou excluent les ports spécifiés. Ce test ne peut être sélectionné que lorsqu'un test de contribution concernant un actif est ajouté à la question.

Tableau 14. Paramètres de questions de restriction pour les tests de communication réelle (suite)

Intitulé du test	Description
include only the following inbound applications	<p>Filtre les actifs de la question du test de contribution qui incluent uniquement ou excluent des applications entrantes ou sortantes.</p> <p>Ce test ne filtre que les connexions qui incluent des données de flux.</p>
include only if the source inbound and destination outbound bytes have a percentage difference less than 10	<p>Filtre les actifs de la question du test de contribution basée sur les communications selon un taux spécifique d'octets entrants vers sortants (ou sortants vers entrants).</p> <p>Ce test est pratique pour détecter les hôtes qui peuvent présenter un comportement de type proxy (communications entrantes = communications sortantes).</p>
include only if the inbound and outbound flow count has a percentage difference less than 10	<p>Filtre les actifs de la question du test de contribution basée sur les communications selon un taux spécifique de flux entrants vers sortants (ou sortants vers entrants).</p> <p>Ce test filtre les connexions qui incluent les données de flux lorsque le nombre de flux est sélectionné.</p> <p>Ce test de restriction requiert deux tests de contribution qui indiquent une source et une destination. Le test suivant présente un ensemble de questions essayant de déterminer quels actifs entre deux points disposent d'un pourcentage de différence entre communications entrantes et sortantes supérieur à 40 %. Par exemple,</p> <p>Test de contribution - have accepted communication to the internet.</p> <p>Test de contribution - and have accepted communication from the internet.</p> <p>Test de restriction - and include only if the inbound and outbound flow count has a percentage difference greater than 40.</p>
include only if the time is between start time and end time inclusive	<p>Filtre les communications au sein de votre réseau qui ont eu lieu dans un intervalle spécifique. Cela vous permet de détecter les communications non conformes aux règles. Par exemple, si votre politique d'entreprise permet les communications FTP entre 1 et 3, ce test peut détecter une tentative d'utilisation du protocole FTP pour communiquer en dehors de cette plage temporelle.</p>
include only if the day of week is between start day and end day inclusive	<p>Filtre les actifs de la question du test de contribution en fonction des communications réseau qui ont eu lieu dans l'intervalle caractéristique. Cela vous permet de détecter les communications non conformes aux règles.</p>
include only if susceptible to vulnerabilities that are exploitable	<p>Filtre les actifs provenant d'une question de test de contribution recherchant des vulnérabilités caractéristiques et restreint les résultats aux actifs exploitables.</p> <p>Ce test de restriction ne contient pas de paramètre configurable. Cependant, il est utilisé conjointement avec le test de contribution sont sensibles à l'une des vulnérabilités suivantes. La règle de contribution contenant le paramètre vulnerabilities est obligatoire.</p>

Tableau 14. Paramètres de questions de restriction pour les tests de communication réelle (suite)

Intitulé du test	Description
include only the following networks	Filtre les actifs provenant d'une question de test de contribution qui inclut ou exclut les réseaux configurés.
include only the following asset building blocks	Filtre les actifs provenant d'une question de test de contribution qui sont ou ne sont pas associés aux éléments structurants d'actifs configurés.
include only the following asset saved searches	Filtre les actifs provenant d'une question de test de contribution qui sont ou ne sont pas associés à la recherche enregistrée d'actifs.
include only the following reference sets	Filtre les actifs provenant d'une question de test de contribution qui inclut ou exclut les ensembles de référence configurés.
include only the following IP addresses	Filtre les actifs qui sont ou ne sont pas associés aux adresses IP configurées.
include only if the Microsoft Windows service pack for operating systems is below 0	Filtre les actifs pour déterminer si un niveau de Service Pack pour un système d'exploitation Microsoft Windows est inférieur au niveau spécifié par la politique de votre entreprise.
include only if the Microsoft Windows security setting is less than 0	Filtre les actifs pour déterminer si un paramètre de sécurité Microsoft Windows est inférieur au niveau spécifié par la politique de votre entreprise.
include only if the Microsoft Windows service equals status	Filtre les actifs pour déterminer si un service Microsoft Windows est de type unknown, boot, kernel, auto, demand ou disabled.
include only if the Microsoft Windows setting equals regular expressions	Filtre les actifs pour déterminer si un paramètre Microsoft Windows correspond à l'expression régulière spécifiée.

Questions de contribution pour des tests de communication possible

Les tests de communication possible pour les actifs incluent des questions et paramètres de contribution que vous pouvez choisir lorsque vous créez un test du moniteur de politique d'administration.

Le tableau suivant répertorie et décrit les paramètres de questions pour les tests de communication possible.

Tableau 15. Paramètres de questions de communication potentiels pour les tests de contribution

Intitulé du test	Description
have accepted communication to any destination	<p>Détecte les actifs disposant de communications éventuelles vers ou depuis n'importe quelle source ou destination spécifiée. Par exemple, pour déterminer si un serveur critique peut éventuellement recevoir des communications depuis n'importe quelle source, configurez le test comme suit :</p> <p>have accepted communication from any source.</p> <p>Vous pouvez ensuite appliquer un test de restriction à renvoyer si le serveur critique en question a reçu des communications sur le port 21. Cela vous permet de détecter les communications non conformes aux règles pour le serveur critique en question.</p>

Tableau 15. Paramètres de questions de communication potentiels pour les tests de contribution (suite)

Intitulé du test	Description
have accepted communication to destination networks	<p>Détecte les actifs disposant de communications éventuelles vers ou depuis le réseau configuré.</p> <p>Ce test vous permet de définir un point de départ ou d'arrivée pour votre question.</p> <p>Par exemple, pour identifier les actifs qui disposent d'une possibilité de communication avec la DMZ, configurez le test comme suit :</p> <p>have accepted communication from source <networks></p> <p>Vous pouvez utiliser ce test pour détecter les communications non conformes aux règles.</p>
have accepted communication to destination IP addresses	<p>Détecte les actifs disposant de communications éventuelles vers ou depuis l'adresse IP configurée. Ce test vous permet d'indiquer une seule adresse IP et de vous en servir comme point central pour des communications éventuelles. Par exemple, si vous souhaitez identifier tous les actifs qui peuvent communiquer avec un serveur de conformité spécifique, configurez le test comme suit :</p> <p>have accepted communications to destination <compliance server IP address></p>
have accepted communication to destination asset building blocks	<p>Détecte les actifs disposant de communications éventuelles vers ou depuis l'actif configuré à l'aide d'éléments structurants. Ce test vous permet de réutiliser des blocs de construction définis dans l'Assistant Règles QRadar dans votre règle. Par exemple, si vous souhaitez identifier tous les actifs qui peuvent communiquer avec un élément Protected Assets, configurez le test comme suit :</p> <p>have accepted communications to destination <BB:HostDefinition:Protected Assets></p> <p>Pour plus d'informations sur les règles et les blocs de construction, voir <i>IBM Security QRadar Administration Guide</i>.</p>
have accepted communication to destination asset saved searches	<p>Détecte les actifs ayant acceptés des communications vers ou depuis les actifs renvoyés par la recherche sauvegardée que vous spécifiez.</p> <p>Une recherche d'actifs sauvegardée doit exister avant que vous ne puissiez utiliser ce test. Pour plus d'informations sur la création et la sauvegarde d'un actif, consultez le <i>IBM Security QRadar - Guide d'utilisation</i></p>
have accepted communication to destination reference sets	<p>Détecte si les communications source ou de destination sont possibles vers ou depuis les ensembles de référence.</p>
have accepted communication to the Internet	<p>Détecte si les communications source ou de destination sont possibles vers ou depuis Internet.</p> <p>Indiquez le paramètre to ou from pour considérer le trafic de communication vers ou depuis l'Internet.</p>

Tableau 15. Paramètres de questions de communication potentiels pour les tests de contribution (suite)

Intitulé du test	Description
are susceptible to one of the following vulnerabilities	<p>Détecte les vulnérabilités spécifiques éventuelles.</p> <p>Si vous souhaitez détecter les vulnérabilités d'un type en particulier, utilisez le test, are susceptible to vulnerabilities with one of the following classifications.</p> <p>Indique les vulnérabilités auxquelles vous souhaitez appliquer le test. Vous pouvez chercher les vulnérabilités à l'aide des options OSVDB ID, CVE ID, Bugtraq ID ou du titre</p>
are susceptible to vulnerabilities with one of the following classifications	<p>Une vulnérabilité peut être associée à au moins une classification de vulnérabilité. Ce test filtre tous les actifs ayant des vulnérabilités éventuelles à l'aide d'un indice Common Vulnerability Scoring System (CVSS) spécifié.</p> <p>Configurez le paramètre classifications afin d'identifier les classifications de vulnérabilité que vous souhaitez que le test applique.</p>
are susceptible to vulnerabilities with CVSS score greater than 5	<p>Une valeur CVSS (Common Vulnerability Scoring System) est une norme de l'industrie permettant d'évaluer la gravité des vulnérabilités éventuelles. La valeur CVSS est composée de trois groupes d'indicateurs : de base, temporels et environnementaux. Ces indicateurs permettent à CVSS de définir et de communiquer les caractéristiques fondamentales d'une vulnérabilité.</p> <p>Ce test filtre les actifs de votre réseau qui comprennent la valeur CVSS configurée.</p>
are susceptible to vulnerabilities disclosed after specified date	<p>Filtre les actifs de votre réseau ayant une éventuelle vulnérabilité divulguée après, avant ou à la date configurée.</p>
are susceptible to vulnerabilities on one of the following ports	<p>Filtre les actifs de votre réseau ayant une éventuelle vulnérabilité associée aux ports configurés.</p> <p>Configurez le paramètre ports pour identifier les actifs ayant d'éventuelles vulnérabilités en fonction du numéro de port spécifié.</p>
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	<p>Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une saisie concernant le nom de l'actif, le fournisseur, la version ou le service.</p> <p>Configurez le paramètre text entries afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.</p>
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	<p>Détecte les actifs de votre réseau ayant une vulnérabilité qui correspond à au moins une expression régulière concernant le nom de l'actif, le fournisseur, la version ou le service.</p> <p>Configurez le paramètre regular expressions afin d'identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez que le test prenne en compte.</p>

Tableau 15. Paramètres de questions de communication potentiels pour les tests de contribution (suite)

Intitulé du test	Description
are susceptible to vulnerabilities contained in vulnerability saved searches	Détecte les risques associés aux recherches sauvegardées qui sont créées dans IBM Security QRadar Vulnerability Manager.

Questions de test de contribution dépréciées

Si un test est remplacé par un autre test, il est caché dans un moniteur de politique d'administration.

Les test suivants sont cachés dans le moniteur de politique d'administration :

- assets that are susceptible to vulnerabilities from the following vendors
- assets that are susceptible to vulnerabilities from the following services

Ces tests de contributions ont été remplacés par d'autres tests.

Paramètres de questions de restriction pour les tests de communication possible

Les tests de communication possible pour les actifs incluent des paramètres de questions de restriction.

Le tableau suivant répertorie et décrit les paramètres de questions de restriction pour les tests de communication possible.

Tableau 16. Tests de restriction pour les tests de communication potentiels

Intitulé du test	Description
include only the following protocols	Filtre les actifs qui ont éventuellement communiqué ou non avec les protocoles configurés, conjointement avec les autres tests ajoutés à la question.
include only the following inbound ports	Filtre les actifs qui ont éventuellement communiqué ou non avec les ports configurés, conjointement avec les autres tests ajoutés à la question.
include only ports other than the following inbound ports	Filtre les actifs provenant d'une question de test de contribution qui ont éventuellement communiqué ou non avec des ports autres que ceux configurés, conjointement avec les autres tests ajoutés à la question.
include only if susceptible to vulnerabilities that are exploitable.	Filtre les actifs provenant d'une question de test de contribution recherchant d'éventuelles vulnérabilités caractéristiques et restreint les résultats aux actifs exploitables. Ce test de restriction ne contient pas de paramètre configurable. Cependant, il est utilisé conjointement avec le test de contribution are susceptible to one of the following vulnerabilities . La règle de contribution contenant le paramètre vulnerabilities est obligatoire.
include only the following networks	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut les réseaux configurés.
include only the following asset building blocks	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut les éléments structurants d'actifs configurés.

Tableau 16. Tests de restriction pour les tests de communication potentiels (suite)

Intitulé du test	Description
include only the following asset saved searches	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut la recherche enregistrée d'actifs associée.
include only the following reference sets	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut les ensembles de référence configurés.
include only the following IP addresses	Filtre les actifs provenant d'une question de test de contribution qui inclut uniquement ou exclut les adresses IP configurées.
include only if the Microsoft Windows service pack for operating systems is below 0	Filtre les actifs pour déterminer si un niveau de Service Pack Microsoft Windows pour un système d'exploitation est inférieur au niveau spécifié par la politique de votre entreprise.
include only if the Microsoft Windows security setting is less than 0	Filtre les actifs pour déterminer si un paramètre de sécurité Microsoft Windows est inférieur au niveau spécifié par la politique de votre entreprise.
include only if the Microsoft Windows service equals status	Filtre les actifs pour déterminer si un service Microsoft Windows est de type unknown, boot, kernel, auto, demand ou disabled.
include only if the Microsoft Windows setting equals regular expressions	Filtre les actifs pour déterminer si un paramètre Microsoft Windows correspond à l'expression régulière spécifiée.

Questions de test relatives aux unités/règles

Les questions de test relatives aux unités/règles servent à identifier les règles d'une unité qui violent une règle définie susceptible d'introduire un risque dans l'environnement.

Les questions de test relatives aux unités et aux règles sont décrites sur le tableau suivant.

Tableau 17. Tests relatifs aux unités/règles

Intitulé du test	Description
allow connections to the following networks	Filtre les règles et les connexions de périphérique vers ou depuis les réseaux configurés. Par exemple, si vous configurez le test d'autorisation des communications vers un réseau, le test filtre toutes les règles et connexions qui autorisent des connexions au réseau configuré.
allow connections to the following IP addresses	Filtre les règles et les connexions des périphériques vers ou depuis les adresses IP configurées. Par exemple, si vous configurez le test d'autorisation des communications vers une adresse IP, ce dernier filtre toutes les règles et connexions qui autorisent des connexions vers l'adresse IP configurée.
allow connections to the following asset building blocks	Filtre les règles et les connexions des périphériques vers ou depuis les éléments structurants d'actifs configurés.
allow connections to the following reference sets	Filtre les règles et les connexions des périphériques vers ou depuis les ensembles de référence configurés.
allow connections using the following destination ports and protocols	Filtre les règles et les connexions des périphériques vers ou depuis les ports et les protocoles configurés.
allow connections using the following protocols	Filtre les règles et les connexions des périphériques vers ou depuis les protocoles configurés.

Tableau 17. Tests relatifs aux unités/règles (suite)

Intitulé du test	Description
allow connections to the Internet	Filtre les règles et les connexions des périphériques vers ou depuis Internet.
are one of the following devices	Filtre tous les périphériques réseau sur les périphériques configurés. Ce test peut filtrer en fonction des périphériques qui sont ou ne sont pas dans la liste configurée.
are one of the following reference sets	Filtre les règles d'unité basées sur les ensembles de référence que vous spécifiez.
are one of the following networks	Filtre les règles de périphérique basées sur les réseaux que vous spécifiez.
are using one of the following adapters	Filtre les règles de périphérique basées sur les adaptateurs que vous spécifiez.

Coefficient d'importance

L'option Coefficient d'importance permet de calculer le niveau de risque et de définir le nombre de résultats renvoyés pour une question.

La plage est comprise entre 1 (faible importance) et 10 (haute importance). La valeur par défaut est 5.

Tableau 18. Matrice des résultats de coefficient d'importance

Coefficient d'importance	Résultats renvoyés pour les tests d'actifs	Résultats renvoyés pour les tests des périphériques/règles
1 (faible importance)	10 000	1 000
10 (haute importance)	1	1

Par exemple, une question de politique stipulant **have accepted communication from the internet and include only the following networks (DMZ)** requiert un facteur d'importance élevé de 10, car aucun résultat de la question n'est acceptable en raison de la nature de risque élevé de la question. Cependant, une question de politique stipulant **have accepted communication from the internet and include only the following inbound applications (P2P)** peut nécessiter un facteur d'importance moindre, étant donné que les résultats de la question n'indiquent pas de risque élevé. Vous pouvez donc surveiller cette communication à titre informatif.

Création d'une question d'actif

Recherchez sur le réseau des actifs qui violent une règle définie ou des actifs qui ont introduit un risque.

Pourquoi et quand exécuter cette tâche

Les questions du moniteur de politique d'administration sont évaluées de manière cohérente. L'ordre des questions du moniteur de politique d'administration a un impact sur les résultats.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans le menu **Actions**, sélectionnez **New Asset Question**.
4. Dans la zone **What do you want to name this question**, entrez un nom pour la question.
5. Dans la liste **Evaluate On**, sélectionnez l'une des options suivantes :

Option	Description
Actual Communication	Inclut des actifs sur lesquels ont été détectées des communications qui utilisent des connexions.
Possible Communication	Comprend tous les actifs sur lesquels les communications sont autorisées dans votre topologie de réseau, comme les pare-feux. Utilisez ces questions pour rechercher si des communications spécifiques sont possibles, qu'une communication soit ou non détectée.

- Dans la liste **Coefficient d'importance**, sélectionnez le niveau d'importance que vous voulez associer à cette question. L'option Coefficient d'importance permet de calculer le niveau de risque et de définir le nombre de résultats renvoyés pour une question.
- Déterminez l'intervalle de temps pour la question.
- Depuis la zone **Which tests do you want to include in your question**, cliquez sur l'icône d'ajout (+) en regard des tests à inclure.
- Configurez les paramètres pour vos tests dans la zone **Find Assets that**.
Les paramètres configurables sont en gras et soulignés. Cliquez sur chaque paramètre pour afficher les options actives de votre question.
- Dans la zone de groupes, cliquez sur les cases à cocher appropriées pour attribuer l'appartenance de groupe à cette question.
- Cliquez sur **Sauvegarder la question**.

Recherche des communications externes utilisant des protocoles non sécurisés

Vous pouvez utiliser une question de moniteur de politique d'administrateur basée sur la liste connue des protocoles sécurisés pour surveiller le trafic dans votre zone démilitarisée (DMZ). Dans la plupart des entreprises, le trafic réseau à travers la zone démilitarisée est limité aux protocoles connus et sécurisés, tels que HTTP ou HTTPS sur des ports spécifiques.

Pourquoi et quand exécuter cette tâche

En cas de risque, il est important de contrôler en continu le trafic dans le DMZ afin de s'assurer que seuls des protocoles sécurisés sont présents. Utilisez IBM Security QRadar Risk Manager pour effectuer cette tâche en créant une question du moniteur de politique d'administration basée sur un test d'actif pour les communications réelles.

Sélectionnez une option permettant de créer une question du moniteur de politique d'administration basée sur la liste connue des protocoles sécurisés pour DMZ.

Procédure

- Cliquez sur l'onglet **Risques**.
- Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
- Dans le menu **Actions**, sélectionnez **New Asset Question**.
- Attribuez un nom à la question dans la zone correspondante.
- Dans la liste déroulante relative au **type de données à renvoyer**, sélectionnez **Actifs**.
- Dans la liste déroulante relative au **type d'évaluation**, sélectionnez **Communication réelle**.
- Dans le menu **Coefficient d'importance**, choisissez le niveau d'importance à associer à votre question.
- Dans la section **Intervalle**, spécifiez la plage de temps de la question.
- Dans la section relative aux **tests à inclure dans la question**, sélectionnez **ont accepté la communication avec les réseaux de destination**.

10. Dans le panneau **Rechercher les actifs qui...**, cliquez sur **réseaux de destination** pour continuer à configurer ce test et indiquer votre DMZ comme réseau de destination.
11. Sélectionnez l'option **et inclure les ports de communications entrantes suivants**.
12. Dans le panneau **Rechercher les actifs qui...**, cliquez sur le paramètre **inclure uniquement** pour qu'il devienne **exclure**.
13. Cliquez sur **ports**.
14. Ajoutez les ports 80 et 443 puis cliquez sur **OK**.
15. Cliquez sur **Sauvegarder la question**.
16. Sélectionnez la question DMZ du moniteur de politique d'administration que vous avez créée.
17. Cliquez sur **Soumettre la question**.
18. Examinez les résultats pour voir si des protocoles autres que les ports 80 et 443 communiquent sur le réseau.
19. Facultatif : Examinez la question DMZ en passant en mode moniteur lors de l'optimisation des résultats.

Recherche d'actifs autorisant la communication par Internet

Les questions de politique d'administration d'IBM Security QRadar Risk Manager permettent de rechercher les actifs utilisés pour établir une communication Internet. IBM Security QRadar Risk Manager évalue la question et affiche les résultats de tous les actifs internes qui autorisent les connexions entrantes depuis Internet.

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 **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**.

Evaluation des unités autorisant des protocoles à risque

Utilisez les questions de moniteur de politique d'administration IBM Security QRadar Risk Manager pour évaluer les unités d'accès autorisant des protocoles à risque.

Pourquoi et quand exécuter cette tâche

IBM Security QRadar Risk Manager évalue une question et affiche les résultats de tous les actifs, dans votre topologie, qui correspondent à la meilleure question. 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 une infraction qui s'applique 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 liste Groupe, sélectionnez **PCI 1**.
4. Sélectionnez la question de test **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**.

Recherche des communications possibles avec les actifs protégés

Vous pouvez créer une question du moniteur de politique d'administration basée sur les adresses IP qui détecte les communications possibles avec les actifs protégés. En cas de risque, il est important de savoir quels utilisateurs de votre organisation peuvent communiquer avec les actifs de réseau critiques.

Pourquoi et quand exécuter cette tâche

IBM Security QRadar Risk Manager effectue cette tâche en créant une question du moniteur de politique d'administration basée sur un test d'actif pour les communications possibles.

