IBM Security QRadar

Guide de configuration de l'évaluation de la vulnérabilité

Octobre 2017

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 89.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.2.5 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Présentation des configurations d'évaluation de la vulnérabilité QRadar

L'intégration avec des scanners d'évaluation de la vulnérabilité permet aux administrateurs et aux professionnels de la sécurité de construire des profils d'évaluation de la vulnérabilité pour des actifs réseau.

Utilisateurs concernés

Les administrateurs doivent disposer d'un accès à QRadar et connaître le réseau de l'entreprise et les technologies de réseau.

Documentation technique

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

Contacter le service clients

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

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

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différentes lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar peut être utilisé uniquement de façon réglementaire. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

1 Présentation du scanner d'évaluation de la vulnérabilité

Intégrez à IBM Security QRadar des scanners d'évaluation des vulnérabilités afin de fournir des profils d'évaluation des vulnérabilités pour les actifs réseau.

Les références à QRadar s'appliquent à tous les produits capables de collecter des informations d'évaluation de la vulnérabilité.

Les profils d'actif pour les serveur et les hôtes de votre réseau fournissent des informations utiles pour résoudre les problèmes de sécurité. L'utilisation des profils d'actifs vous permettent de relier les infractions survenant sur votre système aux actifs physiques ou virtuels dans le cadre de vos investigations de sécurité. Les données d'actif aident à identifier les menaces, les vulnérabilités, les services et ports concernés, et à suivre l'utilisation des actifs sur votre réseau.

L'onglet **Actifs** offre une vue unifiée des informations connues concernant vos actifs. Lorsque de nouvelles informations sont fournies au système via l'évaluation des vulnérabilités, le système met à jour le profil d'actif. Les profils d'évaluation de la vulnérabilité utilisent des données d'événement corrélées, l'activité du réseau, ainsi que des changements de comportement afin de déterminer le niveau de menace pour les éléments métier essentiels de votre réseau. Vous pouvez planifier des analyses et vous assurer que les informations de vulnérabilité sont pertinentes pour les actifs du réseau.

Installation du module Java Cryptography Extension Unlimited

Le module Java™ Cryptography Extension (JCE) est une infrastructure Java qui est requise pour déchiffrer des algorithmes de cryptographie avancés pour messages d'alerte SNMPv3 à la norme AES 192 bits ou AES 256 bits.

Avant de commencer

Chaque hôte géré qui reçoit des alertes SNMPv3 de haut niveau requiert l'extension JCE non restreinte. Si vous utilisez des algorithmes cryptographiques avancés pour la communication SNMP, vous devez mettre à jour l'extension de cryptographie existante sur votre hôte géré avec une extension JCE non restreinte.

Procédure

1. Sous SSH, connectez-vous à votre console QRadar.
2. Pour vérifier la version Java sur la console, entrez la commande suivante : `java -version`.
   Le fichier JCE doit correspondre à la version Java installée sur la console.
3. Téléchargez la dernière version de Java Cryptography Extension depuis le site Web d'IBM.
   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk
4. Effectuez un transfert sécurisé (SCP) des fichiers `local.policy.jar` et `US_export_policy.jar` vers le répertoire suivant de la console : `/opt/ibm/java-[version]/jre/lib/security/`.
5. Facultatif. Les déploiements répartis requièrent que les administrateurs copient les fichiers `local.policy.jar` et `US_export_policy.jar` depuis le dispositif de console vers l'hôte géré.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

2 Scanner AXIS

Vous pouvez importer les données de vulnérabilité à partir depuis un scanner qui produit des données au format AXIS (Asset Export Information Source). Axis est un format de données XML conçu spécifiquement pour compatibilité d'actifs et de vulnérabilités avec des produits IBM Security QRadar.

AXIS est un format standard pour l'importation des résultats d'analyse des données de vulnérabilité. Les données de vulnérabilité des scanners AXIS doivent se conformer au schéma de format AXIS pour pouvoir être importées. Pour intégrer un scanner AXIS àQRadar, des fichiers résultat XML doivent être disponibles sur un *serveur distant* ou un scanner qui prend en charge la communication SFTP ou SMB. Un serveur distant est un système ou un dispositif tiers qui peut héberger les résultats d'analyse XML.

Ajout d'une analyse de vulnérabilité AXIS

Ajoutez une configuration de scanner AXIS afin de collecter des rapports spécifiques ou de lancer des analyses sur le scanner distant.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les paramètres de scanner AXIS lorsque vous sélectionnez SFTP comme méthode d'importation :

Tableau 1. Scanner AXIS - Propriétés SFTP

Paramètre	Description
Remote Hostname	Adresse IP ou nom d'hôte du serveur qui a les fichiers de résultats d'analyse.
Login Username	Nom d'utilisateur que QRadar utilise pour la connexion au serveur.
Enable Key Authentication	Indique que QRadar s'authentifie avec un fichier d'authentification par clé.
Remote directory	Emplacement des fichiers de résultat d'analyse.
Private Key File	Chemin d'accès complet au fichier qui contient la clé privée. Si un fichier de clés n'existe pas, vous devez créer le fichier `vis.ssh.key`.
File Name Pattern	Expression régulière (regex) requise pour filtrer la liste de fichiers spécifiée dans le *répertoire distant*. Le canevas `.*\.xml` importe tous les fichiers XML du répertoire distant.

Le tableau suivant décrit les paramètres de scanner AXIS lorsque vous sélectionnez *SMB Share* comme méthode d'importation :

Tableau 2. Scanner AXIS - Propriétés SMB Share

Paramètre	Description
Hostname	Adresse IP ou nom d'hôte de SMB Share.
Login Username	Nom d'utilisateur que QRadar utilise pour la connexion à SMB Share.
Domain	Domaine qui est utilisé pour la connexion à SMB Share.

Tableau 2. Scanner AXIS - Propriétés SMB Share (suite)

Paramètre	Description
SMB Folder Path	Chemin d'accès complet au partage depuis a racine de l'hôte SMB. Utilisez les barres obliques, par exemple `/share/logs/`.
File Name Pattern	Expression régulière (regex) requise pour filtrer la liste de fichiers spécifiée dans le répertoire distant. Le canevas `.*\.xml` importe tous les fichiers xml dans le répertoire distant.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant le scanner AXIS.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner.
6. Dans la liste **Type**, sélectionnez **Axis Scanner**.
7. Depuis la liste **Import Method**, sélectionnez **SFTP** ou **SMB Share**.
8. Configurez les paramètres ci-après.
9. Configurez une plage CIDR pour le scanner.
10. Cliquez sur **Sauvegarder**.
11. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Pour plus d'informations sur la création d'une planification d'analyse, voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

3 Présentation du scanner Beyond Security Automatic Vulnerability Detection System

L'évaluation de la vulnérabilité désigne l'évaluation des actifs du réseau afin d'identifier et de hiérarchiser des failles de sécurité potentielles. Les produits QRadar qui prennent en charge l'évaluation de la vulnérabilité peuvent importer des données de vulnérabilité depuis des scanners afin d'identifier des profils de vulnérabilité sur les actifs.

Les profils d'évaluation de la vulnérabilité utilisent des données d'événement corrélées, l'activité du réseau, ainsi que des changements de comportement afin de déterminer le niveau de menace pour les éléments métier essentiels de votre réseau. Une fois que les scanners externes génèrent des données d'analyse, QRadar peut extraire des données de vulnérabilité d'après une planification d'analyse.

Pour configurer un scanner Beyond Security AVDS, voir «Ajout d'un scanner de vulnérabilité Beyond Security AVDS».

Ajout d'un scanner de vulnérabilité Beyond Security AVDS

Les dispositifs Beyond Security AVDS (Automated Vulnerability Detection System) créent des données de vulnérabilité au format AXIS (Asset Export Information Source). Les fichiers au format AXIS peuvent être importés dans des fichiers XML qui peuvent être importés.

Pourquoi et quand exécuter cette tâche

Pour intégrer correctement des vulnérabilités Beyond Security AVDS à QRadar, vous devez configurer votre dispositif Beyond Security AVDS pour publier les données de vulnérabilité dans un fichier de résultats XML au format AXIS. Les données de vulnérabilités XML doivent être publiées sur un serveur distant accessible via le protocole SFTP (Secure File Transfer Protocol). Le terme serveur distant fait référence à un système, à un hôte tiers ou à un emplacement de stockage réseau pouvant héberger les fichiers XML de résultat d'analyse.

Les résultats XML les plus récents contenant des vulnérabilités Beyond Security AVDS sont importés lorsqu'une planification d'analyse est lancée. Les planifications d'analyse déterminent la fréquence à laquelle des données de vulnérabilité générées par Beyond Security AVDS sont importées. Après que vous avez ajouté le dispositif Beyond Security AVDS à QRadar, créez une planification d'analyse pour importer les fichiers de résultat de l'analyse. Les vulnérabilités importées par la planification d'analyse mettent à jour l'onglet **Actifs** une fois que s'achève la planification d'analyse.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Beyond Security AVDS.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Beyond Security AVDS**.
7. Dans la zone **Remote Hostname**, entrez l'adresse IP ou le nom d'hôte du système qui contient les résultats d'analyse publiés de votre scanner Beyond Security AVDS.
8. Choisissez l'une des options d'authentification suivantes :

Option	Description
Login Username	Pour s'authentifier avec un nom d'utilisateur et un mot de passe, procédez comme suit : 1. Dans la zone **Login Username**, entrez un nom d'utilisateur autorisé à extraire les résultats de l'analyse depuis l'hôte distant. 2. Dans la zone **Login Password**, entrez le mot de passe associé au nom d'utilisateur.
Enable Key Authorization	Pour s'authentifier avec un fichier d'authentification basé clés, procédez comme suit : 1. Cochez la case **Enable Key Authentication**. 2. Dans la zone **Private Key File**, entrez le chemin de répertoire du fichier de clés. Par défaut, il s'agit de `/opt/qradar/conf/vis.ssh.key`. Si un fichier de clés n'existe pas, vous devez créer le fichier vis.ssh.key.

9. Dans la zone **Remote Directory**, entrez l'emplacement du répertoire des fichiers de résultat de l'analyse.
10. Dans la zone **File Name Pattern**, entrez l'expression régulière (regex) pour filtrer la liste des fichiers spécifiés dans le répertoire distant. Tous les fichiers correspondants sont inclus dans le traitement.

    La valeur par défaut est : `.*\.xml`. Le canevas `.*\.xml` importe tous les fichiers xml dans le répertoire distant.
11. Dans la zone **Max Reports Age (Days)**, entrez l'âge maximal du fichier de résultats d'analyse. Les fichiers plus anciens que le nombre de jours et l'horodatage spécifiés dans le fichier de rapport sont exclus lorsque l'analyse planifiée est lancée. La valeur par défaut est 7 jours.
12. Pour configurer l'option **Ignore Duplicates**, procédez comme suit.
    - Cochez cette case pour effectuer le suivi des fichiers déjà traités par une planification d'analyse. Cette option évite de traiter une seconde fois un fichier de résultats d'analyse.
    - Décochez cette case pour importer les résultats d'analyse de vulnérabilité chaque fois qu'une planification d'analyse est lancée. Cette option peut entraîner l'association de vulnérabilités multiples à un actif.

    Si un fichier de résultats n'est pas analysé dans les 10 jours, il est retiré de la liste de suivi et est traité au lancement suivi de la planification d'analyse.
13. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
14. Cliquez sur **Sauvegarder**.
15. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

4 Scanners Digital Defense Inc AVS

Vous pouvez ajouter un scanner AVS Digital Defense Inc à votre déploiement IBM Security QRadar.