Vous pouvez consulter toutes les connexions au serveur critique dans le temps, mais vous ne devez pas oublier que les employés régionaux n'accèdent pas à ces serveurs critiques. Pour ce faire, vous pouvez créer une question de moniteur de politique d'administration concernant la topologie du réseau par adresse IP.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans le menu **Actions**, sélectionnez **Nouveau**.
4. Attribuez un nom à la question dans la zone correspondante.
5. Dans la liste déroulante relative au **type de données à renvoyer**, sélectionnez **Actifs**.
6. Dans la liste déroulante relative au type d'évaluations, sélectionnez **Communications possibles**.
7. Dans la liste déroulante **Coefficient d'importance**, spécifiez un degré d'importance à associer à votre question.
8. Dans la section **Intervalle**, spécifiez une plage de temps pour la question.
9. Dans la section relative aux **tests à inclure dans la question**, cliquez deux fois pour sélectionner **ont accepté la communication avec les blocs de construction de l'actif de destination**.
10. Dans la section **Rechercher les actifs qui...**, cliquez sur **blocs de construction de l'actif** pour continuer à configurer ce test et indiquer des **actifs protégés**.

Remarque : Pour définir vos actifs distants de réseau, vous devez avoir précédemment défini vos éléments structurants d'actifs distants.

11. Dans la section relative aux **tests à inclure dans la question**, cliquez deux fois pour sélectionner le test de restriction **et inclure les adresses IP suivantes uniquement**.
12. Dans la section **Rechercher les actifs qui...**, cliquez sur **Adresses IP**.
13. Indiquez la plage d'adresse IP ou d'adresse CIDR de votre réseau distant.
14. Cliquez sur **Sauvegarder la question**.
15. Sélectionnez la question du moniteur de politique d'administration que vous avez créée pour les actifs protégés.
16. Cliquez sur **Soumettre la question**.
17. Examinez les résultats pour voir si un actif protégé accepte la communication à partir d'une adresse IP ou d'une plage de routages CIDR inconnues.
18. Facultatif : Contrôlez vos actifs protégés en définissant la question sur le mode moniteur. Si une adresse IP non reconnue se connecte à un actif protégé, QRadar Risk Manager peut générer une alerte.

Informations relatives aux questions

Vous pouvez consulter les informations relatives aux questions et paramètres du moniteur de politique d'administration sur la page **Moniteur de politique d'administration**.

Si vous souhaitez afficher des informations supplémentaires sur une question, sélectionnez-la pour en voir la description.

Si une question est en mode moniteur lorsque vous la sélectionnez, vous pouvez afficher les événements et les infractions générés à partir de la question sélectionnée.

Création d'une question relative au test des violations de règles

Créez une question relative aux unités/règles dans le moniteur de politique d'administration pour identifier les règles d'une unité ayant violé une règle définie ou ayant introduit un risque sur le réseau.

Pourquoi et quand exécuter cette tâche

Les questions du moniteur de politique d'administrateur sont évaluées selon une approche descendante. L'ordre des questions a une incidence sur les résultats.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans le menu **Actions**, cliquez sur **Nouvelle question relative aux unités/règles**.
4. Attribuez un nom à la question dans la zone correspondante.
5. Dans la liste **Coefficient d'importance**, sélectionnez le niveau d'importance à associer à cette question.
6. Dans la zone relative aux **tests à inclure dans la question**, cliquez sur l'icône + en regard des tests à inclure.
7. Dans la zone **Recherche les unités/règles qui**, configurez les paramètres pour vos tests.
Les paramètres configurables sont en gras et soulignés. Cliquez sur chaque paramètre pour afficher les options actives de votre question.
8. Dans la zone de groupes, cliquez sur les cases à cocher appropriées pour attribuer l'appartenance de groupe à cette question.
9. Cliquez sur **Sauvegarder la question**.

Recherche des unités/règles établissant une communication par Internet

Dans le moniteur de politique d'administration, des tests d'unités sont mis en place pour identifier les règles d'une unité qui violent une règle prédéfinie ou les modifications susceptibles d'introduire des risques dans l'environnement.

Pourquoi et quand exécuter cette tâche

Les tests d'unités permettent d'identifier les règles d'une unité qui violent une règle définie ou les modifications qui introduisent un risque dans l'environnement. Du point de vue de la sécurité des réseaux, il convient d'être au courant des modifications apportées aux règles de l'unité. Une situation courante concerne l'accès illicite de serveurs à Internet du fait de la modification des paramètres de pare-feu sur le réseau. IBM Security QRadar Risk Manager peut surveiller les changements de règles des unités réseau en créant une question du moniteur de politique d'administration basée sur les règles de l'unité.

Créez une question du moniteur de politique d'administration qui vérifie les accès Internet des unités.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.

3. Dans le menu **Actions**, sélectionnez l'option permettant de créer **une question relative aux unités/règles**.
4. Dans la zone relative au **type de données à renvoyer**, sélectionnez **Unités/Règles**.
5. Dans la liste **Coefficient d'importance**, sélectionnez le niveau d'importance à associer à la question.
6. Dans la section relative aux **tests à inclure dans la question**, cliquez sur l'icône + en regard du test d'**autorisation des connexions Internet** pour l'ajouter à votre question.
7. Cliquez sur **Sauvegarder la question**.
8. Sélectionnez la question du moniteur de politique d'administration que vous avez créée pour surveiller les règles de l'unité.
9. Cliquez sur **Soumettre la question**.
10. Examinez les résultats pour voir si des règles autorisent l'accès à Internet.
11. Facultatif : Surveillez les actifs protégés en définissant la question du moniteur de politique d'administration sur le mode moniteur.

Soumission d'une question

Vous pouvez soumettre une question pour déterminer le risque associé. Vous pouvez également déterminer le temps requis pour exécuter une question et la quantité de données interrogées.

Pourquoi et quand exécuter cette tâche

Lorsque vous soumettez une question, les informations résultantes dépendent des données interrogées ; actifs ou périphériques et règles.

Une fois la question du moniteur de politique d'administration soumise, vous pouvez afficher le temps requis pour l'exécution de la question. Le temps requis pour exécuter la politique indique également la quantité de données interrogées. Par exemple, si le temps d'exécution est de 3 heures, il y a 3 heures de données. Vous pouvez afficher le temps dans la colonne **Policy Execution Time** pour déterminer une fréquence d'intervalle efficace à configurer pour les questions à contrôler. Par exemple, si le temps d'exécution de la politique est de 3 heures, l'intervalle d'évaluation de la politique doit être supérieur à 3 heures.

Remarque : Lorsque vous éditez une question après sa soumission et que la modification affecte les tests associés, l'affichage de ces modifications peut prendre jusqu'à une heure.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Sélectionnez la question que vous souhaitez soumettre.
4. Cliquez sur **Soumettre la question**.

Résultats d'une question d'actif

Les résultats de l'actif s'affichent une fois que vous soumettez une question du moniteur de politique d'administration.

Le **niveau de risque** indique le niveau de risque associé à cette question. Le calcul du **Score de risque** repose sur le facteur d'importance attribué à la question, et sur le nombre de résultats retournés pour la question.

Les paramètres des résultats de l'actif sont décrits dans le tableau suivant.

Tableau 19. Résultats d'actifs

Paramètre	Description
IP	Adresse IP de l'actif.
Nom	Nom de l'actif tel qu'il apparaît dans le profil d'actif. Pour plus d'informations sur les profils d'actifs, voir le <i>IBM Security QRadar - Guide d'utilisation</i> .
Vlan	Nom du réseau local virtuel associé à l'actif.
Poids	Pondération de l'actif telle qu'elle apparaît dans le profil d'actif.
Port(s) de destination	Liste des ports de destination associée à cet actif dans le cadre des tests de question. S'il existe plusieurs ports associés à cet actif et à cette question, cette zone indique Multiple et le nombre de ports. La liste des ports est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les ports uniques dans lesquels l'actif était la source, la destination ou la connexion. Cliquez sur Multiple (N) pour afficher les connexions. Cet écran comprend les connexions agrégées par port, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.
Protocole(s)	Liste des protocoles associée à cet actif dans le cadre des tests de question. S'il existe plusieurs protocoles associés à cet actif et à cette question, cette zone indique Multiple et le nombre de protocoles. La liste des protocoles est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les protocoles uniques dans lesquels l'actif était la source, la destination ou la connexion. Cliquez sur Multiple (N) pour afficher les connexions. Cet écran comprend les connexions agrégées par protocole, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.
Application(s) de flux	Liste des applications associée à cet actif dans le cadre des tests de question. S'il existe plusieurs applications associées à cet actif et à cette question, cette zone indique Multiple et le nombre d'applications. La liste des applications est obtenue en filtrant les connexions associées à cette question afin d'obtenir toutes les applications uniques dans lesquelles l'actif était la source, la destination ou la connexion. Cliquez sur Multiple (N) pour afficher les connexions. Cet écran comprend les connexions agrégées par application, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.

Tableau 19. Résultats d'actifs (suite)

Paramètre	Description
Vulnérabilité(s)	<p>Liste des vulnérabilités associée à cet actif dans le cadre des tests de question. S'il existe plusieurs vulnérabilités associées à cet actif et à cette question, cette zone indique Multiple et le nombre de vulnérabilités.</p> <p>La liste des vulnérabilités est obtenue en utilisant une liste de toutes les vulnérabilités compilées à partir des tests associés et en utilisant cette liste pour filtrer les vulnérabilités détectées sur cet actif. Si aucune vulnérabilité n'est spécifiée pour cette question, toutes les vulnérabilités de l'actif sont utilisées pour compiler cette liste.</p> <p>Cliquez sur Multiple (N) pour afficher les actifs. Cet écran comprend les connexions agrégées par vulnérabilité, filtrées par l'adresse IP d'actif et basées sur l'intervalle de temps spécifié dans la question.</p>
Nombre de flux	<p>Nombre total de flux associé à cet actif dans le cadre des tests de question.</p> <p>Le nombre de flux est déterminé en filtrant les connexions associées à cette question afin d'obtenir le nombre total de flux dans lesquels l'actif était la source, la destination ou la connexion.</p>
Source(s)	<p>Liste des adresses IP source associées à cet actif dans le cadre des tests de question. S'il existe plusieurs adresses IP source associées à cet actif et à cette question, cette zone indique Multiple et le nombre d'adresses IP source. La liste des adresses IP source est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les adresses IP source uniques dans lesquelles l'actif est la destination de la connexion.</p> <p>Cliquez sur Multiple (N) pour afficher les connexions. Cet écran comprend les connexions agrégées par adresse IP source, filtrées par l'adresse IP d'actif basée sur l'intervalle de temps spécifié dans la question.</p>
Destination(s)	<p>Liste des adresses IP de destination associées à cet actif dans le cadre des tests de question. S'il existe plusieurs adresses IP de destination associées à cet actif et à cette question, cette zone indique Multiple et le nombre d'adresses IP de destination. La liste des adresses IP de destination est obtenue en filtrant les connexions associées à cette question afin d'obtenir tous les adresses IP de destination uniques dans lesquelles l'actif est la source de la connexion.</p> <p>Cliquez sur Multiple (N) pour afficher les connexions. Cet écran comprend les connexions agrégées par adresse IP de destination, filtrées par l'adresse IP d'actif basée sur l'intervalle de temps spécifié dans la question.</p>

Tableau 19. Résultats d'actifs (suite)

Paramètre	Description
Octets source du flux	<p>Nombre total d'octets source associé à cet actif dans le cadre des tests de question.</p> <p>Le nombre d'octets source est déterminé en filtrant les connexions associées à cette question afin d'obtenir le nombre total d'octets source dans lequel l'actif est la source de la connexion.</p>
Octets de destination du flux	<p>Nombre total d'octets de destination associé à cet actif dans le cadre des tests de question.</p> <p>Le nombre d'octets de destination est déterminé en filtrant les connexions associées à cette question afin d'obtenir le nombre total d'octets de destination dans lequel l'actif est la destination de la connexion.</p>

Résultats de la question relative aux unités/règles

Les résultats relatifs aux unités/règles s'affichent une fois que vous soumettez une question de moniteur de politique d'administration.

Le **Score de risque** affiché indique le niveau de risque associé à cette question. Le calcul du **Score de risque** repose sur le facteur d'importance attribué à la question, et sur le nombre de résultats retournés pour la question.

Les paramètres des résultats d'unités et de règles sont décrits dans le tableau suivant.

Tableau 20. Résultats des unités et règles

Paramètre	Description
IP unité	Adresse IP de l'unité.
Nom de l'unité	Nom de l'unité tel qu'il apparaît dans le moniteur de configuration.
Type d'unité	<p>Type d'unité tel qu'il apparaît dans le profil d'actif.</p> <p>Pour plus d'informations sur les profils d'actifs, voir le <i>IBM Security QRadar - Guide d'utilisation</i>.</p>
Liste	Nom de la règle provenant de l'unité.
Entrée	Numéro d'entrée de la règle.
Action	Action associée à la règle correspondant de l'unité. Les options sont les suivantes : permit, deny ou NA.
Source(s)	<p>Réseau source associé à cet actif.</p> <p>Les sources avec un hyperlien indiquent une référence de groupe d'objets. Cliquez sur le lien pour afficher des informations détaillées sur la ou les références de groupe d'objets.</p>

Tableau 20. Résultats des unités et règles (suite)

Paramètre	Description
Service(s) source	<p>Ports source et comparaison associés à la règle correspondante du périphérique au format suivant :</p> <p><comparison>:<port></p> <p>Où</p> <p><comparison></p> <p>peut inclure une des options suivantes :</p> <p>eq - Est égal à</p> <p>ne - N'est pas égal à</p> <p>lt - Inférieur à</p> <p>gt - Supérieur à</p> <p>Par exemple, si le paramètre indique ne:80, tous les ports autres que 80 s'appliquent à ce service source. Si le paramètre indique lt:80, la plage de ports applicables est comprise entre 0 et 79.</p> <p>Ce paramètre affiche le port source de la règle de périphérique. S'il n'existe aucun port pour cette règle de périphérique, le terme NA s'affiche.</p> <p>Les services source avec un hyperlien indiquent une référence de groupe d'objets. Cliquez sur le lien pour afficher des informations détaillées sur la ou les références de groupe d'objets.</p>
Destination(s)	<p>Réseau de destination associé à la règle correspondante du périphérique.</p> <p>Les destinations avec un hyperlien indiquent une référence de groupe d'objets. Cliquez sur le lien pour afficher des informations détaillées sur la ou les références de groupe d'objets.</p>

Tableau 20. Résultats des unités et règles (suite)

Paramètre	Description
Service(s) de destination	<p>Les ports de destination et la comparaison associés à la règle correspondante du périphérique s'affichent au format suivant : <comparison>:<port></p> <p>Où <comparison></p> <p>peut inclure une des options suivantes :</p> <p>eq - Est égal à</p> <p>ne - N'est pas égal à</p> <p>lt - Inférieur à</p> <p>gt - Supérieur à</p> <p>Par exemple, si le paramètre indique ne:80, tous les ports autres que 80 s'appliquent à ce service de destination. Si le paramètre indique lt:80, la plage de ports applicables est comprise entre 0 et 79.</p> <p>Ce paramètre affiche le port de destination de la règle de périphérique. S'il n'existe aucun port pour cette règle de périphérique, le terme NA s'affiche.</p> <p>Les services de destination avec un hyperlien indiquent une référence de groupe d'objets. Cliquez sur le lien pour afficher des informations détaillées sur la ou les références de groupe d'objets.</p>
Groupe(s) utilisateur(s)	Utilisateurs ou groupes associés à la règle correspondante du périphérique.
Protocole(s)	Protocole ou groupe de protocoles associé à la règle correspondant du périphérique.
Signature(s)	Signature de ce périphérique uniquement affichée pour une règle de périphérique IP.
Applications	Applications associé à la règle correspondante du périphérique.

Evaluation des résultats à partir des questions du moniteur de politique d'administration

Vous pouvez évaluer les résultats qui sont renvoyés d'une question de moniteur de politique d'administration dans IBM Security QRadar Risk Manager.

La validation du résultat d'une question revient à configurer votre système de sorte qu'IBM Security QRadar Risk Manager sache que l'actif associé au résultat de la question est sécurisé ou peut être ignoré à l'avenir.

Lorsqu'un utilisateur valide un résultat d'actif, le moniteur de politique d'administration voit ce résultat d'actif comme validé et lorsque la question du moniteur est à nouveau soumise ou contrôlée, l'actif n'est pas répertorié dans les résultats de la question. L'actif validé ne s'affiche pas dans la liste de résultats de

la question à moins que la validation ne soit révoquée. Le moniteur de politique d'administration enregistre l'utilisateur, l'adresse de l'unité, le motif de l'approbation, l'unité ou la règle applicable, ainsi que la date et l'heure.

Validation des résultats

Les résultats du moniteur de politique d'administration approuvés ne sont pas renvoyés à partir des questions du moniteur de politique d'administration. Approuvez les résultats des questions qui ne présentent pas de risque dans votre réseau.

Procédure

1. Dans la table de résultats, cochez la case en regard des résultats à valider.
2. Sélectionnez une des options suivantes :

Option	Description
Tout valider	Sélectionnez cette option pour valider tous les résultats.
Valider les actifs sélectionnés	Cochez la case en regard des résultats à approuver, puis cliquez sur Valider les actifs sélectionnés .

3. Entrez le motif de la validation.
4. Cliquez sur **OK**.
5. Cliquez sur **OK**.
6. Pour **afficher les résultats validés** de la question, cliquez sur l'option prévue à cet effet.

Résultats

La fenêtre Résultats de question approuvés fournit les informations suivantes :

Tableau 21. Paramètres de la fenêtre Résultats de question approuvés

Paramètre	Description
Unité/Règle	Unité associée au résultat dans Résultats relatifs aux unités/règles .
IP	Adresse IP associée à l'actif dans Résultats d'actifs .
Approuvé par	Utilisateur qui a validé les résultats.
Approuvé le	Date et l'heure de validation des résultats.
Notes	Affiche le texte des notes associées à ce résultat et le motif d'approbation de la question.

Si vous souhaitez supprimer les validations d'un résultat, cochez la case de chaque résultat dont vous souhaitez supprimer la validation et cliquez sur **Revoke Selected**. Pour supprimer toutes les validations, cliquez sur **Revoke All**.

Surveillance de la question de politique d'administration

IBM Security QRadar Risk Manager peut surveiller toutes les questions prédéfinies ou définies par l'utilisateur dans le moniteur de politique d'administration. Utilisez le mode moniteur pour générer des événements dans QRadar Risk Manager.

Lorsque vous surveillez une question de politique d'administration, QRadar Risk Manager analyse la question toutes les heures par rapport à votre topologie afin de déterminer si un changement d'actif ou de règle génère un résultat non approuvé. Si QRadar Risk Manager détecte un résultat non approuvé,

une infraction peut être générée pour vous avertir d'un changement dans votre politique. 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 l'affichage des événements, de la corrélation, du rapport d'événement, des règles personnalisées et des tableaux de bord dans QRadar SIEM.

Surveillance d'une question de moniteur de politique d'administration et génération d'événements

Surveillez les résultats des questions de moniteur de politique d'administration et configurez la génération des événements lorsque les résultats des questions changent. Vous pouvez définir l'intervalle d'évaluation de politique et configurer les événements pour lesquels envoyer une notification.

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 la valeur des paramètres ci-après.
6. Cliquez sur **Sauvegarder le moniteur**.
Les paramètres que vous configurez pour un événement sont décrits dans le tableau suivant.

Tableau 22. Paramètres d'événements de question

Paramètre	Description
Intervalle d'évaluation de politique	Fréquence d'exécution de l'événement.
Nom d'événement	Nom de l'événement que vous souhaitez afficher dans les onglets Activité du journal et Infractions .
Description de l'événement	Description de l'événement. La description est affichée dans le panneau Annotations des détails de l'événement.
Catégorie de niveau supérieur	Catégorie d'événement de niveau supérieur que vous souhaitez que cette règle utilise pendant le traitement des événements.
Catégorie de niveau inférieur	Catégorie d'événements de niveau inférieur que vous souhaitez que cette règle utilise pendant le traitement des événements.
Vérifier que l'événement attribué fait partie d'une infraction	Transfère les événements vers le composant Magistrat. Si aucune infraction n'est générée, une nouvelle est créée. Si une infraction existe, cet événement est ajouté. Si vous effectuez des corrélations par question ou simulation, tous les événements d'une question sont associés à une infraction unique. Si vous effectuez des corrélations par actif, une infraction unique est créée ou mise à jour pour chaque actif unique.
Envoyer les événements ayant passé la question	Transfère des événements qui transmettent la question du moniteur de politique d'administration au composant Magistrat.

Tableau 22. Paramètres d'événements de question (suite)

Paramètre	Description
Ajustements du score de vulnérabilité	Ajuste le score du risque de vulnérabilité d'un actif, en fonction de la réussite ou de l'échec de la question. Les scores du risque de vulnérabilité sont ajustés dans IBM Security QRadar Vulnerability Manager.
Actions supplémentaires	<p>Actions supplémentaires à entreprendre lors de la réception d'un événement.</p> <p>Séparez les différentes adresses électroniques par des virgules.</p> <p>Sélectionnez Envoyer une notification si vous voulez que les événements générés à la suite de cette question contrôlée s'affichent dans l'élément System Notifications du tableau de bord.</p> <p>Le résultat syslog peut se présenter comme suit :</p> <pre>Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name:SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description</pre>
Activer le moniteur	Contrôlez la question.

Questions de groupe

Vous pouvez regrouper et afficher vos questions en fonction de vos critères choisis

Utilisez des groupes pour afficher et suivre efficacement vos questions. Par exemple, vous pouvez afficher toutes les questions relatives à la conformité. Effectuez les tâches ci-dessous avec des groupes :

- Création d'un groupe pour les questions.
- Affectation d'une question à un groupe.
- Edition ou suppression de questions dans un groupe.
- Copie d'une question dans un ou plusieurs groupes.

Exportation et importation de questions du moniteur de politique d'administration

Les utilisateurs ayant des privilèges administratifs peuvent exporter et importer les questions du moniteur de politique d'administration.

Les questions d'exportation et d'importation fournissent une méthode pour sauvegarder les questions et les partager avec d'autres utilisateurs IBM Security QRadar Risk Manager.

Restrictions pour les informations sensibles

Les informations sensibles d'entreprise ou de politique peuvent être incluses dans les dépendances. Lorsque vous exportez ou importez les questions du moniteur de politique d'administration, les données sensibles contenues dans les dépendances ne sont pas incluses.

Les questions du moniteur de politique d'administration peuvent contenir les types de dépendances suivants :

- Éléments structurant d'actif
- Recherches sauvegardées d'actifs
- Réseaux
- Emplacements réseau distant

- Emplacements réseau géographique
- Ensembles de référence

Avant d'exporter des questions ayant des dépendances, vous pouvez choisir de fournir plus de contexte sur le type d'informations contenu dans la dépendance. Fournir ces informations permet à d'autres utilisateurs de comprendre quel type d'information référencer lorsqu'ils importent la question dans leur moniteur de politique d'administration.

Exportation de questions de moniteur de politique d'administration

Vous pouvez exporter une ou plusieurs questions de moniteur de politique d'administration vers un fichier XML. L'exportation des questions de moniteur de politique d'administration est utile pour sauvegarder vos questions ou les partager avec d'autres utilisateurs.

Pourquoi et quand exécuter cette tâche

Si des questions de moniteur de politique d'administration comprennent des dépendances, vous pouvez fournir plus de contexte sur le type d'informations contenu dans la dépendance.

Le nom du fichier XML par défaut pour les questions exportées est `policy_monitor_questions_export.xml`.

Procédure

1. Sous l'onglet **Risques**, cliquez sur **Moniteur de politique d'administration**.
2. Sélectionnez une des options suivantes :
 - Pour exporter toutes les questions, dans le menu **Actions**, sélectionnez **Tout exporter**.
 - Pour exporter des questions spécifiques, appuyez sur la touche Ctrl pour sélectionner chaque question que vous souhaitez exporter, puis à partir du menu **Actions**, sélectionnez **Exporter la sélection**.
3. Facultatif : Si des questions contiennent des dépendances, cliquez sur le lien du paramètre pour entrer davantage d'informations. La longueur maximale de caractères pour cette zone est 255.
4. Cliquez sur **Exporter les questions**.

Résultats

Un fichier par défaut, appelé `policy_monitor_questions_export.xml`, est exporté vers votre répertoire de téléchargement.

Importation des questions de moniteur de politique d'administration

Importez une ou plusieurs questions du moniteur de politique d'administration dans IBM Security QRadar Risk Manager.

Pourquoi et quand exécuter cette tâche

Le processus d'importation ne met pas à jour les questions existantes. Chaque question importée devient une nouvelle question dans le moniteur de politique d'administration. Un horodatage est ajouté à toutes les questions importées.

Si une question importée contient une dépendance, un avertissement s'affiche dans la colonne **Etat**. Les questions importées avec des dépendances contiennent des paramètres sans valeur. Pour vous assurer que les questions de moniteur de politique d'administration importées fonctionnent comme prévu, vous devez affecter des valeurs aux paramètres.

Procédure

1. Sous l'onglet **Risques**, cliquez sur **Moniteur de politique d'administration**.
2. Dans le menu **Actions**, sélectionnez **Importer**.
3. Cliquez sur **Choisir un fichier** et accédez au fichier XML que vous souhaitez importer.
4. Cliquez sur **Ouvrir**.
5. Sélectionnez un ou plusieurs groupes pour affecter la question à un groupe.
6. Cliquez sur **Importer une question**.
7. Vérifiez la colonne **Etat** pour les avertissements. Si une question contient un avertissement, ouvrez la question et modifiez les paramètres de dépendance. Sauvegardez la question une fois les paramètres mis à jour.

Que faire ensuite

La surveillance n'est pas activée sur les questions importées. Vous pouvez créer un événement pour contrôler les résultats des questions qui ont été importées.

Intégration à QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager s'intègre à IBM Security QRadar Risk Manager pour vous aider à hiérarchiser les risques et vulnérabilités dans votre réseau.

Politiques de risque et hiérarchisation des vulnérabilités

Vous pouvez intégrer QRadar Vulnerability Manager à QRadar Risk Manager en définissant et surveillant les politiques de risque des actifs ou vulnérabilités.

Lorsque les règles d'administration des risques que vous définissez dans QRadar Risk Manager réussissent ou échouent, les scores de risque des vulnérabilités sont ajustés dans QRadar Vulnerability Manager. Les niveaux d'ajustement dépendent des politiques de risque dans votre organisation.

Lorsque les scores du risque de vulnérabilité sont ajustés dans QRadar Vulnerability Manager, les administrateurs peuvent effectuer les tâches suivantes :

- Obtenir une visibilité immédiate des vulnérabilités ayant fait échouer une politique de risque.
Par exemple, les nouvelles informations peuvent s'afficher sur le tableau de bord QRadar ou être envoyées par e-mail.
- Redéfinissez la priorité des vulnérabilités qui ont besoin d'une attention immédiate.
Par exemple, un administrateur peut utiliser l'option **Score de risque** pour identifier rapidement les vulnérabilités à haut risque.

Si vous appliquez les politiques de risque au niveau d'un actif dans QRadar Risk Manager, toutes les vulnérabilités sur cet actif voient leurs scores de risque ajustés.

Surveillance des comptages d'événements de règle de pare-feu des périphériques Check Point

Dans IBM Security QRadar Risk Manager, vous pouvez surveiller le nombre d'événements de règle de pare-feu de votre périphérique Check Point en l'intégrant au SMS Check Point. Vous pouvez voir ces interactions de règle dans QRadar Risk Manager, et utiliser des rapports de règle pour gérer l'efficacité des règles de votre réseau.

Dans l'image ci-dessous, QRadar reçoit et traite les journaux d'événement de règle des périphériques de pare-feu Check Point via le SMS.

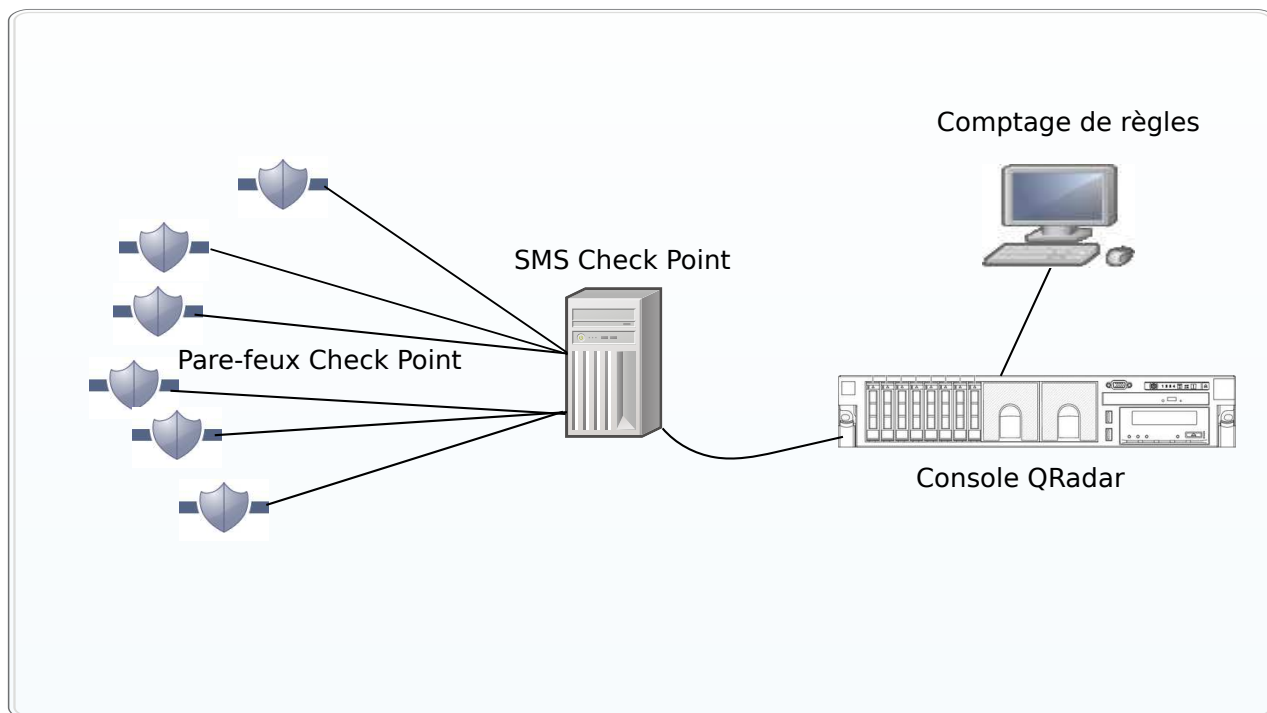


Figure 1. Comptage des règles Check Point

Scénario - Implémentation de la surveillance des règles de pare-feu Check Point dans QRadar

Vous êtes administrateur de systèmes réseau chargé de la sécurité réseau dans une organisation qui utilise Check Point pour implémenter ses règles de sécurité réseau. Le réseau comporte plusieurs pare-feux Check Point qui sont gérés depuis un serveur SMS (Security Management Server) Check Point.

Vous souhaitez afficher des rapports sur l'usage quotidien des règles, afin de disposer d'une meilleure visibilité de votre implémentation de règles.

Vous devez configurer une connexion entre votre système SMS Check Point et QRadar, de sorte QRadar reçoit des journaux d'événement de règle depuis les périphériques Check Point. QRadar traite ces informations de journal d'événement de règle et les affiche pour tous les périphériques qui sont gérés par des pare-feux Check Point. Depuis le tableau de règles QRadar, vous pouvez analyser l'utilisation et l'efficacité des règles de pare-feu en surveillant le nombre d'événements, puis affiner vos règles pour des performances optimales.

Utilisez les informations de règle pour effectuer les tâches suivantes :

- Afficher les règles les moins utilisées et les plus utilisées.
- Evaluer l'aspect pratique des règles qui sont rarement déclenchées.
- Afficher les règles qui bloquent peut-être inutilement l'accès réseau.
- Afficher les règles qui se déclenchent de manière excessive, et appliquer une charge sur la bande passante de votre réseau.
- Afficher des événements détaillés.
- Planifier des rapports.

Avant de commencer, téléchargez l'ensemble d'adaptateurs le plus récent depuis FixCentral, et installez-le sur votre hôte géré QRadar.

Procédez comme suit pour configurer le comptage de règles :

1. Configurez des applications OPSEC dans Check Point SmartDashboard.
2. Créez une source de journal dans QRadar.
3. Configurez la Configuration Source Management dans QRadar Risk Manager. Lancez la reconnaissance et la sauvegarde des périphériques dans Configuration Source Management.
4. Terminez les configurations afin d'afficher les comptages de règles.

Configuration des applications OPSEC dans SmartDashboard

Créez et configurez 2 applications OPSEC dans votre Check Point SmartDashboard. Vous pourrez ainsi simplifier le transfert de fichiers journaux entre Check Point et IBM Security QRadar.

Pourquoi et quand exécuter cette tâche

Créez 2 applications OPSEC (Open Platform for Security), la première avec la propriété d'entité client CPMI (Check Point Management Interface) pour QRadar Risk Manager, et la seconde avec la propriété d'entité client LEA (Log Export API) pour la source de journal QRadar Risk Manager.

Procédure

1. Depuis le menu **Manage** dans la barre d'outils, cliquez sur **Servers and OPSEC Applications**.
2. Cliquez sur **New > OPSEC Application**.
3. Dans la zone **Name**, entrez un nom pour l'application.
4. Dans la liste **Host**, sélectionnez un hôte ou cliquez sur **New** pour en ajouter un.
5. Sous **Client Entities**, sélectionnez la case à cocher **CPMI**.
Cette option est obligatoire pour QRadar Risk Manager Configuration Source Management (CSM).
6. Cliquez sur **Communication**.
7. Dans la zone **One-time password**, entrez un mot de passe et confirmez-le.
Le mot de passe est utilisé plusieurs fois pendant la configuration et vous devez le réutiliser de sorte que QRadar puisse utiliser un certificat de sécurité de Check Point.
8. Cliquez sur **Initialize**.
La zone **Trust state** prend la valeur : **Initialized but trust not established**.
9. Cliquez sur **Close**.
10. Pour remplir la zone **DN** de la section Secure Internal Communication, cliquez sur **OK**.
11. Pour afficher la zone **DN** remplie, sélectionnez OPSEC Application et cliquez sur **Edit**.
La zone **DN** est maintenant remplie. Ces informations sont utilisées par les zones **Application Object SIC Attribute (SIC Name)** et **SIC Attribute (SIC Name)** lors de la configuration de la source de journal et de Configuration Source Management dans QRadar.
12. Créez la seconde application OPSEC à utiliser avec la source de journal.
Suivez les étapes 1 à 11 pour créer la première application OPSEC, avec deux exceptions :
 - Pour la zone **Name** à l'étape 3, utilisez un nom différent de celui de la première application OPSEC.
 - Pour la zone **Client Entities** à l'étape 5, sélectionnez la case à cocher **LEA**.
 Assurez-vous que la zone **Trust state** affiche **Initialized but trust not established**.

Conseil : Utilisez le mot de passe à utilisation unique pour cette application OPSEC afin d'éviter toute confusion entre les mots de passe.
13. Dans SmartDashboard, fermez toutes les fenêtres jusqu'à la fenêtre principale de SmartDashboard.
14. Depuis le menu **Policy** dans la barre d'outils, cliquez sur **Install**.
15. Cliquez sur **Install on all selected gateways, if it fails do not install on gateways of the same version**.

Que faire ensuite

L'étape suivante consiste à configurer la source du journal dans QRadar.

Configuration de la source de journal

Configurez la source de journal dans IBM Security QRadar afin d'obtenir un certificat de Check Point et de recevoir des informations de journal.

Procédure


1. Connectez-vous au QRadar.
2. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
3. Cliquez sur **Sources de données**.
Le panneau Sources de données s'affiche.
4. Cliquez sur l'icône **Sources de journal**.
5. Cliquez sur **Ajouter**.
6. Configurez les valeurs suivantes :

Tableau 23. Paramètres de source de journal Check Point

Paramètre	Description
Nom de la source de journal	Identificateur de la source de journal.
Description de la source de journal	La description est facultative.
Type de source de journal	Sélectionnez Check Point FireWall-1 .
Configuration de protocole	Sélectionnez OPSEC/LEA .
Identificateur de la source de journal	Adresse IP de votre SMS
IP serveur	Entrez l'adresse IP de votre SMS
Port du serveur	Utilisez le port 18184.
Utiliser IP serveur pour source du journal	Ne cochez pas cette case.
Intervalle du rapport de statistiques	La valeur par défaut est 600.
Type d'authentification	Dans la liste, sélectionnez sslca .
Attribut SIC d'objet application OPSEC (nom SIC)	Depuis Check Point SmartDashboard, cliquez sur Manage > Servers and OPSEC Applications et sélectionnez l'application OPSEC qui a la propriété d'entité client LEA. Cliquez sur Edit , puis copiez l'entrée de la zone DN , et collez-la dans la zone Attribut SIC d'objet application OPSEC (nom SIC) .

Tableau 23. Paramètres de source de journal Check Point (suite)

Paramètre	Description
Attribut SIC de la source de journal (Nom SIC de l'entité)	<p>Utilisez l'entrée que vous avez collé dans la zone Attribut SIC d'objet application OPSEC (nom SIC), supprimez le texte de la zone CN= property value, et effectuez les modifications suivantes :</p> <p>Pour la valeur de propriété CN=, utilisez cp_mgmt_ <hostname ></p> <p>où <hostname> est le nom Host de la fenêtre OPSEC Application Properties.</p> <p>Consultez les exemples suivants pour OPSEC Application DN et OPSEC Application Host, qui permettent de créer le nom SIC d'entité :</p> <p>OPSEC Application DN : CN=cpsmsxxx,0=svxxx-CPSMS..bsaobx</p> <p>OPSEC Application Host : Srvxxx-SMS</p> <p>Utilisez le texte des zones OPSEC Application DN et OPSEC Application Host pour la zone Entity SIC Name:</p> <p>CN=cp_mgmt_Srvxxx-SMS,0=svxxx-CPSMS..bsaobx</p> <p>Le contenu de la zone Entity SIC Name dans cette configuration dépend de la configuration d'une passerelle pour le serveur de gestion. Si votre adresse SMS n'est pas utilisée en tant que passerelle, utilisez la configuration de serveur de gestion pour la zone Entity SIC Name, qui est représentée par le texte suivant :</p> <p>CN=cp_mgmt,0=<take_0_value_from_DN_field></p>
Indiquer un certificat	Ne sélectionnez pas cette case à cocher.
Adresse IP de l'autorité de certification	Entrez l'adresse IP du SMS.
Mot de passe du certificat d'extraction	Mot de passe que vous avez indiqué pour OPSEC Applications Properties dans la zone One-time password de la fenêtre Communication.
Application OPSEC	Nom que vous avez indiqué dans la zone Name de la fenêtre OPSEC Applications Properties.
Activé	Sélectionnez cette case pour activer la source de journal. Par défaut, cette option est activée.
Crédibilité	La plage est comprise entre 0 et 10. La crédibilité indique l'intégrité d'un événement ou d'une infraction telle que définie par le classement de crédibilité des périphériques source. La crédibilité s'accroît lorsque plusieurs sources signalent le même événement. La valeur par défaut est 5.
Collecteur d'événement cible	Dans la liste, sélectionnez le Collecteur d'événement cible à utiliser comme cible pour la source du journal.
Événements en coalescence	Active la source du journal pour la coalescence (bundle) des événements. Par défaut, les sources de journal détectées automatiquement héritent de la valeur de la liste Événements en coalescence des propriétés de Paramètres système dans QRadar. Lorsque vous créez une source de journal ou éditez une configuration existante, vous pouvez remplacer la valeur par défaut en configurant cette option pour chaque source de journal.
Stocker le contenu de l'événement	Active la source du journal pour le stockage des informations du contenu de l'événement. Par défaut, les sources de journal détectées automatiquement héritent de la valeur de la liste Stocker le contenu de l'événement des propriétés de Paramètres système dans QRadar. Lorsque vous créez une source de journal ou éditez une configuration existante, vous pouvez remplacer la valeur par défaut en configurant cette option pour chaque source de journal.

7. Cliquez sur **Sauvegarder**.

8. Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Si vous constatez que les modifications sont implémentées automatiquement, il est néanmoins conseillé de cliquer sur **Déployer les changements**.

Vérifiez que la confiance est établie pour l'application OPSEC qui a la propriété d'entité client LEA, en consultant la zone **Trust State** dans la fenêtre Communication de OPSEC Application Properties.

La configuration de la source du journal est terminée.

Pour plus d'informations sur la configuration des sources de journal, voir *IBM Security QRadar Managing Log Sources Guide*.


Etablissement d'une communication sécurisée entre Check Point et IBM Security QRadar

Configurez Configuration Source Management dans IBM Security QRadar afin de vous connecter à Check Point SMS. Ajoutez les détails de l'application OPSEC de SmartDashboard, et demandez un certificat de sécurité Check Point.

Pourquoi et quand exécuter cette tâche

Configurez les détails de l'application OPSEC dans Configuration Source Management et définissez l'échange de certificats. Une fois la configuration terminée, utilisez Configuration Source Management pour détecter la nouvelle entrée.

Procédure

1. Ouvrez une session dans QRadar en tant qu'administrateur.
2. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
3. Cliquez sur **Applications** ou faites défiler l'écran jusqu'à l'icône **Configuration Source Management**.
4. Cliquez sur l'icône **Configuration Source Management**.
5. Dans le menu de navigation, cliquez sur **Credentials**.
6. Dans le panneau Network Groups, cliquez sur le symbole (+).
7. Entrez un nom pour le groupe du réseau.
8. Dans la zone **Add address (IP, CIDR, Wildcard, or Range)**, entrez l'adresse IP de votre SMS.
9. Cliquez sur (+) pour ajouter l'adresse IP.
10. Entrez votre nom d'utilisateur et mot de passe SMS SmartDashboard.

Pour configurer les zones OPSEC, utilisez les informations de la fenêtre OPSEC Application Properties de SmartDashboard, dans laquelle vous avez sélectionné la case à cocher **CPMI** pour l'entité client.

11. Copiez et collez les informations de la zone **DN** dans la zone **OPSEC Entity SIC Name**.
12. Editez l'entrée que vous avez entrée dans la zone **OPSEC Entity SIC Name** en remplaçant la valeur de propriété CN= par : cp_mgmt_<hostname>

où <hostname> est le nom **Host** utilisé pour la zone **Host** de l'application OPSEC.