Avant de commencer

Avant d'ajouter ce scanner, un certificat serveur est requis pour la prise en charge des connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : .crt, .cert ou .der. Pour copier un certificat vers le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat vers le répertoire `/opt/qradar/conf/trusted_certificates` via SCP ou SFTP.
- Lancez SSH sur la console ou l'hôte géré et extrayez le certificat à l'aide de la commande suivante : `/opt/qradar/bin/getcert.sh <IP ou nom d'hôte> <port facultatif - 443 par défaut>`. Un certificat est alors téléchargé du nom d'hôte ou de l'IP spécifié, et placé dans le répertoire `/opt/qradar/conf/trusted_certificates` dans le format approprié.

Pourquoi et quand exécuter cette tâche

A chaque intervalle déterminé par une planification d'analyse, QRadar importe les résultats les plus récents contenant les vulnérabilités de Digital Defense Inc AVS. Pour activer la communication avec le scanner AVS Digital Defense Inc, QRadar utilise les informations de connexion que vous avez spécifiées lors de la configuration de l'unité.

La liste ci-après fournit de plus amples informations sur les paramètres du scanner AVS Digital Defense Inc.

Remote Hostname
Le nom d'hôte du serveur distant qui héberge le scanner Digital Defense Inc AVS.

Remote Port
Le numéro de port du serveur distant qui héberge le scanner Digital Defense Inc AVS.

Remote URL
L'URL du serveur distant qui héberge le scanner Digital Defense Inc AVS.

Client ID
L'ID client principal utilisé pour toute connexion au scanner Digital Defense Inc AVS.

Host Scope
Lorsqu'il est défini sur Internal, il récupère la vue active pour les hôtes internes du scanner AVS Digital Defense Inc. Lorsqu'il est défini sur External, il récupère la vue active du scanner AVS Digital Defense Inc.

Retrieve Data For Account
L'option **Default** indique que les données sont incluses uniquement à partir de l'ID client (**Client ID**) spécifié. Si vous souhaitez inclure des données à partir de l'ID client et de tous ses sous-comptes, sélectionnez **All Sub Accounts**. Si vous souhaitez spécifier un autre ID client unique, sélectionnez **Alternate Client ID**.

Correlation Method
Indique la méthode par laquelle les vulnérabilités sont corrélées.

- L'option **All Available** permet d'interroger le catalogue de vulnérabilités de Digital Defense Inc et de tenter de corréler les vulnérabilités trouvées dans toutes les références renvoyées pour une vulnérabilité spécifique. Les références peuvent inclure CVE, Bugtraq, le bulletin de

sécurité de Microsoft et OSVDB. De multiples références sont souvent corrélées à la même vulnérabilité. Néanmoins, celles-ci apportent plus de résultats et mettent plus longtemps à être traitées que l'option **CVE**.

- L'option **CVE** met en corrélation les vulnérabilités trouvées sur le CVE-ID uniquement.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Sources de données**.
3. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
4. Cliquez sur **Ajouter**.
5. Depuis la zone de liste **Type**, sélectionnez **Digital Defense Inc AVS**.
6. Configurez les paramètres ci-après.
7. Pour configurer les plages CIDR que ce scanner doit prendre en compte, entrez une plage CIDR ou cliquez sur **Parcourir** pour en sélectionner une dans la liste des réseaux.
8. Cliquez sur **Ajouter**.
9. Cliquez sur **Sauvegarder**.
10. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Après avoir ajouté votre scanner AVS Digital Defense Inc, vous pouvez également ajouter une planification d'analyse pour récupérer les informations relatives aux vulnérabilités.

5 Présentation du scanner eEye

QRadar peut collecter des données de vulnérabilité depuis la console eEye REM Security Management ou des scanners eEye Retina CS.

Les options de protocole suivantes sont disponibles pour la collecte d'informations de vulnérabilité depuis des scanners eEye :

- Ajout d'un scanner eEye à protocole SNMP. Voir «Ajout d'un scanner SNMP REM eEye».
- Ajout d'un scanner eEye à protocole JDBC. Voir «Ajout d'une analyse JDBC REM eEye», à la page 10

Tâches associées:

«Installation du module Java Cryptography Extension Unlimited», à la page 1
Le module Java Cryptography Extension (JCE) est une infrastructure Java qui est requise pour déchiffrer des algorithmes de cryptographie avancés pour messages d'alerte SNMPv3 à la norme AES 192 bits ou AES 256 bits.

Ajout d'un scanner SNMP REM eEye

Vous pouvez ajouter un scanner pour collecter des données de vulnérabilité via SNMP auprès de scanners eEye REM ou CS Retina.

Avant de commencer

Pour utiliser des identificateurs et des descriptions CVE, vous devez copier le fichier `audits.xml` depuis votre scanner eEye REM vers l'hôte géré chargé de l'écoute des données SNMP. Si votre hôte géré réside dans un déploiement réparti, vous devez d'abord copier le fichier `audits.xml` vers la console, puis le transférer via SSH vers l'emplacement `/opt/qradar/conf/audits.xml` sur l'hôte géré. L'emplacement par défaut du fichier `audits.xml` sur le scanner eEye est `%ProgramFiles(x86)%\eEye Digital Security\Retina CS\Applications\RetinaManager\Database\audits.xml`.

Pour recevoir les toutes dernières informations CVE, mettez régulièrement à jour QRadar avec le fichier `audits.xml` le plus récent.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre serveur SecureScout.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **eEye REM Scanner**.
7. Dans la liste **Import Type**, sélectionnez **SNMP**.
8. Dans la zone **Base Directory**, entrez un emplacement de répertoire où stocker les fichiers temporaires contenant les données d'analyse eEye REM. Le répertoire par défaut est `/store/tmp/vis/eEye/`.
9. Dans la zone **Cache Size**, entrez le nombre de transactions à conserver en cache avant que les données SNMP ne soient consignées dans le fichier temporaire. La valeur par défaut est de 40. La valeur par défaut est de 40 transactions.
10. Dans la zone **Retention Period**, entrez la période, en jours, pendant laquelle le système doit stocker les informations d'analyse. Si une planification d'analyse n'a pas importé de données avant l'expiration de la période de rétention, les informations d'analyse sont supprimées du cache.

11. Cochez la case **Use Vulnerability Data** pour corréler les vulnérabilités eEye aux identificateurs et aux informations de description CVE (Common Vulnerabilities and Exposures). .
12. Dans la zone **Vulnerability Data File**, entrez le chemin de répertoire du fichier eEye `audits.xml`.
13. Dans la zone **Listen Port**, entrez le numéro de port utilisé pour surveillance des informations de vulnérabilité SNMP entrantes en provenance du scanner eEye REM. Par défaut, il s'agit du port 1162.
14. Dans la zone **Source Host**, entrez l'adresse IP du scanner eEye.
15. Dans la liste **SNMP Version**, sélectionnez la version du protocole SNMP. Par défaut, il s'agit du protocole SNMPv2.
16. Dans la zone **Community String**, entrez la chaîne de communauté SNMP pour le protocole SNMPv2, par exemple `Public`.
17. Dans la liste **Authentication Protocol**, sélectionnez l'algorithme d'authentification des alertes SNMPv3.
18. Dans la zone **Authentication Password**, entrez le mot de passe à utiliser pour authentification de communication SNMPv3. Le mot de passe doit être composé au minimum de 8 caractères.
19. Dans la liste **Encryption Protocol**, sélectionnez l'algorithme de (dé)chiffrement SNMPv3.
20. Dans la zone **Encryption Password**, entrez le mot de passe permettant de déchiffrer les alertes SNMPv3.
21. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
22. Cliquez sur **Sauvegarder**.
23. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Sélectionnez l'une des options suivantes :

- Si vous n'utilisez pas SNMPv3 ou utilisez un chiffrement SNMP de bas niveau, vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.
- Si vote configuration SNMPv3 utilise un chiffrement AES192 ou AES256, vous devez installer l'extension de chiffrement Java non restreinte sur chaque console ou hôte géré recevant des alertes SNMPv3. Voir «Installation du module Java Cryptography Extension Unlimited», à la page 1.

Ajout d'une analyse JDBC REM eEye

Vous pouvez ajouter un scanner pour collecter des données de vulnérabilité via JDBC auprès de scanners eEye REM ou CS Retina.

Avant de commencer

Avant de configurer QRadar pour interrogation de données de vulnérabilité, il est conseillé de créer un compte utilisateur de la base de données et un mot de passe pour QRadar. Si vous affectez à ce compte utilisateur un accès en lecture seule à la base de données RetinaCSDatabase, vous pouvez restreindre l'accès à la base de données contenant les vulnérabilités eEye. Le protocole JDBC permet à QRadar de se connecter et de rechercher des événements dans la base de données MSDE. Assurez-vous qu'aucune règle de pare-feu ne bloque la communication entre le scanner eEye et la console ou l'hôte géré chargé de l'interrogation avec le protocole JDBC. Si vous utilisez des instances de base de données, vous devez vérifier que le port 1433 est disponible afin que SQL Server Browser Service puisse résoudre le nom de l'instance.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant le scanner eEye.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré du déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **eEye REM Scanner**.
7. Dans la liste **Import Type**, sélectionnez **JDBC**.
8. Dans la zone **Hostname**, entrez l'adresse IP ou le nom d'hôte de la base de données eEye.
9. Dans la zone **Port**, entrez `1433`.
10. Facultatif. Dans la zone **Database Instance**, entrez l'instance de base de données pour la base de données eEye.

    Si une instance de base de données n'est pas utilisée, laissez cette zone vide.
11. Dans la zone **Username**, entrez le nom d'utilisateur requis pour interroger la base de données eEye.
12. Dans la zone **Password**, entrez le mot de passe requis pour interroger la base de données eEye.
13. Dans la zone **Domain**, entrez le nom de domaine, s'il est nécessaire, pour connexion à la base de données eEye.

    Si la base de données est configurée pour Windows et à l'intérieur d'un domaine, vous devez spécifier le nom de domaine.
14. Dans la zone **Database Name**, entrez `RetinaCSDatabase` comme nom de la base de données.
15. Cochez la case **Use Named Pipe Communication** si des canaux de communication nommés sont requis pour communiquer avec la base de données eEye. Par défaut, cette case est désélectionnée.
16. Cochez la case **Use NTLMv2** si le scanner eEye utilise NTLMv2 comme protocole d'authentification. Par défaut, cette case est désélectionnée.

    La case Use NTLMv2 force les connexions MSDE à utiliser le protocole NTLMv2 lors de la communication avec des serveurs SQL exigeant une authentification NTLMv2. La sélection de cette case n'a pas d'effet sur les connexions MSDE à des serveurs SQL qui ne requièrent pas une authentification NTLMv2.
17. Pour configurer une plage CIDR pour le scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
18. Cliquez sur **Sauvegarder**.
19. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

6 Présentation du scanner IBM AppScan Enterprise

QRadar extrait les rapports AppScan Enterprise avec le service Web REST (Representational State Transfer) pour importer les données de vulnérabilité et générer des infractions pour votre équipe de sécurité. AppScan Enterprise

Vous pouvez importer des résultats d'analyse provenant des données de rapport IBM Security AppScan Enterprise et disposer ainsi d'un environnement de sécurité centralisé pour une analyse d'application et une génération de rapports de conformité à la sécurité avancées. Vous pouvez importer des résultats d'analyse IBM Security AppScan Enterprise afin de collecter des informations sur des actifs de votre déploiement concernant la vulnérabilité aux logiciels malveillants, applications Web et services Web.