Consultez les exemples suivants pour OPSEC Application DN et OPSEC Application Host, qui permettent de créer le nom SIC d'entité :

- OPSEC Application DN : CN=cpsmsxxx,0=svxxx-CPSMS..bsaobx
- OPSEC Application Host : Srvxxx-SMS

Utilisez le texte des zones OPSEC Application DN et OPSEC Application Host pour la zone **Entity SIC Name**:

Entity SIC Name correspond à CN=cp_mgmt_Srvxxx-SMS,0=svxxx-CPSMS..bsaobx

Le contenu de la zone **Entity SIC Name** dans cette configuration dépend de la configuration d'une passerelle pour le serveur de gestion. Si votre adresse IP SMS n'est pas utilisée comme passerelle, utilisez la configuration du serveur de gestion du tableau :

Tableau 24. Formats du nom SIC d'entité

Type	Nom
Serveur de gestion	CN=cp_mgmt,0=<take_0_value_from_DN_field>
Passerelle vers un serveur de gestion	CN=cp_mgmt_<gateway_hostname>,0=<take_0_value_from_DN_field>

13. Copiez et collez les informations de la zone **DN** dans la zone **OPSEC Application Object SIC Name**.
14. Cliquez sur **Get Certificate**.
15. Entrez l'adresse IP SMS dans la zone **Certificate Authority IP**.
16. Entrez le mot de passe à usage unique dans la zone **Pull Certificate Password**. Le mot de passe à usage unique est issu de la fenêtre Communication du panneau OPSEC Application Properties de SmartDashboard, dans laquelle vous avez sélectionné la case à cocher **CPMI** pour l'entité client.
17. Cliquez sur **OK**.
Si l'opération aboutit, la zone **OPSEC SSL Certificate** est remplie et grisée.
Vérifiez que la propriété **Trust State** de la fenêtre Communication du panneau OPSEC Application Properties est définie sur **Trust established**.
Les données d'identification sont configurées, vous pouvez maintenant lancer une reconnaissance.
18. Dans le menu de navigation, cliquez sur **Discover From Check Point SMS**.
19. Dans la zone **CPSMS IP Address**, entrez l'adresse IP du SMS.

Initialisation du comptage de règles pour Check Point

Terminez les configurations finales dans IBM Security QRadar et Check Point afin de lier les configurations et ainsi pouvoir utiliser le comptage de règles dans QRadar.

Pourquoi et quand exécuter cette tâche

Lorsque la confiance est établie et que les règles sont mises à jour, vous pouvez afficher le comptage de règles dans QRadar. Environ 1 heure est nécessaire à QRadar Risk Manager pour le traitement des comptages.

Procédure

1. Dans QRadar, cliquez sur **Risques > Moniteur de configuration**
2. Cliquez deux fois sur un périphérique Check Point afin d'afficher le comptage de règles.
 - Vérifiez dans la colonne **Sources de journal** que la source de journal est de type mappage automatique.
 - Recherchez la colonne **Nombre d'événements** dans le tableau de règles.

Cas d'utilisation du moniteur de politique d'administration

Plusieurs options sont disponibles lorsque vous créez des questions pour analyser les risques encourus par votre réseau.

Les exemples suivants du moniteur de politique d'administration présentent des cas d'utilisation courants que vous pouvez utiliser dans votre environnement réseau.

Hiérarchisation des vulnérabilités à haut risque par l'application de politiques de risque

Dans IBM Security QRadar Vulnerability Manager, vous pouvez alerter les administrateurs des vulnérabilités à haut risque en appliquant des politiques d'administration du risque à vos vulnérabilités.

Lorsque vous appliquez une politique d'administration du risque, le score du risque d'une vulnérabilité est ajusté, ce qui permet aux administrateurs de donner plus précisément la priorité aux vulnérabilités qui requièrent une attention immédiate.

Dans l'exemple ci-dessous, le score du risque de vulnérabilité est automatiquement accru par un facteur de pourcentage pour toute vulnérabilité qui reste active sur votre réseau après 40 jours.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Dans la barre d'outils, cliquez sur **Rechercher > Nouvelle recherche**.
4. Dans le panneau Paramètres de recherche, configurez les filtres suivants :
 - a. **Risque élevé**
 - b. **Jours depuis la découverte de vulnérabilités supérieur ou égal à 40**
5. Cliquez sur **Rechercher** puis sur **Sauvegarder les critères de recherche** dans la barre d'outils. Saisissez un nom de recherche sauvegardée identifiable dans QRadar Risk Manager.
6. Cliquez sur l'onglet **Risques**.
7. Dans le panneau de navigation, cliquez sur **Moniteur de politique d'administration**.
8. Dans la barre d'outils, cliquez sur **Actions > Nouveau**.
9. Dans la zone **What do you want to name this question**, saisissez un nom.
10. Dans la zone **Which tests do you want to include in your question**, cliquez sur **are susceptible to vulnerabilities contained in vulnerability saved searches**.
11. Dans la zone **Find Assets that**, cliquez sur le paramètre souligné dans **are susceptible to vulnerabilities contained in vulnerability saved searches**.
12. Identifiez votre recherche sauvegardée sur les vulnérabilités à haut risque QRadar Vulnerability Manager, cliquez sur **Ajouter**, puis sur **OK**.
13. Cliquez sur **Sauvegarder la question**.
14. Dans le panneau Questions, sélectionnez votre question dans la liste et cliquez sur **Moniteur** dans la barre d'outils.

Restriction : La zone **Description de l'événement** est obligatoire.
15. Cliquez sur **Envoyer les événements ayant passé la question**.
16. Dans la zone **Ajustements du score de vulnérabilité**, entrez une valeur en pourcentage correspondant à l'ajustement du risque (zone correspondant au **pourcentage d'ajustement du score de vulnérabilité sur l'échec d'une question**).
17. Cliquez sur l'option permettant d'**appliquer un ajustement à toutes les vulnérabilités sur un actif** puis sur **Sauvegarder le moniteur**.

Que faire ensuite

Dans l'onglet **Vulnérabilités**, vous pouvez rechercher les vulnérabilités à haut risque et les hiérarchiser.

Analyses de test de performances CIS

Pour configurer une analyse de test de performances CIS, vous devez effectuer un certain nombre de tâches de configuration au niveau des onglets Admin, Actifs, Vulnérabilités et Risques dans QRadar.

Pour pouvoir définir une analyse de test de performances CIS, les prérequis suivants sont nécessaires :

Licences IBM Security QRadar Vulnerability Manager et IBM Security QRadar Risk Manager valides

Si vous avez appliqué un correctif d'une version précédente de IBM Security QRadar, vous devez faire une mise à jour automatique avant d'effectuer une analyse de test de performances CI.

Une analyse de test de performances comporte 8 étapes :

1. Ajout d'actifs.
2. Configuration d'un jeu de données d'identification.
Il est plus simple d'ajouter des données d'identification centralisées sous l'onglet Admin de IBM Security QRadar mais vous pouvez aussi ajouter les données d'identification lors de la création d'un profil de test de performances.
3. Création d'une recherche sauvegardée d'actif.
Vous utilisez les recherches sauvegardées d'actif lors de la configuration des questions de conformité d'actif.
4. Modification des vérifications de test de performances CIS dans QRadar Vulnerability Manager.
Vous pouvez créer une liste de contrôle de test de performances CIS à l'aide de l'éditeur de test de performances de conformité.
5. Configuration d'un profil d'analyse de test de performances CIS dans QRadar Vulnerability Manager.
6. Création d'une question de conformité d'actif dans IBM Security QRadar Risk Manager.
7. Surveillance de la question de conformité d'actif que vous avez créée.
8. Affichage des résultats d'analyse de test de performances CIS.

Ajout ou édition d'un profil d'actif

Avant d'ajouter une analyse de test de performances CIS, vous devez ajouter les actifs réseau que vous avez l'intention d'analyser dans IBM Security QRadar. Les profils d'actif sont automatiquement détectés et ajoutés ; toutefois, vous devrez peut-être ajouter manuellement un profil.

Pourquoi et quand exécuter cette tâche

Vous pouvez entrer manuellement les informations sur chaque actif en créant un profil d'actif sous l'onglet **Actifs**. Vous pouvez aussi configurer un profil d'actif sous l'onglet **Vulnérabilités** afin d'exécuter une analyse de détection. Cette analyse de détection permet à QRadar® d'identifier les principales caractéristiques d'actif comme le système d'exploitation, le type de périphérique et les services.

Lorsque des actifs sont détectés à l'aide de l'option Reconnaissance des serveurs, certains détails de profil d'actif sont remplis automatiquement. Vous pouvez ajouter manuellement des informations au profil d'actif et éditer certains paramètres.

Vous pouvez uniquement éditer les paramètres qui ont été saisis manuellement. Les paramètres gérés par le système s'affichent en italiques et ne sont pas éditables. Vous pouvez supprimer, en cas de besoin, des paramètres générés par le système.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez une des options suivantes :
Pour ajouter un actif, cliquez sur **Ajouter un actif** et saisissez l'adresse IP ou la plage CIDR de l'actif dans la zone **Nouvelle adresse IP**.
Pour éditer un actif, cliquez deux fois sur l'actif que vous voulez afficher et cliquez sur **Modifier un actif**.
4. Configurez les paramètres dans le volet MAC & Adresse IP. Configurez une ou plusieurs options parmi les suivantes :
Cliquez sur l'icône **Nouvelle adresse MAC** et saisissez une adresse MAC dans la boîte de dialogue.

Cliquez sur l'icône **Nouvelle adresse IP** et saisissez une adresse IP dans la boîte de dialogue.

Si **Contrôleur NIC inconnu** figure dans la liste, vous pouvez le sélectionner, cliquez sur l'icône **Editer** et saisissez une nouvelle adresse MAC dans la boîte de dialogue.

Sélectionnez une adresse MAC ou IP dans la liste, cliquez sur l'icône **Editer**, puis saisissez une nouvelle adresse MAC dans la boîte de dialogue.

Sélectionnez une adresse MAC ou IP dans la liste et cliquez sur l'icône **Retirer**.

5. Configurez les paramètres dans le panneau Noms & Description. Effectuez une ou plusieurs des opérations suivantes :

Paramètre	Description
DNS	Sélectionnez une des options suivantes : Saisissez un nom DNS et cliquez sur Ajouter . Sélectionnez un nom DNS dans la liste et cliquez sur Editer . Sélectionnez un nom DNS dans la liste et cliquez sur Retirer .
NetBIOS	Sélectionnez une des options suivantes : Saisissez un nom NetBIOS et cliquez sur Ajouter . Sélectionnez un nom NetBIOS dans la liste et cliquez sur Editer . Sélectionnez un nom NetBIOS dans la liste et cliquez sur Retirer .
Nom attribué	Saisissez le nom de ce profil d'actif.
Emplacement	Saisissez l'emplacement de ce profil d'actif.
Description	Saisissez la description de ce profil d'actif.
AP sans fil	Saisissez le point d'accès sans fil de ce profil d'accès.
SSID sans fil	Saisissez l'identificateur de sous-système de stockage (SSID) de ce profil d'actif.
ID commutateur	Saisissez l'ID de commutateur de ce profil d'actif.
ID port commutateur	Saisissez l'ID de port de commutateur de ce profil d'actif.

6. Configurez les paramètres dans le volet Système d'exploitation :

- a. Dans la zone de liste **Fournisseur**, sélectionnez un fournisseur de système d'exploitation.
- b. Dans la zone de liste **Produit**, sélectionnez le système d'exploitation pour le profil d'actif.
- c. Dans la zone de liste **Version**, sélectionnez la version du système d'exploitation sélectionné.
- d. Cliquez sur l'icône **Ajouter**.
- e. Dans la zone de liste **Remplacer**, sélectionnez l'une des options suivantes :
 - **Remplacer jusqu'à la prochaine analyse** - Sélectionnez cette option pour indiquer que le scanner fournit des informations sur le système d'exploitation et que les informations peuvent être temporairement éditées. Si vous éditez les paramètres du système d'exploitation, le scanner restaure les informations au moment de sa prochaine analyse.
 - **Remplacer définitivement** - Sélectionnez cette option pour indiquer que vous souhaitez entrer manuellement des informations sur le système d'exploitation et désactiver la mise à jour des informations par le scanner.
- f. Sélectionnez un système d'exploitation dans la liste.
- g. Sélectionnez un système d'exploitation et cliquez sur l'icône **Redéfinir le basculement**.

7. Configurez les paramètres dans le panneau CVSS & Poids. Configurez une ou plusieurs options parmi les suivantes :

Paramètre	Description
Dommages collatéraux potentiels	<p>Configurez ce paramètre pour indiquer le risque de danger de mort ou de perte d'actifs physiques par endommagement ou vol . Vous pouvez également utiliser ce paramètre pour indiquer le risque de perte économique en termes de productivité ou de recettes. Le risque de dommages collatéraux accru augmente la valeur calculée du paramètre CVSS Score .</p> <p>Dans la zone de liste Dommages collatéraux potentiels, sélectionnez l'une des options suivantes :</p> <p>Aucun</p> <p>Faible</p> <p>Faible-Moyen</p> <p>Moyen-Elevé</p> <p>Elevé</p> <p>Non défini</p> <p>Lorsque vous configurez le paramètre Dommages collatéraux potentiels, le paramètre Poids est automatiquement mis à jour.</p>
Exigences de confidentialité	<p>Configurez ce paramètre pour indiquer l'impact sur la confidentialité d'une vulnérabilité correctement exploitée de cet actif. L'impact de confidentialité accru augmente la valeur calculée du paramètre Score CVSS.</p> <p>Dans la zone de liste Exigences de confidentialité, sélectionnez l'une des options suivantes :</p> <p>Faible</p> <p>Moyen</p> <p>Elevé</p> <p>Non défini</p>

Paramètre	Description
Exigences de disponibilité	<p>Configurez ce paramètre pour indiquer l'impact sur la disponibilité de l'actif lorsqu'une vulnérabilité est correctement exploitée. Les attaques qui consomment de la bande passante réseau, des cycles de processeur ou de l'espace disque ont un impact sur la disponibilité d'un actif. L'impact de disponibilité accru augmente la valeur calculée du paramètre Score CVSS.</p> <p>Dans la zone de liste Exigences de disponibilité, sélectionnez l'une des options suivantes :</p> <p>Faible</p> <p>Moyen</p> <p>Elevé</p> <p>Non défini</p>
Exigences d'intégrité	<p>Configurez ce paramètre pour indiquer l'impact sur l'intégrité de l'actif lorsqu'une vulnérabilité est correctement exploitée. L'intégrité fait référence à la fiabilité et la véracité des informations. L'impact d'intégrité accru augmente la valeur calculée du paramètre Score CVSS.</p> <p>Dans la zone de liste Exigences d'intégrité, sélectionnez l'une des options suivantes :</p> <p>Faible</p> <p>Moyen</p> <p>Elevé</p> <p>Non défini</p>
Poids	<p>Dans la zone de liste Poids, sélectionnez un poids pour le profil d'actif. La plage est comprise entre 0 et 10.</p> <p>Lorsque vous configurez le paramètre Poids, le paramètre Dommages collatéraux potentiels est automatiquement mis à jour.</p>

8. Configurez les paramètres dans le volet Propriétaires. Sélectionnez une ou plusieurs options parmi les suivantes :

Paramètre	Description
Propriétaire fonctionnel	Entrez le nom du propriétaire fonctionnel de l'actif. Un directeur de service est un exemple de propriétaire fonctionnel. La longueur maximale est 255 caractères.
Contact propriétaire fonctionnel	Entrez les informations de contact du propriétaire fonctionnel. La longueur maximale est 255 caractères.
Propriétaire technique	Entrez le propriétaire technique de l'actif. Un responsable informatique ou un directeur sont des exemples de propriétaire fonctionnel. La longueur maximale est 255 caractères.
Contact propriétaire technique	Entrez les informations de contact du propriétaire technique. La longueur maximale est 255 caractères.


Paramètre	Description
Utilisateur technique	<p>Dans la zone de liste, sélectionnez le nom d'utilisateur que vous souhaitez associer à ce profil d'actif.</p> <p>Vous pouvez également utiliser ce paramètre pour activer le recours à la vulnérabilité automatique d'IBM Security QRadar Vulnerability Manager. Pour plus d'informations sur le recours automatique, voir <i>IBM Security QRadar Vulnerability Manager User Guide</i>.</p>

9. Cliquez sur **Sauvegarder**.

Configuration d'un jeu de données d'identification

Dans IBM Security QRadar Vulnerability Manager, vous pouvez créer un jeu de données d'identification pour les actifs de votre réseau. Lors d'une analyse, si un outil requiert les données d'identification pour un système d'exploitation Linux, UNIX, ou Windows, celles-ci sont automatiquement transmises à l'outil d'analyse depuis le jeu de données d'identification.

Procédure

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans le panneau **Configuration système**, cliquez sur **Données d'identification centralisées**.
3. Depuis la fenêtre Données d'identification centralisées, cliquez sur **Ajouter** dans la barre d'outils.
Pour configurer un jeu de données d'identification, la seule zone obligatoire de la fenêtre Jeu de données d'identification est la zone **Nom**.
4. Dans la fenêtre Jeu de données d'identification, cliquez sur l'onglet **Actifs**.
5. Entrez une plage CIDR pour les actifs dont vous désirez spécifier les données d'identification et cliquez sur **Ajouter**.
Les utilisateurs doivent détenir des droits d'accès au réseau fournis dans le profil de sécurité d'une adresse IP ou d'une plage d'adresses CIDR, qu'ils utilisent ou créent des données d'identification via les **Données d'identification centralisées**.
6. Facultatif : Cliquez sur les onglets **Linux/Unix**, **Windows**, ou **Périphériques réseau (SNMP)**, puis entrez vos données d'identification.
7. Cliquez sur **Sauvegarder**.

Sauvegarde des critères de recherche d'un actif

Dans l'onglet **Actif**, vous pouvez sauvegarder les critères de recherche configurés afin de pouvoir les réutiliser. Les critères de recherche sauvegardée n'expirent pas.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Effectuez une recherche.
4. Cliquez sur **Sauvegarder les critères**.
5. Saisissez les valeurs pour ces paramètres :

Paramètre	Description
Entrez le nom de cette recherche	Saisissez le nom unique que vous souhaitez affecter à ce critère de recherche.

Paramètre	Description
Gérer les groupes	Cliquez sur Gérer les groupes pour gérer des groupes de recherche. Cette option s'affiche uniquement si vous disposez d'autorisations administrateur.
Affecter la recherche au(x) groupe(s)	Cochez la case du groupe auquel vous souhaitez affecter cette recherche sauvegardée. Si vous ne sélectionnez pas de groupe, cette recherche sauvegardée est affectée au groupe Autre par défaut.
Inclure dans mes recherches rapides	Cochez cette case pour inclure cette recherche à votre zone de liste Recherche rapide , dans la barre d'outils de l'onglet Actifs .
Définir par défaut	Cochez cette case pour définir cette recherche comme recherche par défaut lorsque vous accédez à l'onglet Actifs .
Partager avec tout le monde	Cochez cette case pour partager ces exigences de recherche avec tous les autres utilisateurs.

Edition d'un test de performances de conformité

Utilisez l'éditeur de test de performances de conformité dans IBM Security QRadar Risk Manager pour ajouter ou retirer des tests du test de performances CIS par défaut.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Cliquez sur **Moniteur de politique d'administration**.
3. Cliquez sur **Conformité** afin d'ouvrir la fenêtre de l'éditeur de test de performances de conformité.
4. Dans le menu de navigation, cliquez sur le test de performances CIS par défaut que vous voulez éditer.
5. Dans le panneau **Conformité**, sélectionnez la case à cocher **Activé** sur la ligne affectée au test que vous voulez inclure.

Cliquez n'importe où sur une ligne afin d'afficher une description du test de performances, une justification de déploiement et des informations sur les éléments à vérifier avant d'activer le test.

Lorsque vous avez généré une liste de contrôle CIS personnalisée, sachez que certains tests de performances non inclus par défaut peuvent prendre plus de temps. Pour plus d'informations, consultez la documentation CIS.

Que faire ensuite

Créez une question de conformité d'actif pour tester les actifs par rapport au test de performances que vous avez édité.

Création d'un profil de test de performances

Pour créer des analyses de conformité CIS (Center for Internet Security), vous devez configurer des profils de test de performances. Les analyses de conformité CIS vous permettent de tester la conformité de test de performance CIS Windows et Red Hat Enterprise Linux.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Administration > Profil d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter test de performances**.

4. Si vous voulez utiliser des données d'identification prédéfinies, sélectionnez la case à cocher **Utiliser les données d'identification centralisées**.

Les données d'identification qui sont utilisées pour l'analyse des systèmes Linux doivent disposer de droits root. Les données d'identification qui sont utilisées pour l'analyse des systèmes Windows doivent disposer de droits d'administrateur.

5. Si vous n'utilisez pas l'analyse dynamique, sélectionnez le scanner QRadar Vulnerability Manager dans la liste **Serveur d'analyse**.

6. Pour activer l'analyse dynamique, cliquez sur la case à cocher **Sélection de serveur dynamique**.

Si vous avez configuré des domaines dans la fenêtre **Admin > Gestion des domaines**, vous pouvez sélectionner un domaine dans la liste **Domaines**. Seuls les actifs dans les plages de CIDR et les domaines qui sont configurés pour vos scanners sont analysés.

7. Sous l'onglet de **planification d'analyse**, définissez le planning d'exécution, l'heure de début d'analyse et les éventuelles périodes d'exécution définies.

8. Sous l'onglet **E-mail**, définissez les informations à envoyer à propos de cette analyse et à qui les envoyer.

9. Si vous n'utilisez pas des données d'identification centralisées, ajoutez les données d'identification nécessaires à l'analyse sous l'onglet **Données d'identification supplémentaires**.

Les données d'identification qui sont utilisées pour l'analyse des systèmes Linux doivent disposer de droits root. Les données d'identification qui sont utilisées pour l'analyse des systèmes Windows doivent disposer de droits d'administrateur.

10. Cliquez sur **Sauvegarder**.

Création d'une question de conformité d'actif

Créez une question de conformité d'actif dans le moniteur de politique d'administration pour rechercher sur le réseau des actifs qui échouent aux tests de performances CIS.

Avant de commencer

Les questions du moniteur de politique d'administration sont évaluées de manière cohérente. L'ordre des questions du moniteur de politique d'administration a un impact sur les résultats.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans le menu **Actions**, sélectionnez **New Asset Compliance Question**.
4. Dans la zone **What do you want to name this question**, entrez un nom pour la question.
5. Sélectionnez le niveau d'importance à associer à cette question dans la liste **Coefficient d'importance**.
6. Dans la zone **Which tests do you want to include in your question**, sélectionnez l'icône d'ajout (+) en regard du test **test compliance of assets in asset saved searches with CIS benchmarks** .
Sélectionnez ce test plusieurs fois, si nécessaire.
7. Configurez les paramètres pour les tests dans la zone **Find Assets that**.
Cliquez sur chaque paramètre pour afficher les options actives de votre question. Spécifiez plusieurs recherches enregistrées d'actifs et plusieurs listes de contrôle, si nécessaire.
8. Dans la zone de groupe, cliquez sur les cases à cocher appropriées pour attribuer l'appartenance de groupe à cette question.
Les questions de conformité d'actif doivent être affectées à un groupe en vue de leur inclusion dans des tableaux de bord de conformité ou des rapports.
9. Cliquez sur **Sauvegarder la question**.