Pour intégrer AppScan Enterprise à IBM Security QRadar, vous devez effectuer les tâches suivantes :

1. Générer des rapports d'analyse dans IBM AppScan Enterprise.

   Les informations de configuration des rapports se trouvent dans votre documentation IBM AppScan Enterprise.
2. Configurer AppScan Enterprise pour permettre à QRadar d'accéder aux données de rapport.
3. Configurer votre scanner AppScan Enterprise dans QRadar.
4. Créer un planning dans QRadar pour importer les résultats AppScan Enterprise.

Pour configurer IBM AppScan Enterprise pour disposer de l'accès aux données de rapport, votre administrateur AppScan doit déterminer quels utilisateurs disposent des droits pour publier des rapports dans QRadar. Lorsque les utilisateurs AppScan Enterprise ont configuré les rapports, les rapports générés par AppScan Enterprise peuvent être publiés dans QRadar et ainsi être disponibles pour le téléchargement.

Pour configurer AppScan Enterprise pour permettre d'accéder aux données de rapport d'analyse, voir «Création d'un type d'utilisateur personnalisé pour IBM AppScan Enterprise».

Création d'un type d'utilisateur personnalisé pour IBM AppScan Enterprise

Vous pouvez créer des types d'utilisateur personnalisés pour affecter à des administrateurs des droits d'accès à des tâches d'administration spécifiques et limitées.

Procédure

1. Connectez-vous à votre dispositif IBM AppScan Enterprise.
2. Cliquez sur l'onglet **Administration**.
3. Dans la page Types d'utilisateur, cliquez sur **Créer**.
4. Sélectionnez toutes les autorisations utilisateur suivantes :
   - **Configurer l'intégration QRadar** - Cochez cette case pour permettre aux utilisateurs d'accéder aux options d'intégration de QRadar pour AppScan Enterprise.
   - **Publier dans QRadar** - Cochez cette case pour permettre à QRadar d'accéder aux données de rapports d'analyse publiés.
   - **Compte de service QRadar** - Cochez cette case pour ajouter un accès à l'API REST au compte utilisateur. Cette autorisation n'accorde pas un accès à l'interface utilisateur.
5. Cliquez sur **Sauvegarder**.

Que faire ensuite

Vous pouvez à présent activer les autorisations d'intégration. Voir «Activation de l'intégration avec IBM AppScan Enterprise»

Activation de l'intégration avec IBM AppScan Enterprise

IBM AppScan Enterprise doit être configuré pour activer l'intégration avec QRadar.

Avant de commencer

Pour exécuter cette procédure, vous devez être connecté avec un type d'utilisateur personnalisé.

Procédure

1. Cliquez sur l'onglet **Administration**.
2. Dans le menu **Navigation**, sélectionnez **Network Security Systems**.
3. Dans la sous-fenêtre QRadar Integration Setting, cliquez sur **Edit**.
4. Cochez la case **Enable QRadar Integration**. Tous les rapports publiés précédemment dans QRadar sont affichés. Si aucun des rapports affichés n'est plus requis, vous pouvez les retirer de la liste. Lorsque vous publiez d'autres rapports dans QRadar, ces rapports s'affichent dans la liste.

Que faire ensuite

Vous êtes maintenant sur le point de configurer le mappage de déploiement d'application dans AppScan Enterprise. Voir «Création d'une mappe de déploiement d'application dans IBM AppScan Enterprise».

Création d'une mappe de déploiement d'application dans IBM AppScan Enterprise

La mappe de déploiement d'application permet à AppScan Enterprise de déterminer les emplacements qui hébergent l'application dans votre environnement de production.

Pourquoi et quand exécuter cette tâche

Dès que les vulnérabilités sont reconnues, AppScan Enterprise connaît les emplacements des hôtes et les adresses IP concernés par la vulnérabilité. Si une application est déployée sur plusieurs hôtes, cela signifie qu'AppScan Enterprise génère une vulnérabilité pour chaque hôte dans les résultats d'analyse.

Procédure

1. Cliquez sur l'onglet **Administration**.
2. Dans le menu de navigation, sélectionnez **Systèmes de sécurité réseau**.
3. Dans la sous-fenêtre Paramètres d'intégration QRadar, cliquez sur **Editer**.
4. Dans la zone **Emplacement de test de l'application (hôte ou modèle)**, entrez l'emplacement de test de votre application.
5. Dans la zone **Emplacement de production de l'application (hôte)**, entrez l'adresse IP de votre environnement de production. Pour ajouter des informations de vulnérabilité à IBM Security QRadar, votre mappage de déploiement d'application doit inclure une adresse IP. Si l'adresse IP n'est pas disponible dans les résultats d'analyse AppScan Enterprise, les données de vulnérabilité sans adresse IP sont exclues de QRadar.
6. Cliquez sur **Ajouter**.
7. Répétez cette procédure pour mapper d'autres environnements de production dans AppScan Enterprise.

8. Cliquez sur **Terminé**.

Que faire ensuite

Vous pouvez à présent publier les rapports complétés. Voir «Publication de rapports complétés dans IBM AppScan Enterprise».

Publication de rapports complétés dans IBM AppScan Enterprise

Les rapports de vulnérabilité terminés qui ont été générés par AppScan Enterprise doivent être rendus accessibles à QRadar en publiant le rapport.

Procédure

1. Cliquez sur l'onglet **Travaux & rapports**.
2. Accédez au rapport de sécurité que vous souhaitez rendre disponible sur IBM Security QRadar.
3. Dans la barre de menus de n'importe quel rapport de sécurité, sélectionnez **Publier** > **Accorder** pour accorder à QRadar l'accès aux rapports.
4. Cliquez sur **Sauvegarder**.

Que faire ensuite

Vous pouvez à présent activer les autorisations d'intégration. Voir «Ajout d'un scanner de vulnérabilité IBM AppScan Enterprise».

Ajout d'un scanner de vulnérabilité IBM AppScan Enterprise

Vous pouvez ajouter un scanner pour définir les rapports d'analyse collectés dans IBM Security AppScan par QRadar.

Avant de commencer

Si votre installation AppScan est configurée pour utiliser HTTPS, un certificat serveur est requis. IBM Security QRadar prend en charge les certificats possédant les extensions de fichier suivantes : .crt, .cert ou .der. Pour copier un certificat vers le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat vers le répertoire `/opt/qradar/conf/trusted_certificates` via SCP ou SFTP.
- Lancez SSH sur la console ou l'hôte géré et extrayez le certificat à l'aide de la commande suivante : `/opt/qradar/bin/getcert.sh <IP ou nom d'hôte> <port facultatif - 443 par défaut>`. Un certificat est alors téléchargé du nom d'hôte ou de l'IP spécifié, et placé dans le répertoire `/opt/qradar/conf/trusted_certificates` dans le format approprié.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter plusieurs scanners IBM AppScan à QRadar, chacun avec sa propre configuration. Ces différentes configurations permettent à QRadar d'importer des données AppScan contenant des résultats spécifiques. La planification d'analyse détermine la fréquence d'importation des résultats d'analyse depuis le service Web REST dans IBM AppScan Enterprise.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.

4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner IBM AppScan Enterprise.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **IBM AppScan Scanner**.
7. Dans la zone **ASE Instance Base URL**, entrez l'URL de base complète de l'instance AppScan Enterprise. HTTP et HTTPS sont pris en charge dans l'adresse URL.

   Exemple : API XML - `http://nomhôtease/ase`

   Exemple : JSON API - `http://nomhôtease/ase/api`
8. Dans la liste répertoriant les **types d'API**, sélectionnez l'une des options suivantes :
   - **XML (Before v9.02)** - Si votre version d'AppScan Enterprise est antérieure à la version 9.02, sélectionnez cette option. Ce type d'API utilise le service Web REST XML AppScan.
   - **JSON (v9.0.2 and later)** - Si votre version d'AppScan Enterprise correspond à la version 9.02 ou suivante, sélectionnez cette option. Ce type d'API utilise le service Web REST JSON AppScan.
9. Si vous avez sélectionné **XML (Before v9.02)** comme **type d'API**, sélectionnez l'une des options suivantes dans la liste **Type d'authentification** :
   - **Windows Authentication (AppScan Enterprise version 9.0 and previous)** - Sélectionnez cette option pour utiliser la fonction d'authentification Windows avec le service Web REST.
   - **AppScan Enterprise Authentication** - Sélectionnez cette option pour utiliser l'authentification AppScan Enterprise avec le service Web REST.
10. Dans la zone **Username**, entrez le nom d'utilisateur requis pour extraire les résultats d'analyse de AppScan Enterprise.
11. Dans la zone **Password**, entrez le mot de passe requis pour extraire les résultats d'analyse de AppScan Enterprise.
12. Dans la zone **Report Name Pattern**, entrez une expression régulière (regex) pour filtrer la liste des rapports de vulnérabilité disponibles dans AppScan Enterprise. Par défaut, la zone **Report Name Pattern** contient `.*` comme canevas d'expression régulière. Le canevas `.*` importe tous les rapports d'analyse publiés dans QRadar. Tous les fichiers correspondants au canevas sont traités par QRadar. Vous pouvez spécifier un groupe de rapports de vulnérabilité ou un rapport individuel à l'aide d'un canevas d'expression régulière.
13. Configurez une plage CIDR pour le scanner :
    a. Entrez la plage CIDR pour le scanner ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
14. Cliquez sur **Sauvegarder**.
15. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse pour IBM AppScan Enterprise. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83

7 Présentation du scanner IBM Guardium

Les dispositifs IBM InfoSphere Guardium sont capables d'exporter des informations de vulnérabilité de base de données pouvant être cruciales pour la protection des données client.

Les processus de vérification d'IBM Guardium exportent les résultats des tests qui ont échoué aux tests du Common Vulnerability and Exposures (CVE) générés au moment du démarrage des tests d'évaluation de la sécurité sur le dispositif IBM Guardium. Les données de vulnérabilité d'IBM Guardium doivent être exportées vers un serveur distant ou un serveur de transfert au format Security Content Automation Protocol (SCAP). IBM Security QRadar peut ensuite récupérer les résultats de l'analyse à partir du serveur distant qui stocke la vulnérabilité via SFTP.

IBM Guardium n'exporte des vulnérabilités que depuis des bases de données contenant des résultats de test CVE signalant des échecs. Si aucun test CVE n'a échoué, IBM Guardium peut ne pas exporter de fichier à la fin de l'évaluation de la sécurité. Pour plus d'informations sur la configuration de tests d'évaluation de la sécurité et de création d'un processus d'audit pour exporter les vulnérabilités au format SCAP, consultez votre documentation IBM InfoSphere Guardium.

Une fois que vous avez configuré votre dispositif IBM Guardium, vous êtes prêt à configurer QRadar pour importer les résultats à partir du serveur distant hébergeant les données de vulnérabilité. Vous devez ajouter un scanner IBM Guardium à QRadar et configurer le scanner pour récupérer des données à partir de votre serveur distant. Les vulnérabilités les plus récentes sont importées par QRadar lorsque vous créez une planification d'analyse. Les planifications d'analyse vous permettent de déterminer la fréquence à laquelle QRadar demande des données à partir du serveur distant qui héberge vos données de vulnérabilité IBM Guardium.

Présentation de l'intégration d'IBM InfoSphere Guardium et QRadar.

1. Sur votre dispositif IBM InfoSphere Guardium, créez un fichier SCAP avec vos informations de vulnérabilité. Consultez votre documentation IBM InfoSphere Guardium.
2. Sur votre console QRadar, ajoutez un scanner IBM Guardium. Voir «Ajout d'un scanner de vulnérabilité IBM Guardium»
3. Sur votre console QRadar, créez une planification d'analyse pour importer vos données de résultats d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83

Ajout d'un scanner de vulnérabilité IBM Guardium

L'ajout d'un scanner permet à QRadar de collecter des fichiers de vulnérabilité SCAP auprès d'IBM InfoSphere Guardium.

Pourquoi et quand exécuter cette tâche

Les administrateurs peuvent ajouter plusieurs scanners IBM Guardium, chacun avec sa propre configuration, à IBM Security QRadar. Ces différentes configurations permettent à QRadar d'importer des données de vulnérabilité contenant des résultats spécifiques. La planification d'analyse détermine la fréquence à laquelle les résultats d'analyse SCAP sont importés d'IBM InfoSphere Guardium.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner IBM Guardium.

5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **IBM Guardium SCAP Scanner**.
7. Choisissez l'une des options d'authentification suivantes :

Option	Description
Login Username	Pour s'authentifier avec un nom d'utilisateur et un mot de passe, procédez comme suit : 1. Dans la zone **Login Username**, entrez un nom d'utilisateur autorisé à extraire les résultats de l'analyse depuis l'hôte distant. 2. Dans la zone **Login Password**, entrez le mot de passe associé au nom d'utilisateur.
Enable Key Authorization	Pour s'authentifier avec un fichier d'authentification basé clés, procédez comme suit : 1. Cochez la case **Enable Key Authentication**. 2. Dans la zone **Private Key File**, entrez le chemin de répertoire du fichier de clés. Le répertoire par défaut du fichier de clés est : `/opt/qradar/conf/vis.ssh`. Si un fichier de clés n'existe pas, vous devez créer le fichier vis.ssh.

8. Dans la zone **Remote Directory**, entrez l'emplacement du répertoire des fichiers de résultat de l'analyse.
9. Dans la zone **File Name Pattern**, entrez l'expression régulière (regex) requise pour filtrer la liste des fichiers de vulnérabilité SCAP spécifiée dans la zone **Remote Directory**. Tous les fichiers correspondants sont inclus dans le traitement. Par défaut, la zone Report Name Pattern contient `.*\.xml` comme canevas d'expression régulière. Le canevas `.*\.xml` importe tous les fichiers xml dans le répertoire distant.
10. Dans la zone **Max Reports Age (Days)**, entrez l'âge maximal du fichier de résultats d'analyse. Les fichiers plus anciens que le nombre de jours et l'horodatage spécifiés dans le fichier de rapport sont exclus lorsque l'analyse planifiée est lancée. La valeur par défaut est 7 jours.
11. Pour configurer l'option **Ignore Duplicates**, procédez comme suit.
    - Cochez cette case pour suivi des fichiers déjà traités par une planification d'analyse. Cette option évite de traiter une seconde fois un fichier de résultats d'analyse.
    - Décochez cette case pour importer les résultats d'analyse de vulnérabilité chaque fois qu'une planification d'analyse est lancée. Cette option peut entraîner l'association de vulnérabilités multiples à un actif.

    Si un fichier de résultats n'est pas analysé dans les 10 jours, il est retiré de la liste de suivi et est traité au lancement suivi de la planification d'analyse.
12. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
13. Cliquez sur **Sauvegarder**.
14. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse pour IBM InfoSphere Guardium. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83

Configuration de Guardium pour générer un rapport au format AXIS

Vous pouvez intégrer IBM InfoSphere Guardium à QRadar à l'aide du scanner AXIS (Asset Export Information Source). Toutefois, vous devez vous assurer que les rapports d'évaluation des vulnérabilités Guardium sont exportés au format AXIS.

Procédure

1. Connectez-vous à IBM InfoSphere Guardium.
2. Cliquez sur **Tools**.
3. Dans la page **Tools**, sélectionnez **Security Assessment Builder**.
4. Cliquez sur **New** pour créer une évaluation.
5. Dans la page Security Assessment Builder, entrez des valeurs pour **Description, Period From**, **To**, **Client Ip** (facultatif) et **Server Ip** (facultatif).
6. Cliquez sur **Add Datasource** et ajoutez les sources de données pour lesquelles vous souhaitez exécuter les tests d'évaluation.
7. Dans la page Datasource Finder, sélectionnez une source de données et cliquez sur **Add**.
8. Cliquez sur **Apply** pour sauvegarder la source de données que vous venez d'ajouter.
9. Ajoutez des tests à l'évaluation en cliquant sur **Configure Test**.
10. Sélectionnez des tests dans un inventaire de tests disponibles et cliquez sur **Add Selections** pour les ajouter à l'évaluation.
11. Cliquez sur **Return**.
12. Pour exécuter l'évaluation, cliquez sur **Run Once Now**.
13. Dans l'écran Assessment Results, cliquez sur **Create AXIS Results** pour générer un fichier de sortie au format AXIS.

8 Présentation du scanner IBM SiteProtector

Le module de scanner IBM SiteProtector pour QRadar accède aux données de vulnérabilité des scanners IBM SiteProtector via des requêtes JDBC (Java Database Connectivity).

Le scanner IBM SiteProtector récupère des données depuis la table RealSecureDB et s'enquiert de nouvelles vulnérabilités chaque fois qu'une nouvelle planification d'analyse est lancée. La zone **Compare** permet à la requête d'extraire de la table RealSecureDB les nouvelles vulnérabilités pour garantir que des doublons de vulnérabilités ne soient pas importés. Lors de la configuration du scanner IBM SiteProtector, l'administrateur peut créer un compte utilisateur SiteProtector spécifiquement destiné aux interrogations de données de vulnérabilité. Après que le compte utilisateur est créé, l'administrateur peut vérifier qu'aucun pare-feu ne rejette les requêtes sur le port configuré pour interroger la base de données.

Pour configurer un scanner IBM SiteProtector, voir «Ajout d'un scanner de vulnérabilité IBM SiteProtector».

Ajout d'un scanner de vulnérabilité IBM SiteProtector

QRadar peut interroger des dispositifs IBM InfoSphere SiteProtector quant à l'existence de données de vulnérabilité via JDBC.

Pourquoi et quand exécuter cette tâche

Les administrateurs peuvent ajouter plusieurs scanners IBM SiteProtector, chacun avec sa propre configuration, à IBM Security QRadar. Les configurations multiples permettent à QRadar d'interroger SiteProtector et de n'importer que les résultats concernant une plage CIDR spécifique. La planification d'analyse détermine la fréquence d'interrogation de la base de données sur le scanner SiteProtector quant à l'existence de données de vulnérabilité.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant le scanner IBM SiteProtector.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré du déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **IBM SiteProtector Scanner**.
7. Dans la zone **Hostname**, entrez l'adresse IP ou le nom d'hôte IBM SiteProtector contenant les vulnérabilités à importer.
8. Dans la zone **Port**, entrez `1433` pour le port de la base de données IBM SiteProtector.
9. Dans la zone **Username**, entrez le nom d'utilisateur requis pour interroger la base de données IBM SiteProtector.
10. Dans la zone **Password**, entrez le mot de passe requis pour interroger la base de données IBM SiteProtector.
11. Dans la zone **Domain**, entrez le nom de domaine, s'il est requis, pour connexion à la base de données IBM SiteProtector.

    Si la base de données est configurée pour Windows et à l'intérieur d'un domaine, vous devez spécifier le nom de domaine.
12. Dans la zone **Database Name**, entrez `RealSecureDB` comme nom de la base de données.

13. Dans la zone **Database Instance**, entrez l'instance de base de données pour la base de données IBM SiteProtector. Si vous n'utilisez pas une instance de base de données, vous pouvez laisser cette zone vide.
14. Cochez la case **Use Named Pipe Communication** si des canaux de communication nommés sont requis pour communiquer avec la base de données IBM SiteProtector. Si vous utilisez l'authentification SQL, désactivez Named Pipe Communication. Par défaut, cette case est désélectionnée.
15. Cochez la case **Use NTLMv2** si IBM SiteProtector utilise NTLMv2 comme protocole d'authentification. Par défaut, cette case est désélectionnée.

    La case Use NTLMv2 force les connexions MSDE à utiliser le protocole NTLMv2 lors de la communication avec des serveurs SQL exigeant une authentification NTLMv2. La sélection de cette case n'a pas d'effet sur les connexions MSDE à des serveurs SQL qui ne requièrent pas une authentification NTLMv2.
16. Pour configurer une plage CIDR pour le scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
17. Cliquez sur **Sauvegarder**.
18. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83

9 Présentation du scanner IBM BigFix

Le module de scanner IBM BigFix accède aux données de vulnérabilité d'IBM BigFix en utilisant l'API SOAP installée avec l'application Web Reports.

Pour extraire les données de vulnérabilité d'BigFix for IBM Security QRadar, l'application Web Reports d'BigFix est nécessaire. Les administrateurs créent un utilisateur dans IBM BigFix que QRadar utilise lorsque le système collecte des vulnérabilités.

QRadar est compatible avec IBM BigFix pour les versions 8.2.x à 9.5.2.

Ajout d'un scanner de vulnérabilité IBM BigFix

QRadar accède aux données de vulnérabilité d'IBM BigFix via l'API SOAP installée avec l'application Web Reports.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter plusieurs scanners IBM BigFix dans QRadar. Chaque scanner requiert une configuration différente pour chaque plage CIDR que le scanner doit analyser.

Utilisez plusieurs configurations d'un seul scanner IBM BigFix pour créer des scanners spécifiques qui collectent des données de résultats spécifiques depuis des emplacements spécifiques ou les vulnérabilités de types spécifiques de systèmes d'exploitation.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners VA**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, tapez un nom pour identifier votre scanner IBM BigFix.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **IBM BigFix**.
7. Dans la zone **Hostname**, entrez l'adresse IP ou le nom d'hôte du scanner IBM BigFix contenant les vulnérabilités que vous souhaitez extraire avec l'API SOAP.
8. Dans la zone **Port**, entrez le numéro de port utilisé pour se connecter à IBM BigFix à l'aide de l'API SOAP. Par défaut, le port 80 est le numéro de port qui permet de communiquer avec IBM BigFix. Si vous utilisez HTTPS, vous devez mettre à jour cette zone avec le numéro de port HTTPS. Pour la plupart des configurations, utilisez le port 443.
9. Cochez la case **Use HTTPS** pour établir des connexions sécurisées à l'aide du protocole HTTPS.

   Si vous cochez cette case, le nom d'hôte ou l'adresse IP que vous spécifiez utilise HTTPS pour se connecter à votre système IBM BigFix. Si vous utilisez HTTPS, un certificat serveur est requis. Les certificats doivent être placés dans le répertoire `/opt/qradar/conf/trusted_certificates`. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : .crt, .cert ou .der. Vous pouvez utiliser SCP ou SFTP pour copier manuellement le certificat vers le répertoire `/opt/qradar/conf/trusted_certificates`. Vous pouvez également télécharger une copie du certificat directement de l'hôte QRadar. Pour cela, utilisez SSH pour connecter l'hôte et entrez la commande suivante : `/opt/qradar/bin/getcert.sh [`*`adresse_IP_ou_nom_hôte`*`]`. Vous pouvez également ajouter

un numéro de port à la commande. Le port par défaut est 443. Un certificat est alors téléchargé du nom d'hôte ou de l'IP spécifié et placé dans le répertoire `/opt/qradar/conf/trusted_certificates` dans le format approprié.