Que faire ensuite

Associez un profil de test de performance à la question créée et surveillez ses résultats.

Surveillances des questions de conformité d'actif

Surveillez les questions de conformité d'actif en sélectionnant des profils d'analyse CIS. Les analyses de test de performances CIS sont exécutées sur les actifs.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Dans le panneau **Questions**, sélectionnez la question de conformité d'actif à surveiller.
4. Cliquez sur **Surveiller** afin d'ouvrir la fenêtre Surveiller les résultats.
5. Sélectionnez un profil de test de performances dans la liste **Which benchmark profile to associate with this question?**.

Le profil d'analyse de test de performances sélectionné utilise un scanner QRadar Vulnerability Manager qui est associé à un domaine. Le nom de domaine est affiché dans la zone **Benchmark Profile Details**. Pour plus d'informations sur la gestion de domaine, consultez le manuel *IBM Security QRadar Administration Guide*.

6. Sélectionnez la case à cocher **Enable the monitor results function for this question/simulation**.
7. Cliquez sur **Sauvegarder le moniteur**.

La surveillance démarre à l'heure de début de l'analyse que vous avez définie sous l'onglet de **planification d'analyse** lors de la création du profil d'analyse de test de performances.

Affichage des résultats d'analyse

La page Résultats d'analyse affiche une liste récapitulative des résultats générés par l'exécution d'un profil d'analyse.

Pourquoi et quand exécuter cette tâche

La page Résultats d'analyse fournit les informations suivantes :

Tableau 25. Paramètres de la liste de résultats d'analyse

Paramètre	Description
Profil	Nom du profil d'analyse. Survolez à l'aide de la souris le Profil afin d'afficher les informations sur le profil d'analyse et l'état de l'analyse.
Planning	Planning d'exécution appliqué au profil d'analyse. Si vous avez démarré un analyse manuelle, Manuel est affiché.
Score	Score CVSS (Common Vulnerability Scoring Syst) moyen pour l'analyse. Cette note vous aide à classer les vulnérabilités.
Hôtes	Nombre d'hôtes identifiés et analysés lors de l'exécution du profil d'analyse. Cliquez sur le lien de colonne Hôte pour afficher les données de vulnérabilité des hôtes analysés.
Vulnérabilités	Nombre de différents types de vulnérabilités trouvés via un processus d'analyse. Cliquez sur le lien de colonne Vulnérabilités pour afficher toutes les vulnérabilités uniques.
Instances de vulnérabilité	Nombre de vulnérabilités trouvées via le processus d'analyse.

Tableau 25. Paramètres de la liste de résultats d'analyse (suite)

Paramètre	Description
Services ouverts	<p>Nombre de services ouverts uniques trouvés via le processus d'analyse. Un service ouvert unique est considéré comme un seul service ouvert.</p> <p>Cliquez sur le lien de colonne Services ouverts pour afficher les vulnérabilités catégorisées par service ouvert.</p>
Etat	<p>Les options de l'état du profil d'analyse comprennent :</p> <p>Arrêtée - Cet état s'affiche si l'analyse s'est terminée correctement ou si elle a été annulée.</p> <p>En cours d'exécution - L'analyse est en cours d'exécution</p> <p>En pause - L'analyse est momentanément interrompue.</p> <p>Non démarrée - L'analyse n'est pas encore lancée.</p>
Progress	<p>Indique l'état d'avancement de l'analyse.</p> <p>Survolez à l'aide la souris la barre de progression, pendant que l'analyse est en cours, afin d'afficher des informations sur l'état d'une analyse.</p>
Date/Heure de début	Indique la date et l'heure auxquelles a commencé l'exécution du profil d'analyse.
Durée	Affiche le temps pris pour l'exécution complète de l'analyse.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Résultats de l'analyse**.

12 Gestion des règles

Vous utilisez les pages de gestion des règles IBM Security QRadar Risk Manager pour afficher les détails sur les modifications de conformité aux règles et de risques liés aux règles pour les actifs, les règles et les vérifications de règles.

Les pages de gestion de règles QRadar Risk Manager affichent les données de la dernière règle exécutée. Vous pouvez filtrer les données par actif, par règle ou par vérification de règle.

Cas d'utilisation de la gestion des règles

Utilisez les pages Gestion des règles avec des articles du tableau de bord **Risque** pour trouver plus d'informations sur les actifs et les règles qui ont échoué au test de conformité.

- La page **Par actif** comprend des informations et des liens vers les règles auxquelles les actifs ont échoué.
- La page **Par règle** comprend des informations sur le nombre et le pourcentage d'actifs qui ont réussi ou échoué et, le cas échéant, un lien vers les vérifications de règles que la politique utilise.
- La page **Par vérification de règle** contient des informations sur le nombre et le pourcentage des actifs qui réussissent ou qui échouent à des vérifications de règles particulières.

Utilisez les pages de gestion de règles avec les articles du tableau de bord **Modification du risque** pour enquêter sur les règles et les vérifications de règles qui affichent des augmentations du risque. L'article de tableau de bord **Modification du risque** contient des liens vers les pages **Par règle** et **Par vérification de règle**. Pour en savoir plus sur la configuration des tableaux de bord pour la surveillance de la politique et des modifications du risque, voir le manuel *IBM Security QRadar SIEM*.

13 Simulations réseau dans IBM Security QRadar Risk Manager

Utilisation des simulations pour définir, planifier et réaliser des simulations d'utilisation sur votre réseau. Vous pouvez créer, afficher, dupliquer et supprimer des simulations.

Vous pouvez créer des simulations basées sur une série de règles qui peuvent être combinées et configurées. La simulation peut être planifiée pour être exécutée de manière périodique ou manuellement. Une fois une simulation terminée, vous pouvez vérifier les résultats de la simulation et valider tout résultat acceptable ou à faible risque en fonction de votre politique de réseau. Lorsque vous vérifiez les résultats, cela vous permet de valider les actions ou le trafic acceptable(s) provenant de vos résultats. Après avoir ajusté votre simulation, vous pouvez la configurer pour contrôler les résultats.

Le fait de surveiller une simulation vous permet de définir la façon dont vous souhaitez que le système réponde lorsque des résultats non validés sont renvoyés. Cette réponse peut être un e-mail, la création d'un événement ou l'envoi de la réponse à syslog.

Les simulations peuvent être modélisées hors d'une topologie actuelle ou d'un modèle de topologie.

La page Simulation récapitule les informations sur les simulations et les résultats des simulations.

Les résultats d'une simulations s'affichent uniquement lorsqu'elle est terminée. Une fois la simulation terminée, la colonne **Résultats** répertorie les dates de votre simulation et les résultats correspondants.

Simulations

Affichez les simulations créées par les utilisateurs et les résultats correspondants sur la page des simulations.

La fenêtre Simulations fournit les informations suivantes :

Tableau 26. Paramètres des définitions de simulation

Paramètre	Description
Nom de simulation	Nom de la simulation tel que défini par le créateur de la simulation.
Modèle	Type de modèle. Les simulations peuvent être modélisées à partir de la topologie en cours ou d'un autre modèle de topologie. Les options sont : <ul style="list-style-type: none">• Topologie en cours• Nom du modèle de topologie
Groupes	Groupes associés à la simulation.
Créé par	Utilisateur créateur de la simulation.
Date de création	Date et heure de création de la simulation.
Dernière modification	Date et heure de la dernière modification de la simulation.

Tableau 26. Paramètres des définitions de simulation (suite)

Paramètre	Description
Planification	<p>Fréquence d'exécution planifiée de la simulation. Les options sont les suivantes :</p> <p>Manuelle - La simulation s'exécute de façon manuelle.</p> <p>Une fois - Indiquez la date et l'heure d'exécution planifiée de la simulation.</p> <p>Quotidienne - Indiquez l'heure du jour d'exécution planifiée de la simulation.</p> <p>Hebdomadaire - Indiquez le jour de la semaine et l'heure d'exécution planifiée de la simulation.</p> <p>Mensuelle - Indiquez le jour du mois et l'heure d'exécution planifiée de la simulation.</p>
Dernière exécution	Date et heure de la dernière exécution de la simulation.
Prochaine exécution	Date et heure de la prochaine exécution de la simulation.
Résultats	Si la simulation est exécutée, ce paramètre comprend une liste qui contient les dates des résultats de vos simulations. Vous pouvez sélectionner une date et visualiser les résultats.

Création d'une simulation

Vous pouvez créer des simulations basées sur une série de règles qui peuvent être combinées et configurées.

Pourquoi et quand exécuter cette tâche

Les paramètres qui peuvent être configurés pour les tests de simulation sont soulignés. Le tableau suivant décrit les tests de simulation que vous pouvez configurer.

Tableau 27. Tests de simulation

Intitulé du test	Description	Paramètres
Attack targets one of the following IP addresses	Vous permet de simuler les attaques contre des adresses IP ou des plages CIDR spécifiques.	Configurez le paramètre IP addresses pour spécifier l'adresse IP ou les plages CIDR auxquelles vous voulez appliquer cette simulation.
Attack targets one of the following networks	Vous permet de simuler les attaques visant des réseaux membres d'un ou de plusieurs emplacements réseau définis.	Configurez le paramètre networks pour définir les réseaux auxquels vous souhaitez que cette simulation s'applique.
Attack targets one of the following asset building blocks	Vous permet de simuler les attaques visant un ou plusieurs éléments structurants d'actifs définis.	Configurez le paramètre asset building blocks pour définir les blocs de construction d'actifs auxquels vous souhaitez que cette simulation s'applique.
Attack targets one of the following reference sets	Vous permet de simuler les attaques visant un ou plusieurs jeux de référence définis.	Configurez les paramètres d'ensemble de référence afin de les spécifier à l'emplacement auquel vous souhaitez que cette simulation s'applique.

Tableau 27. Tests de simulation (suite)

Intitulé du test	Description	Paramètres
Attack targets a vulnerability on one of the following ports using protocols	Vous permet de simuler les attaques visant une vulnérabilité sur un ou plusieurs ports définis.	Configurez les paramètres suivants : Open Ports - Indiquez les ports auxquels vous souhaitez que cette simulation s'applique. Protocols - Indiquez le protocole auquel vous souhaitez que cette simulation s'applique.
Attack targets assets susceptible to one of the following vulnerabilities	Vous permet de simuler les attaques visant des actifs sensibles à une ou plusieurs vulnérabilités définies.	Configurez le paramètre vulnerabilities pour identifier les vulnérabilités auxquelles vous souhaitez que ce test s'applique. Vous pouvez rechercher des vulnérabilités à l'aide des options OSVDB ID, Bugtraq ID, CVE ID ou du titre.
Attack targets assets susceptible to vulnerabilities with one of the following classifications	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités pour une ou plusieurs classifications définies.	Configurez le paramètre classifications pour identifier les classifications de vulnérabilité. Par exemple, une classification de vulnérabilité peut être Input Manipulation ou Denial of Service.
Attack targets assets susceptible to vulnerabilities with CVSS score greater than 5	Une valeur CVSS (Common Vulnerability Scoring System) est une norme de l'industrie permettant d'évaluer la gravité des vulnérabilités. Cette simulation filtre les actifs de votre réseau qui comprennent la valeur CVSS configurée. Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités d'un niveau CVSS supérieur à 5.	Cliquez sur la valeur supérieure à 5 , puis sélectionnez un opérateur. L'opérateur par défaut est la valeur supérieure à 5
Attack targets assets susceptible to vulnerabilities disclosed after this date	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités reconnues avant, après ou à la date configurée.	Configurez les paramètres suivants : before after on- Indiquez si vous souhaitez que la simulation prenne en considération les vulnérabilités divulguées pour être postérieures, antérieures ou égales à la date configurée sur les actifs. La valeur par défaut est before. this date - Indiquez la date que vous souhaitez que cette simulation prenne en considération.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités comparant le nom d'actif, le fournisseur, la version ou le service à une ou plusieurs saisies.	Configurez les entrées de texte pour identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez intégrer à la simulation.

Tableau 27. Tests de simulation (suite)

Intitulé du test	Description	Paramètres
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Vous permet de simuler les attaques visant un actif sensible à des vulnérabilités comparant le nom d'actif, le fournisseur, la version ou le service à une ou plusieurs expressions régulières.	Configurez les expressions régulières pour identifier le nom d'actif, le fournisseur, la version ou le service que vous souhaitez intégrer à la simulation.

Les tests de contribution suivants sont dépréciés et cachés dans le moniteur de politique d'administration :

- **attack targets a vulnerability on one of the following operating systems**
- **attack targets assets susceptible to vulnerabilities from one of the following vendors**
- **attack targets assets susceptible to vulnerabilities from one of the following products**

Les tests de contribution obsolètes sont remplacés par d'autres tests.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Dans le menu **Actions**, sélectionnez **Nouveau**.
4. Entrez un nom pour la simulation dans le paramètre **Nom de la simulation**.
5. Dans la liste déroulante **Modèle de base**, sélectionnez le type de données que vous souhaitez renvoyer. Tous les modèles de topologie existant sont répertoriés. Si vous sélectionnez **Topologie en cours**, la simulation utilise le modèle de topologie actuel.
6. Sélectionnez une des options suivantes :

Option	Description
Sélectionnez Utiliser les données de connexion	La simulation sur la connexion et sur les données de topologie.
Désélectionnez Utiliser les données de connexion	La simulation est uniquement basée sur les données de topologie. Si votre modèle de topologie ne comprend aucune donnée et que vous désélectionnez la case Utiliser les données de connexion , la simulation ne renvoie aucun résultat.

7. Dans la liste **Coefficient d'importance**, sélectionnez le niveau d'importance que vous voulez associer à cette simulation.
L'option de coefficient d'importance permet de calculer le niveau de risque. La plage est comprise entre 1 (faible importance) et 10 (haute importance). La valeur par défaut est 5.
8. Dans la liste indiquant le **point de départ de la simulation**, sélectionnez une origine pour la simulation.
La valeur sélectionnée détermine le point de départ de la simulation. Par exemple, l'attaque provient d'un réseau spécifique. Les paramètres de simulation sélectionnés s'affichent dans la fenêtre relative à **l'emplacement de génération de la simulation**.
9. Ajoutez les cibles de l'attaque de simulation au test de simulation.
10. Dans la zone relative aux **simulations à inclure dans la zone d'attaque**, cliquez sur l'icône d'ajout (+) en regard de la simulation de votre choix.

Les options de simulation s'affichent dans la fenêtre relative à l'**emplacement de génération de la simulation**.

11. Dans cette fenêtre, cliquez sur les paramètres soulignés pour continuer à configurer les paramètres de simulation.
12. Dans le menu **Exécuter cette simulation pour**, sélectionnez le nombre d'étapes auxquelles exécuter cette simulation (1 - 5).
13. Dans le menu des étapes, choisissez la planification pour l'exécution de la simulation.
14. Dans la zone de groupes, sélectionnez une case à cocher en regard d'un groupe auquel affecter cette simulation.
15. Cliquez sur **Sauvegarder la simulation**.

Edition d'une simulation

Vous pouvez modifier des simulations.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Sélectionnez la définition de simulation à éditer.
4. Dans le menu **Actions**, sélectionnez **Editer**.
5. Mettez à jour les paramètres, au besoin.
Pour plus d'informations sur les paramètres Simulation, voir tests Simulation.
6. Cliquez sur **Sauvegarder la simulation**.

Duplication d'une simulation

Vous pouvez dupliquer des simulations.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Sélectionnez la simulation que vous souhaitez dupliquer.
4. Dans le menu **Actions**, sélectionnez **Dupliquer**.
5. Entrez le nom de la simulation.
6. Cliquez sur **OK**.

Suppression d'une simulation

Vous pouvez supprimer des simulations.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Sélectionnez la simulation que vous souhaitez supprimer.
4. Dans le menu **Actions**, sélectionnez **Supprimer**.
5. Cliquez sur **OK**.

Exécution manuelle d'une simulation

Utilisez Simulation Editor pour exécuter une simulation manuellement.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu **Actions**, sélectionnez **Exécuter la simulation**.
3. Cliquez sur **OK**.

Résultats

Le processus de simulation peut prendre un certain temps. Lors de l'exécution de la simulation, la colonne Prochaine exécution indique le pourcentage de tâche réalisée. Une fois le processus terminé, la colonne Résultats affiche la date et l'heure de la simulation.

Lorsque vous exécutez une simulation et que vous effectuez ensuite des changements affectant les tests associés à la simulation, ces modifications peuvent prendre plus d'une heure avant de s'afficher.

Simulation d'un changement de configuration réseau

Vous pouvez utiliser un modèle de topologie pour définir les 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 un changement de configuration réseau, procédez comme suit :

1. Créez un modèle de topologie.
2. Simulez une attaque contre le modèle de topologie.

Création d'un modèle de topologie

Créez un modèle de topologie permettant de simuler l'impact des modifications apportées au réseau, ainsi que les attaques.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulations > Modèles 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 à la sous-fenêtre **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

La fonction de simulation permet de simuler une attaque sur des ports ouverts en utilisant des protocoles tels que TCP.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Dans la 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 une origine pour 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** puis sélectionnez **TCP**. SSH utilise TCP.
10. Cliquez sur **Ajouter +** pour ajouter le protocole, puis sur **OK**.
11. Cliquez sur **Sauvegarder la simulation**.
12. Dans la liste **Actions**, sélectionnez **Exécuter la simulation**. La colonne des résultats comporte une liste avec la date d'exécution de la simulation, ainsi qu'un lien pour afficher les résultats.
13. Cliquez sur **Afficher les résultats**.

Simulation d'une attaque sur un protocole SSH

Simulez des attaques sur votre réseau, par exemple une attaque réseau sur un protocole SSH.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, cliquez sur **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 indiquant le **point de départ de la simulation**, sélectionnez une origine pour 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 **Ajouter +** pour ajouter le protocole, puis 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

La liste des actifs présentant des vulnérabilités SSH s'affiche dans les résultats, ce qui permet aux administrateurs réseau d'approuver les connexions SSH autorisées ou attendues dans votre réseau. Les communications qui ne sont pas approuvées peuvent être surveillées pour les événements ou les infractions.

Les résultats fournissent aux administrateurs réseau ou aux professionnels de la sécurité une représentation visuelle du chemin d'attaque. Par exemple, la première étape fournit la liste des actifs directement connectés qui sont affectés par la simulation. La seconde étape répertorie les actifs de votre réseau qui peuvent communiquer avec les actifs de premier niveau dans votre simulation.

Les informations fournies dans l'attaque vous aide à renforcer et tester votre réseau contre des centaines de scénarios d'attaque possibles.

Gestion des résultats de simulations

Une fois qu'une simulation est exécutée, la colonne Résultats affiche une zone de liste déroulante contenant une liste des dates pendant la génération de la simulation.

Les résultats de simulation sont conservés pour 30 jours. Les résultats s'affichent uniquement dans la colonne Résultats après l'exécution d'une simulation.

Affichage des résultats de simulations

Vous pouvez afficher les résultats de simulation dans la colonne Résultats de la page Simulations.

Pourquoi et quand exécuter cette tâche

Les résultats s'affichent uniquement dans la colonne Résultats après l'exécution d'une simulation. Les résultats de la simulation fournissent des informations sur chaque étape de la simulation.

Par exemple, la première étape d'une simulation fournit une liste des actifs directement connectés qui sont affectés par la simulation. La seconde étape répertorie les actifs de votre réseau qui peuvent communiquer avec les actifs de premier niveau dans votre simulation.

Lorsque vous cliquez sur Afficher les résultats, les informations suivantes sont fournies :

Tableau 28. Informations sur le résultat de simulation

Paramètre	Description
Simulation Definition	Description de la simulation.
Using Model	Nom du modèle sur lequel la simulation a été exécutée.
Simulation Result	Date d'exécution de la simulation.
Step Results	Nombre d'étapes du résultat incluant l'étape actuellement affichée.

Tableau 28. Informations sur le résultat de simulation (suite)

Paramètre	Description
Assets Compromised	<p>Nombre total d'actifs impliqués dans cette étape et dans les étapes de simulation.</p> <p>Si le modèle de topologie contient des données d'une plage d'adresses IP de /32 définies comme pouvant être attendues, IBM Security QRadar Risk Manager ne valide pas ces actifs en fonction de la base de données. C'est la raison pour laquelle ces actifs ne sont pas pris en considération dans le total Asset Compromised. QRadar Risk Manager valide uniquement les actifs des plages IP supérieures, telles que /24, pour déterminer quels actifs existent.</p>
Risk Score	Valeur calculée sur la base du nombre de résultats, d'étapes, du nombre d'actifs compromis et du coefficient d'importance affecté à la simulation. Cette valeur indique le niveau de gravité associé à la simulation pour l'étape affichée.

Vous pouvez déplacer le pointeur de la souris sur une connexion afin de déterminer la liste des actifs concernés par cette simulation.

Les 10 premiers actifs s'affichent lorsque vous placez le pointeur de votre souris sur la connexion.

Placez le pointeur de votre souris sur la connexion pour sélectionner le chemin via le réseau tel qu'il est défini par le sous-réseau.

La page des résultats de simulation fournit un tableau appelé, Results for this step. Ce tableau fournit les informations suivantes :

Tableau 29. Résultats pour cette information sur l'étape

Paramètre	Description
Approuver	Vous permet de valider les résultats de la simulation. Voir Approbation des résultats de simulation.
Parent	Adresse IP d'origine de l'étape affichée de la simulation.
IP	Adresse IP de l'actif concerné.
Réseau	Réseau des adresses IP cible telles qu'elles sont définies dans la hiérarchie de réseau.
Nom de l'actif	Nom de l'actif concerné tel qu'il est défini dans le profil d'actif.
Poids de l'actif	Pondération de l'actif concerné telle qu'elle est définie dans le profil d'actif.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Dans la colonne Résultats, sélectionnez la date et l'heure de la simulation que vous souhaitez afficher à l'aide de la liste.
4. Cliquez sur **Afficher les résultats**. Vous pouvez afficher les informations de résultat de la simulation, démarrant à l'étape 1 de la simulation.

- Affichez le tableau des résultats de cette étape pour déterminer les actifs concernés.
- Pour afficher l'étape suivante des résultats de la simulation, cliquez sur **Etape suivante**.

Approbation des résultats de simulations

Dans les simulations, vous pouvez approuver le trafic réseau dont le risque semble faible ou une communication normale sur l'actif. Lorsque vous approuvez les résultats, vous filtrez la liste de sorte que les simulations futures ignorent ces communications.

Pourquoi et quand exécuter cette tâche

Vous pouvez valider les résultats de la simulation.

Les résultats s'affichent uniquement dans la colonne **Résultats** après l'exécution d'une simulation.

Procédure

- Cliquez sur l'onglet **Risques**.
- Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
- Dans la colonne **Résultats**, sélectionnez la date et l'heure de la simulation que vous souhaitez afficher à l'aide de la liste.
- Cliquez sur **Afficher les résultats**.
- Dans le tableau des **résultats de l'étape**, utilisez une des méthodes suivantes pour valider les actifs :

Option	Description
Valider les actifs sélectionnés	Cochez la case en regard de chaque actif à approuver, puis cliquez sur Valider les actifs sélectionnés .
Tout valider	Cliquez sur Tout valider pour approuver tous les actifs de la liste.

- Facultatif : Cliquez sur l'option permettant d'**afficher tous les actifs validés**.

Révocation de l'approbation de simulations

Vous pouvez révoquer une connexion approuvée ou une communication de la liste de simulations approuvée. Lorsque le résultat d'une simulation approuvée est révoqué, toutes les simulations à venir affichent les communications non approuvées dans les résultats de la simulation.

Procédure

- Cliquez sur l'onglet **Risques**.
- Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
- Dans la colonne **Résultats**, sélectionnez la date et l'heure de la simulation que vous souhaitez afficher à l'aide de la liste.
- Afficher les résultats**.
- Cliquez sur l'option permettant d'**afficher tous les actifs validés**.
- Sélectionnez une des options suivantes :

Option	Description
Révoquer la sélection	Cochez la case en regard de chaque actif à révoquer, puis cliquez sur Révoquer la sélection .
Révoquer tout	Cliquez sur Révoquer tout pour supprimer tous les actifs de la liste.

Surveillance des simulations

Vous pouvez contrôler une simulation pour déterminer si les résultats de la simulation ont été modifiés. Si une modification survient, un événement est généré. Vous pouvez configurer un maximum de 10 simulations en mode moniteur.

Pourquoi et quand exécuter cette tâche

Lorsqu'une simulation est en mode moniteur, l'intervalle par défaut est de 1 heure. Cette valeur écrase la valeur temporelle configurée lors de la création de la simulation.

Pour des informations sur les catégories d'événements, voir *IBM Security QRadar - Guide d'utilisation*.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Sélectionnez la simulation que vous souhaitez surveiller.
4. Cliquez sur **Moniteur**.
5. Dans la zone **Nom d'événement**, saisissez le nom de l'événement que vous souhaitez afficher sous les onglets **Activité du journal** et **Infractions**.
6. Dans la zone **Description de l'événement**, saisissez une description pour l'événement. La description est affichée dans le panneau Annotations des détails de l'événement.
7. Dans la liste **Catégorie de niveau supérieur**, sélectionnez la catégorie d'événement de haut niveau que vous souhaitez que cette simulation utilise pendant le traitement des événements.
8. Dans la liste **Catégorie de niveau inférieur**, sélectionnez la catégorie d'événements de bas niveau que vous voulez que cette simulation utilise pendant le traitement des événements.
9. Cochez la case **Vérifier que l'événement attribué fait partie d'une infraction** si vous voulez, en tant que résultat de cette simulation contrôlée, que les événements soient transmis au composant Magistrat. Si aucune infraction n'a été générée, une nouvelle infraction est créée. Si une infraction existe, cet événement est ajouté à l'infraction existante. Si vous cochez cette case, les options suivantes s'affichent :

Option	Description
Question/Simulation	Tous les événements d'une question sont associés à une infraction unique.
Actif	Une infraction unique est créée (ou mise à jour) pour chaque actif unique.

10. Dans la section **Actions supplémentaires**, sélectionnez une ou plusieurs des options suivantes :

Option	Description
E-mail	Cochez cette case puis spécifiez l'adresse électronique pour envoyer les notifications lorsque l'événement est généré. Utilisez une virgule pour séparer plusieurs adresses électroniques.
Envoyer à Syslog	Cochez cette case si vous souhaitez enregistrer l'événement. Par exemple, la sortie du syslog doit ressembler à : Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule'Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name:SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Eventdescription
Envoyer une notification	Cochez cette case si vous souhaitez que les événements générant comme résultat de cette question continue s'affichent dans l'élément System Notifications dans le Dashboard.

11. Dans la section **Activer le moniteur**, cochez la case pour contrôler la simulation.
12. Cliquez sur **Sauvegarder le moniteur**.

Regroupement de simulations

L'affectation de simulations à des groupes est une manière efficace d'afficher toutes les simulations et de procéder à leur suivi. Par exemple, vous pouvez afficher toutes les simulations liées à la conformité.

Pourquoi et quand exécuter cette tâche

Lorsque vous créez de nouvelles simulations, vous pouvez les assigner à un groupe existant.

Une fois un groupe créé, vous pouvez glisser-déplacer les groupes de l'arborescence des menus pour changer l'organisation.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Cliquez sur **Groupes**.
4. Dans l'arborescence du menu, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.
5. Cliquez sur **Nouveau**.
6. Dans la zone **Nom**, entrez un nom pour le nouveau groupe. Le nom du groupe peut contenir plus de 255 caractères.
7. Dans la zone **Description**, entrez une description pour le groupe. La description peut contenir plus de 255 caractères.
8. Cliquez sur **OK**.

14 Modèles de topologie

Vous pouvez utiliser un modèle de topologie pour définir les modèles de réseau virtuel basés sur votre réseau existant.

Vous pouvez créer un modèle de réseau en vous basant sur une série de modifications pouvant être combinées et configurées. Cela vous permet de déterminer l'effet des changements de configuration sur votre réseau à l'aide d'une simulation. Pour plus d'informations sur les simulations, voir [Utilisation des simulations](#).

Vous pouvez afficher les modèles de topologie sur la page Simulations. La page des modèles de topologie fournit les informations suivantes :

Tableau 30. Paramètres des définitions de modèle

Paramètre	Description
Nom de modèle	Nom du modèle de topologie tel qu'il a été défini par l'utilisateur lors de sa création.
Groupe(s)	Groupes auxquels cette topologie est associée.
Créé par	Utilisateur qui a créé la définition de modèle.
Créé le	Date et heure de création de la définition de modèle.
Dernière modification	Nombre de jours écoulés depuis la création de la définition de modèle.

Création d'un modèle de topologie

Vous pouvez créer un ou plusieurs modèles de topologie.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit l'intitulé du test et les paramètres que vous pouvez configurer.

Tableau 31. Tests de topologie

Intitulé du test	Paramètres
<p>A rule is added to the selected devices that allows connections from source CIDRs to destination CIDRs on protocols, ports</p>	<p>Configurez les paramètres suivants :</p> <p>Dispositifs : spécifiez les dispositifs à ajouter à cette règle. Dans la fenêtre Personnaliser un paramètre, cochez la case Tous pour inclure tous les dispositifs ou recherchez les dispositifs en utilisant l'un des critères de recherche suivants :</p> <p>IP/CIDR : sélectionnez l'option IP/CIDR et spécifiez l'adresse IP ou le CIDR auquel ajouter cette règle.</p> <p>Nom d'hôte : sélectionnez l'option Nom d'hôte et spécifiez le nom d'hôte sur lequel filtrer. Pour rechercher plusieurs noms d'hôte, utilisez un caractère générique (*) au début ou à la fin de la chaîne.</p> <p>Adapter : sélectionnez l'option Adaptateur et utilisez le menu pour filtrer la liste des dispositifs par adaptateur.</p> <p>Fournisseur : sélectionnez l'option Fournisseur et utilisez le menu pour filtrer la liste des dispositifs par fournisseur. Vous pouvez également définir un modèle pour le fournisseur. Pour rechercher plusieurs modèles, utilisez un caractère générique (*) au début ou à la fin de la chaîne.</p> <p>autorise refuse - Sélectionnez l'état (autorisé ou refusé) des connexions que vous souhaitez que ce test applique.</p> <p>CIDR : sélectionnez des adresses IP source ou des plages CIDR à ajouter à cette règle.</p> <p>CIDR : sélectionnez des adresses IP cible ou des plages CIDR à ajouter à cette règle.</p> <p>Protocoles : spécifiez les protocoles à ajouter à cette règle. Pour inclure tous les protocoles, cochez la case Tous.</p> <p>Ports : spécifiez les ports à ajouter à cette règle. Pour inclure tous les ports, cochez la case Tous.</p>

Tableau 31. Tests de topologie (suite)

Intitulé du test	Paramètres
<p>Une règle est ajoutée aux dispositifs IPS sélectionnés pour permettre les connexions des CIDR source vers les CIDR cible avec les vulnérabilités.</p>	<p>Configurez les paramètres suivants :</p> <p>IPS devices - Indiquez les périphériques IPS que vous souhaitez intégrer à ce modèle de topologie. Pour inclure tous les dispositifs IPS, cochez la case Tous.</p> <p>autorise refuse - Indiquez l'état (autorisé ou refusé) des connexions que vous souhaitez que ce test applique.</p> <p>Routages CIDR - Indiquez une adresse IP source ou une plage de routages CIDR à inclure dans ce modèle de topologie.</p> <p>Routages CIDR - Indiquez une adresse IP de destination ou une plage de routages CIDR à inclure dans ce modèle de topologie.</p> <p>vulnérabilités - Indiquez les vulnérabilités que vous souhaitez appliquer à ce modèle de topologie. Vous pouvez chercher les vulnérabilités en utilisant Bugtraq ID, OSVDB ID, CVE ID ou le titre.</p>
<p>Les actifs ci-dessous permettent les connexions aux ports sélectionnés.</p>	<p>Configurez les paramètres suivants :</p> <p>Actifs : spécifiez les actifs que vous souhaitez inclure dans ce modèle de topologie.</p> <p>accepte refuse - Spécifiez l'état (accepté ou refusé) des connexions que vous souhaitez que ce modèle de topologie applique. La valeur d'autorisation est sélectionnée par défaut.</p> <p>ports - Indiquez les ports que vous souhaitez intégrer à ce modèle de topologie. Pour inclure tous les ports, cochez la case Tous.</p>
<p>Les actifs dans les blocs fonctionnels permettent les connexions aux ports</p>	<p>Configurez les paramètres suivants :</p> <p>Actifs des blocs fonctionnels : spécifiez les blocs fonctionnels à inclure dans ce modèle de topologie.</p> <p>autorise refuse - Indiquez l'état (autorisé ou refusé) que vous souhaitez que ce modèle de topologie applique. La valeur d'autorisation est sélectionnée par défaut.</p> <p>ports - Indiquez les ports que vous souhaitez intégrer à ce modèle de topologie. Pour inclure tous les ports, cochez la case Tous.</p>

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, sélectionnez **Simulation > Modèles de topologie**
3. Dans le menu **Actions**, sélectionnez **Nouveau**.
4. Dans la zone **What do you want to name this model**, entrez un nom pour la définition du modèle.
5. Dans la sous-fenêtre **Which modifications do you want to apply to your model**, sélectionnez les modifications que vous souhaitez appliquer à la topologie pour créer votre modèle.

6. Configurez les tests ajoutés à la sous-fenêtre **Configurer le modèle comme suit**.
7. Une fois le test affiché dans la sous-fenêtre, les paramètres configurables sont soulignés. Cliquez sur chaque paramètre pour poursuivre la configuration de cette modification pour votre modèle. Dans la zone de groupes, cochez la case pour tout groupe à affecter à cette simulation.
8. Cliquez sur **Sauvegarder le modèle**.

Edition d'un modèle de topologie

Vous pouvez modifier un modèle de topologie.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Modèles de topologie**.
3. Sélectionnez la définition de modèle à éditer.
4. Dans le menu **Actions**, sélectionnez **Editer**.
5. Mettez à jour les paramètres, au besoin.
Pour plus d'informations sur les paramètres Editeur de modèle, voir **Création d'un modèle de topologie**.
6. Cliquez sur **Sauvegarder le modèle**.

Duplication d'un modèle de topologie

Vous pouvez dupliquer un modèle de topologie.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Modèles de topologie**.
3. Sélectionnez la définition de modèle à dupliquer.
4. Dans le menu **Actions**, sélectionnez **Dupliquer**.
5. Tapez un nom que vous souhaitez attribuer au modèle de topologie copié.
6. Cliquez sur **OK**.
7. Modifier le modèle.

Suppression d'un modèle de topologie

Vous pouvez modifier un modèle de topologie.

Procédure

1. Cliquez sur l'onglet **Risque**.
2. Sur le menu de navigation, sélectionnez **Simulation > Modèles de topologie**.
3. Sélectionnez la définition de modèle à supprimer.
4. Dans le menu **Actions**, sélectionnez **Supprimer**.
5. Cliquez sur **OK**.

Modèles de topologie de groupe

Vous pouvez regrouper et afficher vos modèles de topologie en fonction de vos critères choisis.

La catégorisation de votre modèle de topologie est une manière efficace d'afficher vos modèles et de procéder à leur suivi. Par exemple, vous pouvez afficher tous les modèles de topologie relatifs à la conformité.

Lorsque vous créez de nouveaux modèles de topologie, vous pouvez les affecter au groupe existant. Pour plus d'informations sur l'affectation d'un groupe, voir [Création d'un modèle de topologie](#).

Affichage des groupes

Vous pouvez afficher les modèles de topologie à l'aide des groupes.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Modèles de topologie**.
3. Dans la liste **Groupe**, sélectionnez le groupe que vous souhaitez afficher.

Création d'un groupe

Vous pouvez créer un groupe pour efficacement afficher et suivre les modèles de topologie.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Modèles de topologie**.
3. Cliquez sur **Groupes**.
4. Dans l'arborescence du menu, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.

Une fois le groupe créé, vous pouvez glisser-déplacer les groupes des éléments de l'arborescence des menus pour changer l'organisation.

5. Cliquez sur **Nouveau**.
6. Entrez le nom que vous souhaitez affecter au nouveau groupe. Le nom peut contenir jusqu'à 255 caractères.
7. Entrez une description pour le groupe. La description peut contenir plus de 255 caractères.
8. Cliquez sur **OK**.
9. Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers un emplacement dans votre arborescence de menus.

Edition d'un groupe

Vous pouvez éditer un groupe.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Modèles de topologie**.
3. Cliquez sur **Groupes**.
4. Dans l'arborescence de menu, sélectionnez le groupe que vous souhaitez éditer.
5. Cliquez sur **Editer**.
6. Mettez les valeurs des paramètres à jour
7. Cliquez sur **OK**.
8. Pour changer l'emplacement du groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers un emplacement dans votre arborescence de menus.

Copie d'un élément dans un autre groupe

En utilisant la fonctionnalité des groupes, vous pouvez copier un modèle de topologie vers un ou plusieurs groupes.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulations > Modèles de topologie**.
3. Cliquez sur **Groupes**.
4. Dans l'arborescence de menu, sélectionnez la question que vous souhaitez copier dans un autre groupe.
5. Cliquez sur **Copier**.
6. Cochez la case pour le groupe dans lequel vous souhaitez copier la simulation.
7. Cliquez sur **Copier**.

Affectation d'une topologie à un groupe

Vous pouvez affecter un modèle de topologie à un groupe.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Sélectionnez le modèle de topologie à affecter à un groupe.
4. Dans le menu **Actions**, sélectionnez **Affecter un groupe**.
5. Sélectionnez le groupe auquel vous souhaitez affecter la question.
6. Cliquez sur **Affecter des groupes**.

Suppression d'un élément d'un groupe

Vous pouvez supprimer un élément d'un groupe.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Sur le menu de navigation, sélectionnez **Simulation > Simulations**.
3. Cliquez sur **Groupes**.
4. Dans l'arborescence de menus, sélectionnez le groupe de niveau supérieur.
5. Dans la liste des groupes, sélectionnez l'élément ou le groupe que vous souhaitez supprimer.
6. Cliquez sur **Retirer**.
7. Cliquez sur **OK**.

15 Gestion des rapports IBM Security QRadar Risk Manager

Vous pouvez créer, modifier, répartir ou gérer les rapports pour vos périphériques réseau. Des rapports détaillés sur les règles de pare-feu et les connexions entre les périphériques sont souvent nécessaires pour satisfaire les diverses normes de réglementation, telles que la conformité PCI.

Les options de rapport suivantes sont spécifiques à QRadar Risk Manager:

Tableau 32. Les options de rapport pour QRadar Risk Manager

Option de rapport	Description
Connexions	Les diagrammes de connexion pour vos périphériques réseau établis au cours de votre intervalle de temps spécifié.
Règles du périphérique	Les règles configurées sur votre périphérique réseau pendant votre intervalle de temps spécifié. Vous pouvez afficher les types de règles suivants pour un ou plusieurs périphériques réseau à l'aide de cette option de rapport : Règles d'acceptation les plus utilisées Règles de refus les plus utilisées Règles d'acceptation les moins utilisées Règles de refus les moins utilisées Règles grisées Règles d'objet inutilisées
Objets non utilisés du périphérique	Fournit un tableau contenant le nom, la date/heure de configuration et une définition des groupes de références d'objet non utilisés sur le périphérique. Un groupe de références d'objet est un terme générique utilisé pour décrire une collection d'adresses IP, d'adresses CIDR, de noms d'hôtes, de ports ou d'autres paramètres de périphérique regroupés et affectés aux règles du périphérique.

Production manuelle d'un rapport

Les rapports peuvent démarrer manuellement. Si vous générez plusieurs rapports manuellement, ces derniers sont ajoutés à une file d'attente et portent le libellé de leur position dans la file d'attente.

Pourquoi et quand exécuter cette tâche

Le fait de générer manuellement un rapport ne réinitialise pas le planning de rapport existant. Par exemple, si vous générez un rapport hebdomadaire pour les refus de pare-feu les plus actifs, générez manuellement le rapport. Le rapport hebdomadaire continuera à être généré selon le planning initialement configuré.

lorsqu'un rapport génère, la colonne **Heure de la prochaine exécution** affiche l'un des trois messages suivants :

- **Génération** - Le rapport est en cours de production.

- **En file d'attente (position dans la file d'attente)** - Le rapport est mis en file d'attente pour la génération. Le message indique la position du rapport en file d'attente. Par exemple, 1 de 3.
- **(x heure(s) x minute(s) y secondes(s))** - Le rapport est planifié pour s'exécuter. Le message est un compte à rebours qui indique quand le rapport suivant sera exécuté.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez le rapport que vous souhaitez générer.
3. Cliquez sur **Exécuter le rapport**.
4. Facultatif. Cliquez sur **Actualiser** pour actualiser les informations dans la colonne **Heure de la prochaine exécution**.

Que faire ensuite

Après la production d'un rapport, vous pouvez afficher le rapport généré dans la colonne **Rapports générés**.

Utilisez l'assistant du rapport

Vous pouvez utiliser l'assistant Création de rapports pour créer un rapport. L'assistant Création de rapports fournit un guide étape par étape sur la conception, la planification et la production des rapports.

L'assistant utilise les éléments clés suivants pour vous aider à créer un rapport :

- **Présentation** - La position et la taille de chaque conteneur
- **Conteneur** - Marque de réservation et emplacement du contenu de votre rapport
- **Contenu** - Définit les données de rapport que IBM Security QRadar Risk Manager contient dans le graphique du conteneur

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

Le délai planifié des rapports générés toutes les semaines ou tous les mois doit s'écouler avant que ces derniers ne renvoient des résultats. Pour un rapport planifié, vous devez attendre l'heure planifiée pour la construction des résultats. Par exemple, une recherche hebdomadaire nécessite 7 jours pour construire les données. Cette recherche renvoie des résultats après un délai de 7 jours.

Création d'un rapport

Vous pouvez créer des rapports pour un intervalle spécifique puis sélectionner un type de graphique.

Pourquoi et quand exécuter cette tâche

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

Vous pouvez indiquer Console de rapports ou E-mail comme options de distribution de rapport. Le tableau suivant décrit les paramètres spécifiques pour ces options de distribution.