10. Dans la zone **Username**, tapez le nom d'utilisateur du compte qui a accès à IBM BigFix.
11. Dans la zone **Password**, tapez le mot de passe.
12. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit examiner ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
13. Cliquez sur **Sauvegarder**.
14. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Configuration des données d'identification de l'API SOAP pour le service de plug-in du serveur BES pour IBM BigFix sur un serveur Windows 32 bits

La configuration des données d'identification de l'API SOAP pour le serveur BES sur le serveur Windows 32 bits requiert l'exécution d'une série d'opérations.

Procédure

Pour configurer les données d'identification de l'API SOAP pour le serveur BES sur le serveur Windows 32 bits, procédez comme suit :

1. Entrez le nom d'utilisateur Web Reports pour <*SOAPUsername*> dans la clé de registre suivante : `[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\BESReports]SOAPUsername`.
2. Entrez le mot de passe chiffré Web Reports pour <*SOAPPassword*> dans la clé de registre suivante : `[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\BESReports]SOAPPassword`.
3. Entrez l'URL du serveur Web Reports <*WRHTTP*> dans la clé de registre suivante : `[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\BESReports]WRHTTP`
4. Entrez la valeur 2 pour la méthode de chiffrement des mots de passe pour <*SOAPPasswordIsEncryped*> dans la clé de registre suivante : `[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\BESReports] SOAPPasswordIsEncrypted`.

Pour plus d'informations sur la configuration des données d'identification de l'API SOAP, voir la note technique relative à l'installation et à la configuration du service de plug-in du serveur BigFix (http://www-01.ibm.com/support/docview.wss?uid=swg21506199).

Configuration des données d'identification de l'API SOAP pour le service de plug-in du serveur BES pour IBM BigFix sur un serveur Windows 64 bits

La configuration des données d'identification de l'API SOAP pour le serveur BES sur le serveur Windows 64 bits requiert l'exécution d'une série d'opérations.

Procédure

Pour configurer les données d'identification de l'API SOAP pour le serveur BES sur le serveur Windows 64 bits, procédez comme suit :

1. Entrez le nom d'utilisateur Web Reports pour <*SOAPUsername*> dans la clé de registre suivante : `[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports] SOAPUsername`.
2. Entrez le mot de passe chiffré Web Reports pour <*SOAPPassword*> dans la clé de registre suivante :

`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports] SOAPPassword`.

3. Entrez l'URL du serveur Web Reports <*WRHTTP*> dans la clé de registre suivante :
   `[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports]WRHTTP`.
4. Entrez la valeur 2 pour la méthode de chiffrement des mots de passe pour <*SOAPPasswordIsEncryped*> dans la clé de registre suivante :
   `[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports] SOAPPasswordIsEncrypted`.

Pour plus d'informations sur la configuration des données d'identification de l'API SOAP, voir la note technique relative à l'installation et à la configuration du service de plug-in du serveur BigFix (http://www-01.ibm.com/support/docview.wss?uid=swg21506199).

Configuration des données d'identification de l'API SOAP pour le service de plug-in du serveur BES pour IBM BigFix sur un serveur Linux

La configuration des données d'identification de l'API SOAP pour le serveur BES sur le serveur Linux requiert l'exécution d'un certain nombre d'opérations.

Procédure

Pour configurer les données d'identification de l'API SOAP pour le serveur BES sur le serveur Linux, procédez comme suit :

1. Ouvrez le fichier `/var/opt/BESServer/Applications/SOAPCredentials`.
2. Remplacez <*SOAPUsername*> par le nom d'utilisateur du compte qui a accès au fichier.
3. Remplacez <*SOAPPassword*> par le mot de passe du compte qui a accès au fichier.
4. Remplacez <*WRHTTP*> par l'URL Web Reports du compte qui a accès au fichier.

Pour plus d'informations sur la configuration des données d'identification de l'API SOAP, voir la note technique relative à l'installation et à la configuration du service de plug-in du serveur BigFix (http://www-01.ibm.com/support/docview.wss?uid=swg21506199).

10 Présentation du scanner IBM Tivoli Endpoint Manager

IBM Tivoli Endpoint Manager s'appelle désormais IBM BigFix.

Pour plus d'informations sur les scanners IBM BigFix, voir 9, «Présentation du scanner IBM BigFix», à la page 23

11 Présentation du scanner Juniper Profiler NSM

QRadar peut collecter des informations de vulnérabilité depuis la base de données PostgreSQL sur le scanner Juniper Profiler NSM en s'enquérant de ces données via JDBC.

La console Juniper Networks Netscreen Security Manager (NSM) collecte en mode passif des informations utiles sur les actifs de votre réseau via les détecteurs Juniper Networks IDP déployés. QRadar se connecte à la base de données Profiler stockée sur le serveur NSM pour récupérer ces enregistrements. Le serveur QRadar doit avoir accès à la base de données Profiler. QRadar prend en charge les versions NSM 2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1, et 2010.x. Pour en savoir plus, consultez la documentation de votre fournisseur. Pour collecter des données depuis la base de données PostgreSQL, QRadar doit pouvoir accéder au port de la base de données Postgres via le port TCP 5432. Cet accès lui est accordé dans le fichier `pg_hba.conf`, situé sur le chemin `/var/netscreen/DevSvr/pgsql/data/pg_hba.conf` sur le système hébergeant Juniper NSM Profiler.

Pour ajouter un scanner Juniper NSM Profiler, voir «Ajout d'un scanner Juniper NSM Profiler».

Ajout d'un scanner Juniper NSM Profiler

Les administrateurs peuvent ajouter un scanner Juniper NSM Profiler pour extraire des données de vulnérabilité via JDBC.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre serveur Profiler.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner. Les certificats de votre scanner Juniper NSM Profiler doivent résider sur l'hôte géré sélectionné dans la liste Managed Host.
6. Dans la liste **Type**, sélectionnez **Juniper NSM Profiler Scanner**, puis configurez les paramètres.

Paramètre	Description
Server Host Name	Adresse IP ou nom d'hôte du scanner Juniper NSM Profiler qui contient les vulnérabilités que vous voulez extraire.
Database Username	Nom d'utilisateur requis pour accéder au scanner Juniper NSM Profiler.
Database Password	Mot de passe requis pour accéder au scanner Juniper NSM Profiler.
Database Name	Nom de la base de données du serveur ci-dessus qui contient les données du scanner Juniper NSM Profiler.

7. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
   a. Dans la zone de texte, entrez la plage CIDR pour le scanner ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
   b. Cliquez sur **Ajouter**.
8. Cliquez sur **Sauvegarder**.

12 Présentation du scanner McAfee Vulnerability Manager

Le scanner McAfee Vulnerability Manager permet à QRadar d'importer des données de vulnérabilité depuis un fichier XML ou de rechercher un fichier de résultats à l'aide de McAfee OpenAPI.

QRadar peut collecter des données de vulnérabilités depuis les dispositifs McAfee Vulnerability Manager. Les versions logicielles suivantes sont prises en charge :

- versions 6.8 et 7.0 pour l'API SOAP McAfee Vulnerability Manager
- versions 6.8, 7.0 et 7.5 pour les importations XML distantes

Les options d'importation suivantes sont disponibles pour la collecte d'informations de vulnérabilité depuis McAfee Vulnerability Manager :

- Pour ajouter une importation distante au format XML de données de vulnérabilité, voir «Ajout d'une analyse par importation de fichier XML distant».

  Remarque : Lorsque vous effectuez l'exportation depuis McAfee Vulnerability Manager, vous devez cliquer sur l'onglet **Scan Reports**, puis sélectionner l'option de sortie **XML**.
- Pour extraire des vulnérabilités à l'aide de l'API SOAP, voir «Ajout d'un scanner McAfee Vulnerability Manager via une API SOAP», à la page 35

Ajout d'une analyse par importation de fichier XML distant

Le scanner McAfee Vulnerability Manager permet à QRadar d'importer des données de vulnérabilité depuis un fichier XML avec SFTP, SMB, ou de rechercher un fichier de résultats à l'aide de McAfee OpenAPI.

QRadar peut collecter des données de vulnérabilités depuis les dispositifs McAfee Vulnerability Manager. Les versions logicielles suivantes sont prises en charge :

- versions 6.8 et 7.0 pour l'API SOAP McAfee Vulnerability Manager
- versions 6.8, 7.0 et 7.5 pour les importations XML distantes

Les options d'importation suivantes sont disponibles pour la collecte d'informations de vulnérabilité depuis McAfee Vulnerability Manager :

- Ajouter une importation distante au format XML de données de vulnérabilité avec SFTP.
- Ajouter une importation distante au format XML de données de vulnérabilité avec SMB.

  Remarque : Lorsque vous effectuez l'exportation depuis McAfee Vulnerability Manager, vous devez cliquer sur l'onglet **Scan Reports**, puis sélectionner l'option de sortie **XML**.
- Extraire des vulnérabilités à l'aide de l'API SOAP.

Tâches associées:

«Ajout d'une analyse par importation de fichier XML distant via SFTP», à la page 32
Utilisez SFTP pour importer les données de vulnérabilité XML HostData créées par le dispositif McAfee Vulnerability Manager.

«Ajout d'une analyse par importation de fichier XML distant via SMB», à la page 34
Utilisez SMB pour vous connecter à un serveur distant et importer les données de vulnérabilité XML HostData créées par le dispositif McAfee Vulnerability Manager.

«Ajout d'un scanner McAfee Vulnerability Manager via une API SOAP», à la page 35
Vous pouvez ajouter un scanner McAfee Vulnerability Manager pour permettre à QRadar de collecter des informations sur les hôtes et les vulnérabilités via l'OpenAPI McAfee.

Configuration des exportations distantes pour McAfee Vulnerability Manager

Pour importer des rapports d'analyse dans QRadar, vous pouvez configurer McAfee Vulnerability Manager pour exporter des rapports d'analyse sur un serveur distant.

Pourquoi et quand exécuter cette tâche

Configurez McAfee Vulnerability Manager pour exporter des résultats d'analyse sur un serveur distant. Vous pouvez importer les résultats d'analyse du référentiel distant dans QRadar à l'aide de SFTP (Secure File Transfer Protocol) ou SMB (Server Message Block).

Avertissement : Les données sont exportées dans un fichier compressé qui contient des fichiers XML HostData et RiskData. Seuls les fichiers XML HostData sont pris en charge car ils contiennent les informations d'hôte et de vulnérabilité requises. Vérifiez que seuls des fichiers XML HostData décompressés sont placés dans le répertoire distant ou que le masque de nom de fichier configuré correspond uniquement aux fichiers XML des rapports non compressés.

Procédure

1. Connectez-vous au serveur de gestion des configurations. Cliquez sur **Démarrer**, puis sélectionnez **Tous les programmes** > **Foundstone** > **Console FCM**.
2. Sélectionnez **Outils** > **Préférences**, puis cliquez sur l'onglet **Serveur de rapport**.
3. Sélectionnez **Copier les rapports sur une unité réseau**.
4. Entrez le chemin vers l'unité réseau. Par exemple, `\\CompName\ShareName`.
5. Cliquez sur **Appliquer**.

   Remarque : Si le service **`Serveur de rapports`** ne possède pas les droits d'accès appropriés à l'unité réseau, configurez les paramètres au service **`Serveur de rapports`**.

Ajout d'une analyse par importation de fichier XML distant via SFTP

Utilisez SFTP pour importer les données de vulnérabilité XML HostData créées par le dispositif McAfee Vulnerability Manager.

Avant de commencer

Vérifiez que McAfee Vulnerability Manager est configuré pour exporter des résultats d'analyse sur un serveur distant.