Tableau 33. Options de distribution de rapports générées

Option	Description
Console de rapports	Cochez cette case pour envoyer le rapport généré à l'onglet Rapports . Il s'agit du canal de distribution par défaut.
Sélectionner les utilisateurs pouvant consulter la sortie générée par ce rapport.	<p>Cette option s'affiche uniquement une fois que vous sélectionnez la case Console de rapports.</p> <p>Dans la liste des utilisateurs, sélectionnez les utilisateurs IBM Security QRadar Risk Manager auxquels vous souhaitez accorder le droit d'afficher les rapports générés.</p> <p>Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs. Pour plus d'informations sur les autorisations, voir <i>IBM Security QRadar Administration Guide</i>.</p>
Sélectionner tous les utilisateurs	<p>Cette option s'affiche uniquement une fois que vous sélectionnez la case Console de rapports.</p> <p>Cochez cette case si vous voulez accorder le droit à tous les utilisateurs QRadar Risk Manager d'afficher les rapports générés.</p> <p>Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs. Pour plus d'informations sur les autorisations, voir <i>IBM Security QRadar Administration Guide</i>.</p>
E-mail	Cochez cette case si vous souhaitez distribuer le rapport généré par courrier électronique.
Entrer les adresses e-mails de destination du rapport	<p>Cette option s'affiche uniquement une fois que vous sélectionnez la case E-mail.</p> <p>Entrez l'adresse électronique pour chaque destinataire du rapport généré ; séparez avec des virgules une liste d'adresses électroniques. Le nombre maximum de caractères pour ce paramètre est 255.</p> <p>Les destinataires d'e-mail reçoivent ce courrier électronique de <code>no_reply_reports@qradar</code>.</p>
Inclure le rapport sous forme de pièce jointe (non-HTML uniquement)	<p>Cette option s'affiche uniquement une fois que vous sélectionnez la case E-mail.</p> <p>Cochez cette case pour envoyer le rapport généré en tant que pièce jointe.</p>
Inclure un lien vers la console de rapports	<p>Cette option s'affiche uniquement une fois que vous sélectionnez la case E-mail.</p> <p>Cochez cette case pour joindre un lien Console de rapports dans le courrier électronique.</p>

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Dans la liste **Actions**, sélectionnez **Créer**.
3. Cliquez sur **Suivant** afin de se déplacer à la page suivante de l'assistant Création de rapports.
4. Sélectionnez la fréquence pour le planning de production de rapports.
5. Dans la sous-fenêtre Autoriser la génération manuelle de ce rapport, sélectionnez **Oui** pour activer ou **Non** pour désactiver la production manuelle du rapport. Cette option n'est pas disponible pour les rapports générés manuellement.
6. Cliquez sur **Suivant**.
7. Sélectionnez une présentation pour votre rapport puis cliquez sur **Suivant**.
8. Entrez un titre de rapport. Le titre peut comporter jusqu'à 100 caractères de longueur. N'utilisez pas des caractères spéciaux.
9. Choisissez un logo. Le logo QRadar est le logo par défaut. Pour plus d'informations sur la stratégie de marque de votre rapport, voir le *IBM Security QRadar Administration Guide*.
10. Dans la liste **Type de graphique**, sélectionnez un des rapports spécifiques QRadar Risk Manager.
11. Configurez les données de rapport pour votre graphique.
12. Cliquez sur **Sauvegarder les détails du conteneur**.
13. Cliquez sur **Suivant**.
14. Sélectionnez les formats de rapport. Vous pouvez sélectionner plusieurs options.

Remarque : Les rapports Règles du périphérique et Objets non utilisés du périphérique ne peuvent être générés qu'aux formats PDF, HTML et RTF.

15. Cliquez sur **Suivant**.
16. Sélectionnez les canaux de distribution souhaités pour votre rapport.
17. Cliquez sur **Suivant**.
18. Entrez une description pour ce rapport. La description s'affiche sur la page Récapitulatif et dans le courrier électronique de distribution de rapport généré.
19. Sélectionnez les groupes auxquels vous voulez affecter ce rapport. Pour plus d'informations sur les groupes, voir Gestion des rapports dans le *IBM Security QRadar Administration Guide*.
20. Facultatif. Sélectionnez Oui pour exécuter ce rapport une fois que la configuration de l'assistant terminée. Cliquez sur **Suivant** afin d'afficher le rapport récapitulatif. vous pouvez sélectionner les onglets disponibles sur le rapport récapitulatif afin de prévisualiser les sélections du rapport.
21. Cliquez sur **Terminer**.

Résultats

Le rapport génère immédiatement. Si vous désélectionnez la case **Voulez-vous exécuter ce rapport maintenant ?** sur la dernière page de l'assistant, le rapport est enregistré et généré comme planifié.

Le titre du rapport est le titre par défaut pour le rapport généré. Si vous reconfigurez un rapport afin d'entrer un nouveau titre, le rapport est enregistré en tant que nouveau rapport sous le nouveau nom, mais le rapport d'origine reste le même.

Edition d'un rapport

Vous pouvez modifier un rapport pour ajuster la planification d'un rapport, d'une présentation, d'une configuration, d'un titre, d'un format ou d'un mode de diffusion. Vous pouvez éditer les rapports existants ou éditer un rapport par défaut.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez le rapport que vous souhaitez éditer.
3. Dans la liste **Actions**, sélectionnez **Editer**.
4. Sélectionnez la fréquence pour la nouvelle planification de génération de rapports.
5. Pour autoriser ce rapport à générer un panneau manuel, sélectionnez une des options suivantes :
 - **Oui** - Active la production manuelle de ce rapport.
 - **Non** - Désactive la production manuelle de ce rapport.
6. Cliquez sur **Suivant** afin de se déplacer à la page suivante de l'assistant Création de rapports.
7. Configurez la présentation de votre rapport :
 - a. Dans la liste **Orientation**, sélectionnez l'orientation de la page.
 - b. Sélectionnez une option de mise en page de votre rapport IBM Security QRadar Risk Manager.
 - c. Cliquez sur **Suivant**.
8. Indiquez les valeurs pour les paramètres suivants :
 - **Titre du rapport** - Entrez un titre de rapport. Le titre peut comporter jusqu'à 100 caractères de longueur. N'utilisez pas des caractères spéciaux.
 - **Logo** - Dans la liste, sélectionnez un logo. Le logo QRadar est le logo par défaut. Pour plus d'informations sur la stratégie de marque de votre rapport, voir le *IBM Security QRadar Administration Guide*.
9. Configurez le conteneur pour vos données de rapport :
 - a. Cliquez sur **Définir**.
 - b. Configurez les données de rapport pour votre graphique.
 - c. Cliquez sur **Sauvegarder les détails du conteneur**.
 - d. Si nécessaire, répétez les étapes pour éditer des conteneurs supplémentaires.
 - e. Cliquez sur **Suivant** afin de se déplacer à la page suivante de l'assistant Création de rapports.
10. Cliquez sur **Suivant** pour passer à l'étape suivante de l'assistant Création de rapports.
11. Cochez les cases pour les formats de rapport. Vous pouvez sélectionner plus d'une option.

Remarque : Les rapports spécifiques QRadar Risk Manager tels que les rapports Règles du périphérique et Objets non utilisés du périphérique ne prennent en charge que les formats PDF, HTML et RTF.

12. Cliquez sur **Suivant** afin de se déplacer à la page suivante de l'assistant Création de rapports.
13. Sélectionnez les canaux de distribution pour votre rapport.
14. Cliquez sur **Suivant** afin de se déplacer à la page suivante de l'assistant Création de rapports.
15. Entrez une description pour ce rapport. La description s'affiche sur la page Récapitulatif et dans le courrier électronique de distribution de rapports générés.
16. Sélectionnez les groupes auxquels vous voulez affecter ce rapport. Pour plus d'informations sur les groupes, voir Gestion des rapports dans le *IBM Security QRadar Administration Guide*.
17. Facultatif. Sélectionnez Oui pour exécuter ce rapport une fois la configuration de l'assistant terminée.
18. Cliquez sur **Suivant** afin d'afficher le rapport récapitulatif. La page Récapitulatif s'affiche fournissant des détails pour le rapport. vous pouvez sélectionner les onglets disponibles sur le rapport récapitulatif afin de prévisualiser les sélections du rapport.
19. Cliquez sur **Terminer**.

Duplication d'un rapport

Vous pouvez dupliquer n'importe quel rapport.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez le rapport que vous souhaitez dupliquer.
3. Dans la liste **Actions**, cliquez sur **Dupliquer**.
4. Entrez un nouveau nom, sans espaces, pour le rapport.

Partage d'un rapport

Vous pouvez partager des rapports avec d'autres utilisateurs. Lorsque vous partagez un rapport, vous devez fournir une copie du rapport sélectionné à un autre utilisateur pour modifier ou planifier.

Avant de commencer

Vous devez disposer de privilèges administratifs afin de partager des rapports. En outre, pour qu'un nouvel utilisateur puisse afficher et accéder aux rapports, un administrateur doit partager tous les rapports nécessaires avec le nouvel utilisateur.

Pourquoi et quand exécuter cette tâche

Toutes les mises à jour effectuées par l'utilisateur sur un rapport partagé n'affectent pas la version originale du rapport.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez les rapports que vous souhaitez partager.
3. Dans la liste **Actions**, cliquez sur l'option pour effectuer un **partage**.
4. Dans la liste des utilisateurs, sélectionnez les utilisateurs avec lesquels vous souhaitez partager ce rapport.

Si aucun utilisateur ayant un accès approprié n'est disponible, un message s'affiche.

5. Cliquez sur **Partager**.

Pour plus d'informations sur les rapports, voir *IBM Security QRadar - Guide d'utilisation*.

Configuration des graphiques

Le type de graphique détermine les données configurées et affichées dans le graphique. Vous pouvez créer plusieurs graphiques pour des données spécifiques collectées par les unités dans IBM Security QRadar Risk Manager.

Les types de graphique suivants sont spécifiques à QRadar Risk Manager :

- Connection
- Règles du périphérique
- Objets non utilisés du périphérique

Graphiques de connexion

Vous pouvez utiliser le graphique **Connexions** pour afficher les informations de connexion réseau. Vous pouvez baser vos graphiques sur des données provenant des recherches enregistrées à partir de l'onglet **Risques**.

Vous pouvez personnaliser les données que vous souhaitez afficher dans le rapport généré. Vous pouvez configurer le graphique pour tracer les données sur une période de temps configurable. Cette fonctionnalité vous aide à détecter les tendances des connexions.

Le tableau suivant fournit les informations de configuration pour le conteneur de graphique de connexions.

Tableau 34. Paramètres du graphique de connexions

Paramètre	Description
Détails du conteneur - Connexions	
Titre du graphique	Entrez un titre de graphique ne dépassant pas les 100 caractères.
Sous-titre du graphique	Décochez la case pour modifier le sous-titre créé automatiquement. Entrez un titre ne dépassant pas les 100 caractères.
Type de graphique	<p>Dans la liste, sélectionnez le type de graphique à afficher sur le rapport généré. Les options sont les suivantes :</p> <p>Barres - Affiche les données dans un graphique à barres. Il s'agit du type de graphique par défaut. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée.</p> <p>Courbes - Affiche les données dans un graphique à courbes.</p> <p>Secteurs - Affiche les données dans un graphique circulaire. Ce type de graphique nécessite que la recherche enregistrée corresponde à une recherche groupée.</p> <p>Barres empilées - Affiche les données dans un graphique à barres empilées.</p> <p>Courbes superposées - Affiche les données dans un graphique à courbes empilées.</p> <p>Table - Affiche les données sous la forme d'un tableau. L'option Table est uniquement disponible pour le conteneur de largeur pleine page seulement.</p>
Graphique	Dans la liste, sélectionnez le nombre de connexions à afficher dans le rapport généré.
Planification manuelle	<p>Le panneau Planification manuelle s'affiche uniquement si vous sélectionnez l'option de planification Manuelle dans l'Assistant Création de rapports.</p> <p>Pour créer une planification manuelle :</p> <ol style="list-style-type: none"> 1. Dans la zone de liste De, entrez la date de début que vous souhaitez pour le rapport ou sélectionnez la date en utilisant l'icône Calendaire. La valeur configurée par défaut est la date actuelle. 2. Dans les zones de liste, sélectionnez l'heure de début que vous souhaitez pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1:00. 3. Dans la liste A, entrez la date de fin choisie pour le rapport ou sélectionnez la date en utilisant l'icône de Calendrier. La valeur configurée par défaut est la date actuelle. 4. Dans les listes, sélectionnez l'heure de fin choisie pour le rapport. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1:00.

Tableau 34. Paramètres du graphique de connexions (suite)

Paramètre	Description
Planification horaire	<p>Le panneau Planification horaire s'affiche uniquement si vous sélectionnez l'option de planification Horaire dans l'assistant Création de rapports.</p> <p>La planification horaire place automatiquement dans des graphiques toutes les données de l'heure précédente.</p>
Planification quotidienne	<p>La sous-fenêtre Planification quotidienne s'affiche uniquement si vous sélectionnez l'option de planification Quotidienne dans l'assistant Création de rapports.</p> <p>Sélectionnez une des options suivantes :</p> <p>Toutes les données de la journée précédente (24 heures)</p> <p>Données de la journée précédente depuis - A partir des listes, sélectionnez la durée que vous souhaitez pour le rapport généré. L'heure est disponible par incréments d'une demi-heure. La valeur par défaut est 1:00.</p>
Planification hebdomadaire	<p>Le panneau Planification hebdomadaire s'affiche uniquement si vous sélectionnez l'option de planification Hebdomadaire dans l'assistant Création de rapports.</p> <p>Sélectionnez une des options suivantes :</p> <p>Toutes les données de la semaine précédente</p> <p>Toutes les données de la semaine précédente à partir de - A partir des listes, sélectionnez la durée choisie pour le rapport généré. La valeur configurée par défaut est le dimanche.</p>
Planification mensuelle	<p>La sous-fenêtre Planification mensuelle s'affiche uniquement si vous sélectionnez l'option de planification Mensuelle dans l'assistant Création de rapports.</p> <p>Sélectionnez une des options suivantes :</p> <p>Toutes les données du mois précédent</p> <p>Données du mois précédent depuis - A partir des listes, sélectionnez la durée que vous souhaitez pour le rapport généré. La valeur configurée par défaut s'étend du 1er au 31.</p>
Contenu du graphique	
Groupe	<p>Dans la liste, sélectionnez un groupe de recherche sauvegardée afin d'afficher les recherches sauvegardées appartenant à ce groupe dans la liste Recherches sauvegardées disponibles.</p>
Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste	<p>Pour affiner la liste Recherches sauvegardées disponibles, entrez le nom de la recherche que vous souhaitez localiser dans la zone Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste. Vous pouvez également entrer un mot-clé pour afficher la liste des recherches incluant ce mot clé. Par exemple, entrez DMZ afin d'afficher une liste de toutes les recherches qui incluent DMZ dans le nom de la recherche.</p>

Tableau 34. Paramètres du graphique de connexions (suite)

Paramètre	Description
Recherches sauvegardées disponibles	Fournit une liste des recherches enregistrées disponibles. Par défaut, toutes les recherches sauvegardées disponibles sont affichées. Cependant, vous pouvez filtrer la liste en sélectionnant un groupe de la liste Groupes ou en tapant le nom d'une recherche enregistrée connue dans la zone Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste .
Créer une recherche de connexions	Cliquez sur Créer une recherche de connexions afin de créer une nouvelle recherche.

Graphiques Règles du périphérique

Vous pouvez utiliser le graphique Règles du périphérique pour afficher les règles de pare-feu et le nombre d'événements de règles de pare-feu déclenchés dans votre réseau.

Les rapports Règles d'unité vous permettent de créer un rapport pour les règles de pare-feu suivantes :

- Règles d'unité d'acceptation les plus actives
- Règles d'unité de refus les plus actives
- Règles d'unité d'acceptation les moins actives
- Règles d'unité de refus les moins actives
- Règles d'unité inutilisées
- Règles d'unité grisées

Les rapports que vous générez vous permettent de comprendre quelles règles sont acceptées, refusées, inutilisées ou appliquées dans un périphérique unique, dans un adaptateur spécifique ou dans plusieurs périphériques. Les rapports permettent à IBM Security QRadar Risk Manager d'automatiser la production de rapports sur l'état des règles de vos périphériques et d'afficher les rapports dans IBM Security QRadar SIEM Console.

Cette fonctionnalité vous permet d'identifier la façon dont les règles sont utilisées sur vos périphériques réseau.

Pour créer un conteneur pour le graphique de règles de périphérique, configurez les valeurs des paramètres suivants :

Tableau 35. Graphiques Règles d'unité

Paramètre	Description
Détails du conteneur - Règles du périphérique	
Limiter les règles aux premières	<p>Dans la liste, sélectionnez le nombre de règles qui s'affichent dans le rapport généré.</p> <p>Par exemple, si vous limitez votre rapport aux 10 premières règles, créez un rapport pour les règles d'acceptation les plus utilisées dans tous les périphériques. Le rapport renvoie 10 résultats. Les résultats contiennent une liste des 10 règles d'acceptation les plus utilisées en fonction du nombre d'événements parmi tous les périphériques visibles dans QRadar Risk Manager.</p>

Tableau 35. Graphiques Règles d'unité (suite)

Paramètre	Description
Type	<p>Sélectionnez le type de règles de périphérique à afficher dans le rapport. Les options sont les suivantes :</p> <p>Règles d'acceptation les plus utilisées - Affiche les règles d'acceptation les plus utilisées par le nombre d'événements pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus grand nombre d'événements acceptés, dans l'ordre décroissant, pour l'intervalle de temps spécifié dans le rapport.</p> <p>Règles de refus les plus utilisées - Affiche les règles de refus les plus utilisées par le nombre d'événements pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus grand nombre d'événements refusés, dans l'ordre décroissant, pour l'intervalle de temps spécifié dans le rapport.</p> <p>Règles inutilisées - Affiche toutes les règles d'un périphérique unique ou d'un groupe de périphériques inutilisées. Les règles inutilisées ne présentent aucun événement pour l'intervalle de temps spécifié pour le rapport.</p> <p>Règles d'acceptation les moins utilisées - Affiche les règles d'acceptation les moins utilisées pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus petit nombre d'événements acceptés, dans l'ordre croissant, pour l'intervalle de temps spécifié dans le rapport.</p> <p>Règles de refus les moins utilisées - Affiche les règles de refus les moins utilisées pour un périphérique unique ou un groupe de périphériques. Ce rapport répertorie les règles présentant le plus petit nombre d'événements refusés, dans l'ordre croissant, pour l'intervalle de temps spécifié dans le rapport.</p> <p>Règles en mémoire vive - Affiche toutes les règles d'un périphérique unique ne pouvant s'appliquer car la règle est verrouillée par une règle en cours d'application. Les résultats s'affichent dans un tableau des règles à l'origine de la désactivation et de toutes les règles ne pouvant s'appliquer sur votre périphérique, car elles sont désactivées par une règle en cours d'application sur le périphérique.</p> <p>Remarque : Les rapports de règles grisées peuvent uniquement être exécutés par un périphérique unique. Ces règles ne présentent aucun événement pour l'intervalle de temps spécifié.</p>

Tableau 35. Graphiques Règles d'unité (suite)

Paramètre	Description
Plage de date/heure	<p>Sélectionnez l'intervalle de temps de votre rapport. Les options sont les suivantes :</p> <p>Configuration en cours - Les résultats du rapport Règles du périphérique sont basés sur les règles existant dans la configuration actuelle du périphérique. Ce rapport affiche les règles et les nombres d'événements pour la configuration de périphérique existante.</p> <p>La configuration d'un périphérique réseau est basée sur sa dernière sauvegarde par Configuration Source Management.</p> <p>Intervalle - Les résultats du rapport Règles du périphérique sont basés sur les règles existant dans l'intervalle de temps de l'intervalle. Ce rapport affiche les règles et les nombres d'événements pour l'intervalle spécifié compris entre la dernière heure et 30 jours.</p> <p>Plage spécifique - Les résultats du rapport Règles du périphérique sont basés sur les règles existant entre l'heure de début et l'heure de fin de l'intervalle. Ce rapport affiche les règles et les nombres d'événements pour l'intervalle de temps spécifié.</p>
Fuseau horaire	<p>Sélectionnez le fuseau horaire que vous souhaitez utiliser comme base de votre rapport. Le fuseau horaire par défaut est basé sur la configuration de votre QRadar SIEM Console.</p> <p>Lors de la configuration du paramètre Fuseau horaire pour votre rapport, prenez en compte l'emplacement des périphériques associés aux données de rapport. Si le rapport utilise des données couvrant plusieurs fuseaux horaires, les données utilisées pour le rapport sont basées sur l'intervalle de temps spécifique du fuseau horaire.</p> <p>Par exemple, si votre QRadar SIEM Console est configurée pour l'heure standard EST, que vous planifiez un rapport quotidien entre 13h00 et 15h00 et que vous paramétrez le fuseau horaire sur l'heure standard CST, les résultats du rapport contiennent des informations entre 14h00 et 16h00 EST.</p>

Tableau 35. Graphiques Règles d'unité (suite)

Paramètre	Description
Sélection de données ciblées	<p>Sélection de données ciblées est utilisé pour filtrer la plage Date/Heure à une valeur spécifique. Grâce aux options Sélection de données ciblées, vous pouvez créer un rapport pour afficher vos règles de périphérique sur une période de temps personnalisée définie, avec la possibilité d'inclure uniquement les données des heures et des jours que vous sélectionnez.</p> <p>Par exemple, vous pouvez programmer un rapport pour qu'il soit exécuté du 1er au 31 octobre et afficher vos règles les plus actives, les moins actives ou inutilisées ainsi que leurs nombres de règles générées pendant vos heures de travail, telles que du lundi au vendredi, de 8 heures à 21 heures.</p> <p>Remarque : Les détails de filtre s'affichent uniquement lorsque vous cochez la case Sélection de données ciblées dans l'assistant Création de rapports.</p>
Format	<p>Sélectionnez le format de votre rapport de règles de périphérique. Les options sont les suivantes :</p> <p>One aggregate report for specified devices- Ce format de rapport cumule les données de rapport de plusieurs périphériques.</p> <p>Par exemple, si vous créez un rapport pour afficher les dix règles les plus souvent refusées, un rapport de cumul affiche les dix règles les plus souvent refusées dans tous les périphériques sélectionnés pour le rapport. Ce rapport renvoie 10 résultats au total pour le rapport.</p> <p>One report per device - Ce format de rapport affiche les données de rapport pour un seul périphérique.</p> <p>Par exemple, si vous créez un rapport pour afficher les dix règles les plus souvent refusées, un rapport de cumul affiche les dix règles les plus souvent refusées pour chaque périphérique sélectionné pour le rapport. Ce rapport renvoie les 10 meilleurs résultats pour chaque périphérique sélectionné pour le rapport. Si vous avez sélectionné 5 périphériques, le rapport renvoie 50 résultats.</p> <p>Remarque : Les rapports de règles grisées peuvent afficher uniquement un rapport par périphérique.</p>

Tableau 35. Graphiques Règles d'unité (suite)

Paramètre	Description
Unités	<p>Sélectionnez les périphériques contenus dans le rapport. Les options sont les suivantes :</p> <p>Toutes les unités - Sélectionnez cette option pour inclure tous les périphériques de QRadar Risk Manager de votre rapport.</p> <p>Adaptateur - Dans la liste, sélectionnez un type d'adaptateur à inclure dans votre rapport. Un seul type d'adaptateur peut être sélectionné dans la liste pour un rapport.</p> <p>Unités spécifiques - Sélectionnez cette option pour intégrer uniquement des périphériques spécifiques dans votre rapport. La fenêtre de sélection d'unité vous permet de sélectionner et d'ajouter des périphériques à votre rapport.</p> <p>Pour ajouter des périphériques individuels à votre rapport, procédez comme suit :</p> <ol style="list-style-type: none"> 1. Cliquez sur Parcourir pour afficher la fenêtre de sélection d'unité. 2. Sélectionnez tous les périphériques et cliquez sur Ajouter la sélection. <p>Pour ajouter tous les périphériques à votre rapport, procédez comme suit :</p> <ol style="list-style-type: none"> 1. Cliquez sur Parcourir pour afficher la fenêtre de sélection d'unité. 2. Cliquez sur Tout ajouter. <p>Pour rechercher des périphériques à intégrer à votre rapport, procédez comme suit :</p> <ol style="list-style-type: none"> 1. Cliquez sur Parcourir pour afficher la fenêtre de sélection d'unité. 2. Cliquez sur Rechercher. 3. Sélectionnez les options de recherche pour filtrer la liste complète de périphériques par configuration obtenue, adresse IP ou CIDR, nom d'hôte, type, adaptateur, fournisseur ou modèle. 4. Cliquez sur Rechercher. 5. Sélectionnez tous les périphériques et cliquez sur Ajouter la sélection.

Graphiques Objets non utilisés du périphérique

Un rapport Objets non utilisés du périphérique affiche les groupes de référence d'objet qui ne sont pas en cours d'utilisation par votre périphérique réseau.

Ce rapport affiche les références d'objet telles qu'une collection d'adresses IP, de plages d'adresses CIDR ou de noms d'hôtes non utilisés par votre périphérique réseau.

Lorsque vous configurez un conteneur d'objets d'unité non utilisés, vous pouvez configurer les valeurs pour les paramètres suivants :

Tableau 36. Paramètres de rapports Objets non utilisés du périphérique

Paramètre	Description
Détails du conteneur - Objets non utilisés du périphérique	
Limiter les objets aux premiers	Dans la liste, sélectionnez le nombre de règles qui s'affichent dans le rapport généré.
Unités	<p>Sélectionnez les périphériques contenus dans le rapport. Les options sont les suivantes :</p> <p>Toutes les unités - Sélectionnez cette option pour inclure tous les périphériques d'IBM Security QRadar Risk Manager de votre rapport.</p> <p>Adaptateur - Dans la liste, sélectionnez un type d'adaptateur à inclure dans votre rapport. Un seul type d'adaptateur peut être sélectionné dans la liste pour un rapport.</p> <p>Unités spécifiques - Sélectionnez cette option pour intégrer uniquement des périphériques spécifiques dans votre rapport. La fenêtre de sélection d'unité vous permet de sélectionner et d'ajouter des périphériques à votre rapport.</p> <p>Pour ajouter des périphériques individuels à votre rapport, procédez comme suit :</p> <ol style="list-style-type: none"> 1. Cliquez sur Parcourir pour afficher la fenêtre de sélection d'unité. 2. Sélectionnez tous les périphériques et cliquez sur Ajouter la sélection. <p>Pour ajouter tous les périphériques à votre rapport, procédez comme suit :</p> <ol style="list-style-type: none"> 1. Cliquez sur Parcourir pour afficher la fenêtre de sélection d'unité. 2. Cliquez sur Tout ajouter. <p>Pour rechercher des périphériques à intégrer à votre rapport, procédez comme suit :</p> <ol style="list-style-type: none"> 1. Cliquez sur Parcourir pour afficher la fenêtre de sélection d'unité. 2. Cliquez sur Rechercher. 3. Sélectionnez les options de recherche pour filtrer la liste complète de périphériques par configuration obtenue, adresse IP ou CIDR, nom d'hôte, type, adaptateur, fournisseur ou modèle. 4. Cliquez sur Rechercher. 5. Sélectionnez tous les périphériques et cliquez sur Ajouter la sélection.

16 Données de journaux d'audit

Les modifications apportées par les utilisateurs IBM Security QRadar Risk Manager sont enregistrées dans l'onglet **Activité du journal** de IBM Security QRadar SIEM.

Tous les journaux apparaissent dans la catégorie Audit du gestionnaire de risques. Pour plus d'informations sur l'utilisation de l'onglet **Activité du journal** dans QRadar SIEM, voir le *IBM Security QRadar - Guide d'utilisation*.

Actions consignées

Les actions sont consignées pour les composants.

Le tableau suivant répertorie les catégories et les actions correspondantes qui sont consignées.

Tableau 37. Actions consignées

Catégorie	Action
Moniteur de politique d'administration	Créez une question.
	Editez une question.
	Supprimez une question.
	Soumettez manuellement une question.
	Soumettez automatiquement une question.
	Validez les résultats.
	Révoquez la validation des résultats.
Modèle de topologie	Créez un modèle de topologie.
	Editez un modèle de topologie.
	Supprimez un modèle de topologie.
Topologie	Enregistrez la disposition.
	Créez une recherche sauvegardée de topologie.
	Editez une recherche sauvegardée de topologie.
	Supprimez une recherche sauvegardée de topologie.
	Mise en place d'un système de prévention contre les intrusions.
Moniteur de configuration	Création d'un mappage de source de journal
	Edition d'un mappage de source de journal
	Suppression d'un mappage de source de journal
Simulations	Créez une simulation.
	Editez une simulation.
	Supprimez une simulation.
	Exécutez manuellement une simulation.
	Exécutez automatiquement une simulation.
	Validez les résultats de la simulation.
	Révoquez les résultats de la simulation.

Tableau 37. Actions consignées (suite)

Catégorie	Action
Configuration Source Management	Authentifiez-vous pour la première fois auprès d'une session avec succès.
	Ajoutez un périphérique.
	Supprimez un périphérique.
	Editez l'adresse IP ou l'adaptateur pour un périphérique.
	Enregistrez une configuration de données d'identification.
	Supprimez une configuration de données d'identification.
	Enregistrez une configuration de protocole.
	Supprimez une configuration de protocole.
	Créez une planification pour un journal de sauvegarde.
	Supprimez une planification pour un journal de sauvegarde.
	Editez un journal de sauvegarde.
	Ajoutez un journal de sauvegarde.
	Supprimez un journal de sauvegarde.
	Exécutez un journal de sauvegarde planifié.
	Exécutez un travail planifié qu'il ait abouti ou échoué.
	Une fois le traitement d'un travail de sauvegarde terminé et la configuration conservée, aucun changement n'est constaté.
	Une fois le traitement d'un travail de sauvegarde terminé et la configuration conservée, des changements ont été constatés.
	Une fois le traitement d'un travail de sauvegarde terminé et la configuration conservée, des changements non définitifs ont été constatés.
	Le traitement d'un travail de sauvegarde est terminé et la configuration auparavant conservée a disparu du périphérique.
	Début d'une tentative de mise en fonctionnement de l'adaptateur comprenant des protocoles et des données d'identification.
Une tentative de mise en fonctionnement de l'adaptateur comprenant des protocoles et des données d'identification a abouti.	

Affichage de l'activité d'utilisateur

Vous pouvez afficher l'activité d'utilisateur pour les utilisateurs IBM Security QRadar Risk Manager.

Procédure

1. Cliquez sur l'onglet **Activité du journal**. Si vous avez déjà sauvegardé une recherche en tant que recherche par défaut, les résultats de cette recherche sauvegardée s'affichent.
2. Cliquez sur **Rechercher > Nouvelle recherche** pour créer une nouvelle recherche.

3. Dans la sous-fenêtre **Intervalle**, sélectionnez une option pour l'intervalle à capturer pour cette recherche.
4. Dans la sous-fenêtre **Paramètres de recherche**, définissez vos critères de recherche :
 - a. Dans la première liste, sélectionnez **Catégorie**.
 - b. Dans la liste déroulante **Catégorie de niveau supérieur**, sélectionnez **Audit du gestionnaire de risques**.
 - c. Facultatif. Dans la liste déroulante **Catégorie de niveau inférieur**, sélectionnez une catégorie pour affiner votre recherche.
5. Cliquez sur **Ajouter un filtre**.
6. Cliquez sur **Filtre** pour rechercher les événements de QRadar Risk Manager.

Affichage du fichier journal

Les journaux d'audit, stockés en texte brut, sont archivés et compressés lorsque le fichier du journal d'audit atteint une taille de 200 Mo.

Pourquoi et quand exécuter cette tâche

Le fichier journal en cours est appelé audit.log. Si le fichier journal d'audit atteint la taille de 200 Mo, il est compressé et l'ancien journal d'audit est renommé audit.1.gz. Le numéro de fichier incrémente chaque fois qu'un fichier journal est archivé. IBM Security QRadar Risk Manager peut stocker jusqu'à 50 fichiers journaux archivés.

La taille maximale d'un message d'audit (si l'on exclut la date, l'heure et le nom d'hôte) est de 1024 caractères.

Chaque entrée du fichier journal s'affiche au format suivant :

```
<date_time> <host name> <user>@<IP address>
(thread ID) [<category>] [<sub-category>]
[<action>] <payload>
```

Le tableau suivant décrit les paramètres utilisés dans le fichier journal.

Tableau 38. Informations de fichier journal d'audit

Paramètre	Description
<date_time>	La date et l'heure de l'activité au format : Mois Date HH:MM:SS.
<host name>	Le nom d'hôte de la console dans laquelle cette activité a été consignée.
<user>	Le nom de l'utilisateur qui a effectué l'action.
<IP address>	L'adresse IP de l'utilisateur qui a effectué l'action.
(thread ID)	L'identificateur de l'unité d'exécution Java™ qui a consigné cette activité.
<category>	La catégorie de haut niveau de cette activité.
<sub-category>	La catégorie de bas niveau de cette activité.
<action>	L'activité qui s'est déroulée.
<payload>	L'enregistrement complet qui a changé, le cas échéant.

Procédure

1. En utilisant Secure Shell (SSH), connectez-vous à votre console IBM Security QRadar SIEM Console en tant qu'utilisateur root.

2. Grâce à SSH à partir de la console IBM Security QRadar SIEM Console, connectez-vous au dispositif QRadar Risk Manager en tant que superutilisateur.
3. Accédez au répertoire suivant : `/var/log/audit`
4. Ouvrez votre fichier suivi responsable.

Détails du fichier journal

Les administrateurs utilisent les fichiers journaux d'IBM Security QRadar Risk Manager pour afficher l'activité des utilisateurs et traiter les incidents système.

Le tableau suivant décrit l'emplacement et le contenu des fichiers journaux de QRadar Risk Manager.

Tableau 39. Fichiers journaux QRadar Risk Manager

Nom du fichier journal	Emplacement	Description
<code>audit.log</code>	<code>/var/log/audit/</code>	Contient les informations d'audit en cours.
<code>audit.<1-50>.gz</code>	<code>/var/log/audit/</code>	Contient les informations d'audit archivées. Lorsque le fichier <code>audit.log</code> atteint la taille de 200 Mo, il est comprimé et renommé <code>audit.1.gz</code> . Le numéro de fichier incrémente chaque fois qu'un fichier journal est archivé. QRadar Risk Manager peut stocker jusqu'à 50 fichiers journaux archivés.
<code>qradar.log</code>	<code>/var/log/</code>	Contient toutes les informations de processus qui sont consignées par le serveur QRadar Risk Manager.
<code>qradar.error</code>	<code>/var/log/</code>	Toutes les exceptions <code>System.out</code> et tous les messages <code>System.err</code> qui sont générés par le serveur QRadar Risk Manager sont consignés dans ce fichier.

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 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 tacites, 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.

Toute référence à ces informations sur des sites web non-IBM est fournie par souci de commodité uniquement et ne constitue en aucun cas une adhésion au contenu de ces sites web. Les documents sur ces sites web ne font pas partie des documents de ce produit IBM et l'utilisation de ces sites web se fait à vos propres risques.

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

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 et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

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.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées 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. Tous ces noms sont fictifs, et toute ressemblance avec des noms de personnes ou de sociétés réelles serait purement fortuite.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group 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.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site web IBM.

Utilisation personnelle

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ou publier tout ou partie de ces publications ou en produire des oeuvres dérivées sans le consentement exprès d'IBM.

Utilisation commerciale

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas reproduire, distribuer ou afficher tout ou partie de ces publications en dehors de votre entreprise ou en tirer des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Exception faite des droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, tacite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité en ligne

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des sessions 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 de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (<http://www.ibm.com/privacy/fr/fr>) et 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 que 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 des logiciels et des produits IBM Security QRadar Risk Manager.

Les références croisées suivantes sont utilisées :

- *Voir* renvoie d'un terme peu utilisé au terme généralement utilisé ou d'une abréviation à la forme développée.
- *Voir aussi* renvoie à un terme connexe ou à un anonyme.

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

«A» «C» «D» «G» «I» «L», à la page 150 «M», à la page 150 «N», à la page 150 «P», à la page 150 «R», à la page 150 «T», à la page 150 «V», à la page 150

A

actif Objet administrable déployé ou destiné à être utilisé dans un environnement opérationnel.

adaptateur Composant logiciel intermédiaire qui permet à deux autres composants logiciels de communiquer entre eux.

attaque Toute tentative, par une personne non autorisée, de compromettre l'exécution d'un logiciel ou d'un système en réseau.

attribut Données associées à un composant. Par exemple, un nom d'hôte une adresse IP ou le nombre de disques durs peuvent être des attributs associés à un composant de serveur.

C

chemin d'attaque Source, destination et périphériques associés à une attaque.

conversion d'adresses réseau (NAT) Dans un pare-feu, conversion d'adresses IP (Internet Protocol) sécurisées en adresses enregistrées en externe. Elle

permet les communications avec les réseaux externes mais masque les adresses IP utilisées dans le pare-feu.

D

données voisines

Données collectées depuis des adaptateurs et utilisées pour identifier des informations sur des dispositifs connectés à des hôtes gérés QRadar Quality Manager.

G

graphique de série temporelle

Représentation graphique des connexions réseau dans le temps.

graphique de topologie

Graphique qui décrit les sous-réseaux, les périphériques et les pare-feux.

graphique des connexions

Un graphique qui affiche les connexions entre les noeuds de réseau distant et adresses IP locales et les noeuds de réseau local.

I

indicateur NAT

Indicateur sur le graphique de topologie qui indique que le chemin entre deux connexions réseau contient des conversions d'adresses sources ou de destination.

indicateur de risque

Mesure du degré d'exposition d'un système à une infraction de sécurité.

infraction

Acte qui ignore ou enfreint la politique de l'entreprise.

L

ligne de connexion

Ligne sur le graphique de connexion entre un noeud de réseau distant et un noeud de réseau local ou entre deux noeuds de réseau local.

M

modèle de topologie

Représentation virtuelle de la disposition des actifs réseau utilisée pour simuler une attaque.

N

NAT Voir conversion d'adresses réseau (NAT).

P

périphérique à contextes multiples

Dispositif unique partitionné en plusieurs périphériques virtuels. Chaque périphérique virtuel est un périphérique indépendant, avec sa propre politique de sécurité.

protocole risqué

Protocole associé aux services qui s'exécutent dans un port ouvert via des communications entrantes d'Internet vers la DMZ.

R

recherche

Fonction qui permet d'effectuer des recherches dans un ensemble de résultats provenant d'une recherche réalisée.

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

T

test d'actif

Test utilisé pour identifier les indicateurs de risque potentiels qui signalent lorsque les actifs d'un réseau violent une règle définie ou introduisent des risques dans l'environnement.

test de contribution

Test qui examine les indicateurs de risque spécifiés dans une question.

test de restriction

Test qui filtre les résultats renvoyés par une question de test de contribution.

V

vulnérabilité

Risque lié à la sécurité dans un système d'exploitation, un logiciel système ou un composant de logiciel d'application.

Index

A

- actifs 77
- activité de l'utilisateur
 - journal d'audit 142
- administrateur réseau ix
- afficheur de journal de sauvegarde 23
- ajouter un actif 98
- Applications 30
- approbation de simulation
 - révocation 118
- assistant de rapports 128

C

- cas d'utilisation du moniteur de politique d'administration
 - communication possible sur les actifs protégés 78
 - communication réelle pour DMZ 76
 - communication test d'unité sur l'accès Internet 79
- CheckPoint SmartConsole
 - comptage des règles 90
- chemin d'attaque 60
- coefficient d'importance 75
- communication réelle 68
 - questions de contribution 65
- configuration 9
- configuration de périphérique 21, 50
 - comparaison 48
- configuration de réseau 114
- configuration des unités réseau
 - recherche 47
- Configuration Source Management 13
- conformité 103
- connexions 5, 31, 45
 - recherche 39
- connexions réseau
 - surveiller 5
- CPSMS 93
- création
 - profils de test de performances 103
- création de simulation 115
- critères de recherche 40

D

- données d'identification 13
 - configuration 14
- données de journaux d'audit 141
- données des journaux 141
- données voisines
 - collecte 22

E

- éditer un actif 98
- emplacements des journaux 144
- état de sauvegarde 23

- évaluer des unités 77
- exportation 45, 88

F

- fichier journal 143, 144
- filtrage des règles de périphérique 55
- fonctions non prises en charge 4

G

- glossaire 149
- graphique 34, 36, 38
- graphique de série temporelle 34, 38
- graphique de topologie 57
- graphique des connexions 36
- graphiques 34
 - configuration 132
 - connexions 132
 - Objets non utilisés du périphérique 139
 - règles d'unité 135
- groupes de périphériques
 - regroupement de périphériques 60

H

- haute disponibilité (HA) 4
- heure système 10

I

- importation 88
- importation de périphérique, fichier CSV 17
- Indicateurs NAT 58
- information de configuration de sauvegarde 22
- informations de connexion 4
- informations de connexion par défaut 4
- informations de sauvegarde 22
- informations système 9
- infraction 60
- intégrations de sécurité
 - QRadar Risk Manager 90
- introduction ix
- Intrusion Prevention System 59
 - suppression 59
- IPS 59
- IPv6 4

J

- journal d'audit
 - actions 141
- journal de sauvegarde 23

L

- les rapports
 - génération manuelle 127
 - gestion 127
- liste de périphériques
 - filtre 19

M

- mappage de sources de journal 52
 - création 53
- masques de réseau non contigus 4
- mode de contrôle 87
- mode document
 - navigateur Web Internet Explorer 4
- mode moniteur 86, 105
- mode navigateur
 - navigateur Web Internet Explorer 4
- modèle de topologie 114, 121
 - affectation à un groupe 126
 - affichage des groupes 125
 - copier les modèles vers les groupes 126
 - création 122
 - création d'un groupe 125
 - duplication 124
 - modification 124
 - modification d'un groupe 125
 - suppression 124
- modèles de topologie
 - groupe 125
- moniteur de politique d'administration
 - gestion des questions 63
 - scénarios d'utilisation 96
 - supprimer l'élément du groupe de question 126
- Moniteur de politique d'administration 63
- mot de passe 4

N

- nom d'utilisateur 4

O

- onglet Actifs 98

P

- PCI section 1 77
- PCI section 10 77
- périphérique
 - ajout 18, 49
 - gestion de périphériques 49, 51
 - suppression 50
- périphériques 18
- planification des reconnaissances 30
- port ouvert 115

- profil d'actif 98
- profils d'actifs 102
- protocole 115
- protocoles 27, 28, 115
- protocoles:à risque 77

Q

- QRadar Risk Manager 3
 - intégration 90
- question 75, 79, 104
 - soumission 80
- question d'actif 75
- question de conformité d'actif 104, 105
- questions de contribution dépréciées 68
- questions de contrôle 87
- questions de moniteur de politique d'administration
 - exportation 89
- questions de restriction 68
- Questions de test de contribution dépréciées 73
- questions du moniteur de politique d'administration
 - importation 89
- questions moniteur de politique d'administration 64, 88
 - évaluation des résultats 85
 - groupement 88
- questions relatives aux unités/règles 79

R

- rapport 128
 - duplication 132
 - édition 131
 - partage 132
- recherche 42
 - annulation 44
 - configuration du comptage de règles 96
 - CSM 95
 - SmartDashboard 92
- reconnaissance d'unité 15, 16
- reconnaissance de périphérique 51
- renommage d'un travail de sauvegarde 26
- résultats
 - validation 86
- Résultats d'actifs 80
- résultats de l'analyse
 - visualisation 105
- résultats de l'unité 83
- résultats de la recherche 43, 44
- résultats de simulation 116
 - gestion 116
 - validation 118
- risques pour les réseaux 114
- routage dynamique 4

S

- sauvegarde 44
- sauvegarde de critères 102
- sauvegarde des critères de recherche d'un actif 102

- simulation 115
 - duplication 113
 - simulation manuelle 114
 - suppression 113
- simulation SSH 115
- simulations 109
 - édition 113
 - groupement 120
 - suivi 119
- Simulations 109
- surveillance des questions 105

T

- test de performances de conformité 103
- tests de communication possible
 - questions de contribution 70
 - tests de restriction 73
- tests de simulation 110
- travail de sauvegarde 23, 25, 27

U

- unité
 - ajout 18
 - importation 16
 - suppression 19
- unités
 - ajout 19
- unités/règles, questions de test 74

V

- violations 86
- visualisation
 - résultats de l'analyse 105