Pourquoi et quand exécuter cette tâche

QRadar se connecte au référentiel distant via SFTP et importe les rapports d'analyse XML complétés depuis le répertoire distant.

Vous pouvez utiliser la méthode de collecte par importation de fichiers pour importer des rapports d'analyse complétés depuis McAfee Vulnerability Manager V7.0 et V7.5.

Avertissement :

1. L'importation peut inclure des fichiers XML HostData et RiskData. Seuls les fichiers XML HostData sont pris en charge car ils contiennent les informations d'hôte et de vulnérabilité requises. Assurez-vous que seuls les fichiers XML HostData sont placés dans le répertoire distant ou que le masque de nom de fichier que vous configurez correspond uniquement aux rapports HostData.
2. Les données sont exportées dans un fichier compressé qui contient des fichiers XML HostData et RiskData. Seuls les fichiers XML HostData sont pris en charge car ils contiennent les informations d'hôte et de vulnérabilité requises. Vérifiez que seuls des fichiers XML HostData décompressés sont placés dans le répertoire distant ou que le masque de nom de fichier configuré correspond uniquement aux fichiers XML des rapports HostData non compressés.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant McAfee Vulnerability Manager.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **McAfee Vulnerability Manager**.
7. Dans la liste **Import Type**, sélectionnez **Remote XML Import**.
8. Dans la zone **Remote Hostname**, entrez l'adresse IP ou le nom d'hôte du serveur distant hébergeant vos données McAfee Vulnerability Manager XML.
9. Dans la zone **Remote Port**, entrez le port depuis lequel extraire les données de vulnérabilité XML.
10. Choisissez l'une des options d'authentification suivantes :

Option	Description
Login Username	S'authentifie avec un nom d'utilisateur et un mot de passe. Le mot de passe ne doit pas contenir de point d'exclamation (!) car ce caractère peut provoquer des échecs d'authentification avec SFTP.
Enable Key Authorization	Authentification avec un fichier d'authentification basé clés. Si un fichier de clés n'existe pas, vous devez créer le fichier vis.ssh.key et le placer dans le répertoire `/opt/qradar/conf/vis.ssh.key`.

11. Dans la zone **Remote Directory File**, entrez le chemin de répertoire des données de vulnérabilité XML.
12. Dans la zone **File Name Pattern**, entrez l'expression régulière (regex) pour filtrer la liste des fichiers spécifiés dans le répertoire distant. Tous les fichiers correspondants sont inclus dans le traitement. Assurez-vous que ce canevas correspond uniquement aux rapports HostData XML.
13. Dans la zone **Max Reports Age (days)**, entrez l'âge maximal du fichier de résultats d'analyse.
14. Pour configurer une plage CIDR pour le scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
15. Cliquez sur **Sauvegarder**.
16. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Concepts associés:

«Ajout d'une analyse par importation de fichier XML distant», à la page 31
Le scanner McAfee Vulnerability Manager permet à QRadar d'importer des données de vulnérabilité depuis un fichier XML avec SFTP, SMB, ou de rechercher un fichier de résultats à l'aide de McAfee

OpenAPI.

Ajout d'une analyse par importation de fichier XML distant via SMB

Utilisez SMB pour vous connecter à un serveur distant et importer les données de vulnérabilité XML HostData créées par le dispositif McAfee Vulnerability Manager.

Avant de commencer

Vérifiez que McAfee Vulnerability Manager est configuré pour exporter les résultats d'analyse sur un serveur distant.

Pourquoi et quand exécuter cette tâche

QRadar se connecte au référentiel distant via SMB et importe les rapports d'analyse XML complétés depuis un répertoire distant.

Vous pouvez utiliser la méthode de collecte par importation de fichiers pour importer des rapports d'analyse complétés depuis McAfee Vulnerability Manager V7.0 et V7.5.

Avertissement :

1. L'importation peut inclure des fichiers XML HostData et RiskData. Seuls les fichiers XML HostData sont pris en charge car ils contiennent les informations d'hôte et de vulnérabilité requises. Assurez-vous que seuls les fichiers XML HostData sont placés dans le répertoire distant ou que le masque de nom de fichier que vous configurez correspond uniquement aux rapports HostData.
2. Les données sont exportées dans un fichier compressé qui contient des fichiers XML HostData et RiskData. Seuls les fichiers XML HostData sont pris en charge car ils contiennent les informations d'hôte et de vulnérabilité requises. Vérifiez que seuls des fichiers XML HostData décompressés sont placés dans le répertoire distant ou que le masque de nom de fichier configuré correspond uniquement aux fichiers XML des rapports HostData non compressés.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners VA**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant McAfee Vulnerability Manager.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **McAfee Vulnerability Manager**.
7. Dans la liste des **Import Type**, sélectionnez **SMB Share**.
8. Dans la zone du **Hostname**, entrez le nom d'utilisateur du serveur distant qui héberge vos données XML McAfee Vulnerability Manager.
9. Dans la zone **Login Username**, entrez le nom d'utilisateur utilisé par QRadar pour se connecter à SMB Share.
10. Dans la zone **Login Password**, entrez le mot de passe utilisé par QRadar pour se connecter à SMB Share.
11. Dans la zone **Domain**, entrez le domaine utilisé pour la connexion à SMB Share.
12. Dans la zone du **SMB Folder Path**, entrez le chemin d'accès complet partage depuis la racine de l'hôte SMB. Utilisez des barres obliques lorsque vous entrez le chemin. Par exemple : `/share/logs`.
13. Dans la zone **File Name Pattern**, entrez une expression régulière (regex) pour filtrer la liste des fichiers qui sont indiqués dans le répertoire distant. Tous les fichiers correspondants sont inclus dans le traitement. Assurez-vous que ce canevas correspond uniquement aux rapports HostData XML.

14. Dans la zone Max Reports Age (days), entrez l'âge maximal du fichier de résultats d'analyse.
15. Configurez une plage CIDR pour le scanner.
    a. Dans la zone de texte, entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
16. Cliquez sur **Sauvegarder**.
17. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Concepts associés:

«Ajout d'une analyse par importation de fichier XML distant», à la page 31
Le scanner McAfee Vulnerability Manager permet à QRadar d'importer des données de vulnérabilité depuis un fichier XML avec SFTP, SMB, ou de rechercher un fichier de résultats à l'aide de McAfee OpenAPI.

Ajout d'un scanner McAfee Vulnerability Manager via une API SOAP

Vous pouvez ajouter un scanner McAfee Vulnerability Manager pour permettre à QRadar de collecter des informations sur les hôtes et les vulnérabilités via l'OpenAPI McAfee.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant le scanner.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner. Les certificats de votre scanner doivent résider sur l'hôte sélectionné dans la liste **Hôte géré**.
6. Dans la liste **Type**, sélectionnez **McAfee Vulnerability Manager**.
7. Dans la zone **SOAP API URL**, entrez l'adresse IP ou le nom d'hôte McAfee Vulnerability Manager qui contient les vulnérabilités que vous désirez extraire avec l'API SOAP. Par exemple, `https://adresse IP foundstone:port SOAP`. Valeur par défaut : `https://localhost:3800.`
8. Dans la zone **Customer Name**, entrez le nom du client rattaché au nom de l'utilisateur.
9. Dans la zone **Username**, entrez le nom d'utilisateur requis pour accéder à McAfee Vulnerability Manager.
10. Facultatif : Dans la zone **Client IP Address**, entrez l'adresse IP du serveur sur lequel effectuer l'analyse.

    Conseil : Cette zone n'est généralement pas utilisée ; cependant, elle peut vous être nécessaire pour valider certains environnements d'analyse.
11. Dans la zone **Password**, entrez le mot de passe requis pour accès à McAfee Vulnerability Manager.
12. Dans la zone **Configuration Name**, entrez le nom d'une configuration d'analyse existant dans McAfee Vulnerability Manager et à laquelle l'utilisateur a accès. Vérifiez que cette analyse est active ou s'exécute fréquemment.
13. Dans la zone **CA Truststore**, entrez le chemin de répertoire et le nom du fichier de clés certifiées CA.

    Le chemin par défaut est `/opt/qradar/conf/mvm.keystore`.
14. Dans la zone **CA Keystore**, entrez le chemin de répertoire et le nom de fichier du magasin de clés client.

    Le chemin par défaut est `/opt/qradar/conf/mvm.truststore`.
15. Dans la liste **McAfee Vulnerability Manager Version**, sélectionnez la version de votre logiciel McAfee Vulnerability Manager.
16. Pour supprimer des vulnérabilités identifiées auparavant mais non détectées par la dernière analyse, cochez la case **Vulnerability Cleanup**.

17. Pour configurer une plage CIDR pour le scanner, procédez comme suit :
    a. Entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.

       McAfee Vulnerability Manager accepte uniquement des plages d'adresses CIDR sur un sous-réseau 0/0 ajoutées sous la forme 0.0.0.0/0.
    b. Cliquez sur **Ajouter**.
18. Cliquez sur **Sauvegarder**.
19. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer des certificats depuis McAfee Vulnerability Manager. Voir «Création de certificats pour McAfee Vulnerability Manager».

Concepts associés:

«Ajout d'une analyse par importation de fichier XML distant», à la page 31
Le scanner McAfee Vulnerability Manager permet à QRadar d'importer des données de vulnérabilité depuis un fichier XML avec SFTP, SMB, ou de rechercher un fichier de résultats à l'aide de McAfee OpenAPI.

Création de certificats pour McAfee Vulnerability Manager

Pour se connecter via l'API à code source ouvert Foundstone, configurez des certificats de tiers à l'aide de l'outil de gestion de certificats de McAfee.

Avant de commencer

Si l'outil Certificate Manager Tool n'est pas installé sur le serveur McAfee Foundstone Enterprise Manager, contactez l'assistance technique McAfee.

Pourquoi et quand exécuter cette tâche

Vous devez traiter les certificats côté client dans des fichiers de clés et de magasin de clés certifiés valides pour QRadar sur le serveur McAfee Foundstone Enterprise Manager.

Le serveur McAfee Foundstone Enterprise Manager doit être compatible avec la version d'OpenSSL répondant aux normes FIPS utilisée par le Foundstone Certficate Manager pour générer correctement les certificats. Un SDK Java doit être présent sur ce serveur pour effectuer ce traitement. Pour obtenir le SDK Java le plus récent, accédez au site Web suivant :

http://java.sun.com.

Procédure

1. Connectez-vous au serveur McAfee Foundstone Enterprise Manager.
2. Lancez l'outil Foundstone Certificate Manager.
3. Cliquez sur l'onglet **Create SSL Certificates**.
4. Entrez l'adresse de l'hôte de QRadar.

   Le certificat doit être créé avec l'adresse hôte du dispositif QRadar qui extraie les données de vulnérabilité de McAfee Vulnerability Manager.
5. Facultatif : Cliquez sur **Resolve**.

   i une erreur survient lorsque le gestionnaire de certificat Foundstone tente de résoudre l'hôte, entrez l'adresse IP dans la zone **Host Address**. Si la résolution de l'hôte échoue, reportez-vous à l'étape 7, à la page 37.

6. Cliquez sur **Create Certificate Using Common Name**.
7. Cliquez sur **Create Certificate Using Host Address**.
8. Enregistrez dans un répertoire sur le serveur McAfee Vulnerability Manager le fichier compressé contenant les fichiers de certificat.
9. Copiez dans un fichier texte la phrase passe fournie.
10. Répétez éventuellement cette procédure pour générer d'autres certificats pour les hôtes gérés dans votre déploiement.

Que faire ensuite

Vous pouvez maintenant traiter les certificats afin de créer les fichiers de clés et de magasin de clés certifiées requis. Voir «Traitement des certificats pour McAfee Vulnerability Manager».

Traitement des certificats pour McAfee Vulnerability Manager

Pour créer le magasin de clés certifiées et les fichiers de clés requis par QRadar.

Avant de commencer

Vous devez avoir accès au portail de support pour télécharger les fichiers requis pour créer le magasin de clés certifiées et les fichiers de clés. Les fichiers de commande requièrent que le chemin corresponde au répertoire principal Java sur le serveur McAfee Vulnerability Manager.

Procédure

1. Connectez-vous au portail de support pour télécharger les fichiers suivants:
   - `VulnerabilityManager-Cert.bat.gz`
   - `q1labs_vis_mvm_cert.jar`
2. Décompressez les fichiers et copiez les certificats et les fichiers téléchargés vers le même répertoire sur votre serveur McAfee Vulnerability Manager.
3. Ouvrez l'interface de ligne de commande sur le serveur McAfee Vulnerability Manager.
4. Accédez à l'emplacement du répertoire des fichiers.
5. Pour exécuter le fichier de commandes, entrez la commande suivante: `VulnerabilityManager-CERT .bat "C:\Program Files\Java\ jdk1.6.0_20" .`

   Les guillemets dans la commande spécifient le répertoire de base Java.
6. Répétez ce processus pour créer des magasins de clés certifiées et des fichiers de clés pour les autres hôtes gérés éventuels dans votre déploiement.

Résultats

La magasin de clés certifiées et les fichiers de clés sont créés. Si une erreur est signalée, les administrateurs peuvent vérifier le chemin du répertoire principal Java.

Que faire ensuite

Vous pouvez à présent importer les certificats pour votre dispositif QRadar. Voir «Importation de certificats pour McAfee Vulnerability Manager»

Importation de certificats pour McAfee Vulnerability Manager

Le fichier de clé ainsi que les magasins de clés certifiées doivent être importés sur l'hôte géré chargé de l'analyse.

Avant de commencer

Vous devez ajouter le scanner à un hôte géré dans la configuration d'analyse avant d'importer des certificats. A des fins de sécurité, utilisez un protocole de transfert de fichier sécurisé pour copier un fichier de certificat.

Procédure

1. Pour importer les certificats, effectuez une copie sécurisée des fichiers mvm.keystore et mvm.truststore vers les répertoires suivants dans QRadar :
   - `/opt/qradar/conf/`
   - `/opt/qradar/conf/trusted_certificates/`

     Remarque : Si le répertoire `/opt/qradar/conf/trusted_certificates/` n'existe pas, ne créez pas ce répertoire. Si le répertoire n'existe pas, les administrateurs peuvent ignorer la copie de fichier pour le répertoire concerné.

   Si vous utilisez un déploiement réparti, vous devez copier les fichiers vers la console et transférer sous SSH les fichiers depuis le dispositif de la console vers l'hôte réparti.
2. Connectez-vous à QRadar.
3. Cliquez sur l'onglet **Admin**.
4. Dans l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.

   Remarque : Lorsque vous cliquez sur **Déployer la configuration entière**, QRadar redémarre tous les services. Le redémarrage du service entraîne une coupure dans la collecte des événements et des flux jusqu'à ce que s'achève le processus de déploiement.
5. Répétez l'opération d'importation des certificats pour tous les hôtes gérés dans votre déploiement qui collectent des vulnérabilités à l'aide de McAfee Vulnerability Manager.

13 Présentation du scanner Microsoft

IBM Security QRadar peut importer des rapports d'analyse provenant de scanners SCCM (Microsoft System Center Configuration Manager).

Pour intégrer un scanner Microsoft SCCM, procédez comme suit :

1. Sur votre scanner Microsoft SCCM, configurez l'activation WMI.
2. Si les mises à jour automatiques ne sont pas activées sur QRadar Console, téléchargez et installez le RPM de Microsoft SCCM.
3. Sur QRadar Console, ajoutez un scanner Microsoft SCCM.
4. Sur QRadar Console, créez une planification d'analyse pour importer vos données de résultats d'analyse.

Concepts associés:

«Activation de WMI pour les scanners Microsoft SCCM»
Pour pouvoir configurer un scanner Microsoft SCCM, vous devez d'abord configurer les paramètres DCOM de votre système pour chaque hôte que vous souhaitez surveiller.

Tâches associées:

«Ajout d'un scanner Microsoft SCCM», à la page 40

24, «Planification d'une analyse de vulnérabilité», à la page 83
Les planifications d'analyse sont des intervalles affectés aux scanners et qui déterminent quand des données d'évaluation de vulnérabilités doivent être importées depuis vos dispositifs d'analyse sur votre réseau. Les planifications d'analyse peuvent également définir les plages CIDR ou les sous-réseaux à inclure dans l'importation des données lors de l'importation des données de vulnérabilité.

Activation de WMI pour les scanners Microsoft SCCM

Pour pouvoir configurer un scanner Microsoft SCCM, vous devez d'abord configurer les paramètres DCOM de votre système pour chaque hôte que vous souhaitez surveiller.

L'hôte du scanner doit remplir les conditions suivantes :

- Vous êtes membre du groupe Administrateurs sur cet hôte.
- L'un des systèmes d'exploitation suivants est installé :
  - Windows 7
  - Windows 2008
  - Windows 2008 R2
  - Windows 2012
  - Windows 2012 R2 (seule la version 64 bits est prise en charge)
  - Vista

  Important : SCCM n'est pas pris en charge sur les versions de Windows que Microsoft a placées dans la catégorie *Fin de vie*. Si la date de la version du logiciel est postérieure à la *date de fin du support étendu*, le produit risque de ne pas fonctionner comme prévu. IBM ne crée pas de correctifs de code ou de vulnérabilité pour corriger les problèmes sur les anciens systèmes d'exploitation. Par exemple, Microsoft Windows Server 2003 R2 et Microsoft Windows XP sont des systèmes d'exploitation postérieurs à la *date de fin du support étendu*. Toute question relative à ces informations peut être

débattue dans les forums IBM Security QRadar. Pour plus d'informations sur les cycles de vie du support, voir le site Web sur les cycles de vie de Microsoft Support (https://support.microsoft.com//en-us/lifecycle/search)

- DCOM est configuré et activé.

  Si un pare-feu est installé sur l'hôte ou se trouve entre l'hôte et QRadar, comme un composant matériel ou un autre pare-feu intermédiaire, le pare-feu doit être configuré pour autoriser les communications DCOM. Configurez le pare-feu de manière à rendre le port 135 accessible sur l'hôte et à autoriser les ports DCOM. Les ports DCOM sont des ports aléatoires au-dessus de 1024. En fonction de la version de Windows utilisée, vous pouvez être amené à configurer des ports spécifiques accessibles pour DCOM. Pour plus d'informations, reportez-vous à la documentation de Windows.
- Windows Management Instrumentation (WMI) est activé.
- Le service de registre distant est activé.

Pour connaître les instructions de configuration de DCOM et de WMI sous Windows 7, Windows 2008 et Windows 2012 R2, reportez-vous aux documents suivants sur le site de support IBM :

- Windows 7 (http://www.ibm.com/support/docview.wss?uid=swg21678809)
- Windows 2008 (http://www.ibm.com/support/docview.wss?uid=swg21681046)
- Windows 2012 R2 (http://www.ibm.com/support/docview.wss?uid=swg21986943)

Ajout d'un scanner Microsoft SCCM

Avant de commencer

Vérifiez que WMI est activé sur l'hôte de votre scanner.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Configurez les paramètres Microsoft suivants :

Paramètre	Description
Nom du scanner	Nom permettant d'identifier votre instance de scanner.
Hôte géré	Hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
Type	Microsoft SCCM
Nom d'hôte	Adresse IP ou nom d'hôte du serveur distant qui héberge les fichiers de résultat d'analyse.
Domaine	Domaine utilisé pour se connecter au serveur distant.

5. Configurez les paramètres restants.
6. Pour configurer une plage CIDR pour le scanner, procédez comme suit :
   a. Entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
   b. Cliquez sur **Ajouter**.
7. Cliquez sur **Sauvegarder**.

14 Présentation du scanner nCircle IP360

QRadar prend en charge à la fois les versions nCircle et Tripwire du scanner IP360. Les administrateurs peuvent importer des rapports d'analyse XML2 depuis des serveurs SSH contenant des informations de vulnérabilité IP360.

Il est impossible de connecter directement QRadar aux périphériques nCircles. Vous pouvez configurer un périphérique d'analyse nCircle IP360 pour exporter les résultats d'analyse au format XML2 vers un serveur SSH distant. Pour importer les résultats d'analyse les plus récents du serveur distant vers QRadar, vous pouvez planifier une analyse ou interroger le serveur distant concernant les mises à jour des résultats d'analyse.

Les résultats de l'analyse contiennent des informations d'identification relatives à la configuration de l'analyse à partir de laquelle ils ont été produits. Les résultats d'analyse les plus récents sont utilisés lorsque QRadar importe une analyse. QRadar ne prend en charge que les résultats d'analyse exportés uniquement à partir du scanner IP360 au format XML2.

Pour intégrer un scanner nCircle IP360, procédez comme suit :

1. Sur le scanner nCircle IP360, configurez votre scanner nCircle pour exporter les résultats d'analyses. Voir «Exportation de résultats d'analyse nCircle IP360 vers un serveur SSH».
2. Sur votre console QRadar, ajoutez un scanner nCircle IP360. Voir «Ajout d'un scanner nCircle IP360»
3. Sur votre console QRadar, créez une planification d'analyse pour importer vos données de résultats d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83

Exportation de résultats d'analyse nCircle IP360 vers un serveur SSH

QRadar utilise une fonction d'exportation automatique pour publier les données d'analyse XML2 des dispositifs nCircle IP360. QRadar prend en charge les versions VnE Manager IP360 allant de la 6.5.2 à la 6.8.2.8.

Avant de commencer

Assurez-vous que le serveur distant est un système UNIX avec SSH activé.

Procédure

1. Connectez-vous à l'interface utilisateur VNE Manager IP360.
2. Dans le menu de navigation, sélectionnez **Administer** > **System** > **VNE Manager** > **Automated Export**.
3. Cliquez sur l'onglet **Export to File**.
4. Configurez les paramètres d'exportation. L'exportation doit être configurée pour utiliser le format XML2.
5. Notez les paramètres de la cible affichés dans l'interface utilisateur pour l'exportation de l'analyse. Ces paramètres sont nécessaires pour configurer l'intégration de QRadar avec votre dispositif nCircle IP360.

Ajout d'un scanner nCircle IP360

QRadar utilise le protocole SSH (Secure Shell) pour accéder à un serveur distant (serveur d'exportation SSH) afin d'extraire et d'interpréter les données d'analyse de dispositifs nCircle IP360. QRadar prend en charge les versions VnE Manager IP360 allant de la 6.5.2 à la 6.8.2.8.

Avant de commencer

Cette configuration a besoin des paramètres de cible que vous avez enregistrés lors de l'exportation des données d'analyse XML2 sur le serveur distant.

Pourquoi et quand exécuter cette tâche

Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH auquel QRadar connecte doit prendre en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification par SSH du scanner échoue. Vérifiez que la ligne suivante figure dans votre fichier `sshd_config`, qui se trouve généralement dans `/etc/ssh directory` sur le serveur SSH : `PasswordAuthentication yes`. Si le serveur de votre scanner n'utilise pas OpenSSH, la configuration peut différer. Pour plus d'informations, consultez la documentation de votre scanner.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Configurez les paramètres nCircle IP360 suivants :

Paramètre	Description
Scanner Name	Nom permettant d'identifier votre instance nCircle IP360.
Managed Host	Hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
Type	nCircle IP360
SSH Server Host Name	Adresse IP ou nom d'hôte du serveur distant qui héberge les fichiers de résultat d'analyse.
SSH Port	Numéro de port pour la connexion au serveur distant.
Remote Directory	Emplacement des fichiers de résultat d'analyse.
File Pattern	Expression régulière (regex) requise pour filtrer la liste de fichiers spécifiée dans la zone **Remote Directory**. Pour afficher la liste de tous les fichiers de format XML2 qui se terminent par XML, utilisez l'entrée suivante : `XML2.*\.xml`

5. Configurez les paramètres restants.
6. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
   a. Entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
   b. Cliquez sur **Ajouter**.
7. Cliquez sur **Sauvegarder**.
8. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

15 Présentation du scanner Nessus

QRadar peut utiliser une relation client serveur Nessus pour extraire des rapports d'analyse de vulnérabilité. Vous pouvez également utiliser l'API Nessus XMLRPC, ou l'API JSON pour accéder aux données de numérisation directement à partir de Nessus.

Lorsque vous configurez votre client Nessus, vous devez créer un compte d'utilisateur Nessus pour votre système QRadar. Un compte d'utilisateur unique assure que QRadar dispose des informations d'identification correctes pour se connecter et communiquer avec le serveur Nessus. Après la création du compte d'utilisateur, un test de connexion vérifie les informations d'identification utilisateur et l'accès à distance.

Remarque : N'installez pas le logiciel Nessus sur un système critique en raison des exigences d'UC quand les analyses sont actives.

Options de collecte de données

Les options suivantes sont disponibles pour la collecte de données d'informations de vulnérabilité depuis des scanners Nessus :

Scheduled Live Scan (Analyse planifiée immédiate)
Les analyses immédiates permettent de démarrer à distance des analyses prédéfinies via SSH dans Nessus et les données sont importées à la fin de l'analyse.

Scheduled Results Import (Importation planifiée de résultats)
Les fichiers de résultat statiques d'analyses terminées sont importées via SSH depuis un référentiel contenant les résultats de l'analyse Nessus.

Scheduled Live Scan (Analyse planifiée immédiate) - API XMLRPC
L'API XMLRPC permet de démarrer à distance les analyses prédéfinies et de les collecter activement.

L'API Nessus XMLRPC n'est disponible que sur les serveurs et les clients Nessus dont le logiciel correspond à la version 4.2 jusqu'à la version 5.x.

Scheduled Live Scan (Analyse planifiée immédiate) - API JSON
L'API JSON permet de démarrer à distance les analyses prédéfinies et de les collecter activement.

L'API JSON n'est pas disponible sur les serveurs et clients Nessus dont le logiciel est antérieur à la version 6.0.

Scheduled Completed Report Import (Importation de l'analyse planifiée immédiate) - API XMLRPC
L'API XMLRPC permet d'importer les rapports terminés à partir du serveur Nessus.

L'API Nessus XMLRPC n'est disponible que sur les serveurs et les clients Nessus dotés de la version 4.2 jusqu'à la version 5.x.

Scheduled Completed Report Import - API JSON
L'API JSON permet d'importer les rapports terminés à partir du serveur Nessus.

L'API JSON n'est pas disponible sur les serveurs et les clients Nessus dont le logiciel est antérieur à la version 6.0.

Certificats serveur

Avant d'ajouter un scanner, un certificat serveur est requis pour prendre en charge les connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : `.crt`, `.cert` ou `.der`. Pour copier un certificat dans le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat dans le répertoire `/opt/qradar/conf/trusted_certificates` via SCP (Secure Copy) ou SFTP (Secure File Transfer Protocol).
- Pour télécharger automatiquement le certificat dans le répertoire `/opt/qradar/conf/trusted_certificates`, connectez-vous via SSH à la console ou à l'hôte géré et saisissez la commande suivante :

  `/opt/qradar/bin/getcert.sh <adresse_IP_ou_nom_hôte> <port_facultatif_(valeur_par_défaut_443)>`.

Ajout d'une analyse planifiée Nessus immédiate

Une analyse immédiate s'exécute sur votre serveur Nessus et importe les données de résultat d'un répertoire temporaire du client Nessus contenant les données du rapport d'analyse.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Nessus.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner.
6. Dans la liste **Type**, sélectionnez **Nessus Scanner**.
7. Dans la liste **Collection Type**, sélectionnez **Scheduled Live Scan**.
8. .
9. Configurez les paramètres suivants :

Paramètre	Description
Server Username	Nom d'utilisateur requis pour accéder au serveur Nessus.
Server Password	Votre mot de passe d'accès au serveur Nessus ne doit pas contenir de point d'exclamation (!) car ceci pourrait causer des échecs d'authentification avec SSH.
Client Temp Dir	Chemin du répertoire du client Nessus que QRadar peut utiliser pour stocker les fichiers temporaires. QRadar utilise le répertoire temporaire sur le client Nessus pour télécharger des cibles d'analyse et lire les résultats d'analyse. Les fichiers temporaires sont supprimés du répertoire temporaire lorsque l'analyse est terminée et le rapport d'analyse est téléchargé.
Nessus Executable	Chemin du répertoire du fichier exécutable sur le serveur Nessus.
Nessus Configuration File	Chemin du répertoire du fichier de configuration Nessus, sur le client Nessus.
Client Hostname	Nom d'hôte ou adresse IP du client Nessus.
Client SSH Port	Port SSH sur le serveur Nessus qui peut être utilisé pour récupérer des fichiers de résultat de l'analyse.
Client Username	Nom d'utilisateur pour authentifier la connexion SSH.

Paramètre	Description
Client Password	Si la zone **Enable Key Authentication** est activée, le mot de passe est ignoré. Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH qui se connecte à QRadar doit prendre en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification par SSH du scanner échoue. Vérifiez que la ligne suivante figure dans votre fichier `/etc/ssh/sshd_config` : `PasswordAuthentication yes`. Si le serveur de votre scanner n'utilise pas OpenSSH, consultez dans la documentation de son fournisseur les informations de configuration du scanner.
Private Key File	Chemin du répertoire du fichier de clés. Si un fichier de clés n'existe pas, vous devez créer le fichier `vis.ssh.key`.
CIDR Mask	Taille du sous-réseau que vous souhaitez analyser. La valeur représente la portion la plus large du sous-réseau que le scanner peut analyser à un moment donné. Le masque segmente l'analyse afin d'optimiser les performances de l'opération.

10. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
11. Cliquez sur **Sauvegarder**.
12. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Ajout d'une importation planifiée de résultats Nessus

Une importation planifiée de résultats extrait des rapports d'analyse Nessus terminés depuis un emplacement externe.

Pourquoi et quand exécuter cette tâche

Un rapport de fin d'analyse peut être stocké sur un serveur Nessus ou un référentiel de fichiers. QRadar se connecte au serveur Nessus, ou au référentiel de fichiers en utilisant SSH puis importe les fichiers de rapport d'analyse terminée. Les rapports sont filtrés par une expression régulière définie ou l'âge de rapport maximal. QRadar prend en charge les importations de rapports d'analyse Nessus au format `.nessus` ou les rapports d'analyse exportés dans un format de sortie Nessus, tel que XML2.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Nessus.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Nessus Scanner**.
7. Dans la liste **Collection Type**, sélectionnez **Scheduled Results Import**.
8. Dans la zone **Remote Results Hostname**, entrez l'adresse IP ou le nom d'hôte du client ou serveur Nessus hébergeant vos fichiers de résultats d'analyse Nessus ou XML2.
9. Choisissez l'une des options d'authentification suivantes :

Option	Description
Login Username	Pour s'authentifier avec un nom d'utilisateur et un mot de passe, procédez comme suit : 1. Dans la zone **SSH Username**, entrez le nom d'utilisateur requis pour accéder au scanner Nessus ou le référentiel hébergeant les fichiers de résultats d'analyse. 2. Dans la zone **SSH Password**, entrez le mot de passe associé au nom d'utilisateur. Le mot de passe ne doit pas contenir de point d'exclamation (!) car ce caractère peut provoquer des échecs d'authentification avec SSH.
Enable Key Authorization	Pour s'authentifier avec un fichier d'authentification basé clés, procédez comme suit : 1. Cochez la case **Enable Key Authentication**. 2. Dans la zone **Private Key File**, entrez le chemin de répertoire du fichier de clés. Par défaut, il s'agit de `/opt/qradar/conf/vis.ssh.key`. Si un fichier de clés n'existe pas, vous devez créer le fichier vis.ssh.key.

10. Dans la zone **Remote Results Directory**, entrez l'emplacement du répertoire des fichiers de résultat de l'analyse. Le répertoire par défaut est : `./`.
11. Dans la zone **File Name Pattern**, entrez l'expression régulière (regex) pour filtrer la liste des fichiers spécifiés dans le répertoire distant. Tous les fichiers correspondants sont inclus dans le traitement. Par défaut, la zone **Report Name Pattern** contient `.*\.nessus` comme modèle d'expression régulière. Le modèle `.*\.nessus` importe tous les fichiers de résultats formatés Nessus dans le répertoire distant.
12. Dans la zone **Max Reports Age (Days)**, entrez l'âge maximal du fichier de résultats d'analyse. Les fichiers plus anciens que le nombre de jours et l'horodatage spécifiés dans le fichier de rapport sont exclus lorsque l'analyse planifiée est lancée. La valeur par défaut est 7 jours.
13. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
14. Cliquez sur **Sauvegarder**.

Ajout d'une analyse immédiate Nessus avec l'API XMLRPC

IBM Security QRadar peut utiliser l'API XMLRPC pour commencer une analyse préconfigurée qui est basée sur un nom d'analyse et un nom de politique facultative sur le serveur Nessus.

Pourquoi et quand exécuter cette tâche

Pour démarrer une analyse opérationnelle depuis QRadar, vous devez indiquer le nom de l'analyse et le nom de la règle pour les données d'analyse opérationnelle que vous souhaitez récupérer. Au fur et à mesure que l'analyse immédiate progresse, vous pouvez placer le pointeur de la souris sur le scanner Nessus dans la fenêtre Scan Scheduling pour afficher le pourcentage d'analyse immédiate terminé. A la fin de l'analyse opérationnelle, QRadar utilise l'interface API XMLRPC pour récupérer les données d'analyse et mettre à jour les informations de vulnérabilité de vos actifs.

L'API Nessus XMLRPC n'est disponible que sur les serveurs et les clients Nessus dotés de la version 4.2 jusqu'à la version 5.0.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Nessus.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Nessus Scanner**.
7. Dans la liste **Collection Type**, sélectionnez **Scheduled Live Scan - XMLRPC API**.
8. Configurez les paramètres suivants :

Paramètre	Description
Hostname	Adresse IP ou nom d'hôte du serveur Nessus.
Port	Numéro de port du serveur Nessus.
Username	Nom d'utilisateur requis pour accéder au serveur Nessus.
Password	Votre mot de passe d'accès au serveur Nessus ne doit pas contenir de point d'exclamation (!) car ceci pourrait produire des échecs d'authentification avec SSH.
Scan Name	Nom de l'analyse que vous voulez afficher lorsque l'analyse immédiate s'exécute sur le serveur Nessus. Si cette zone est vide, l'API tente de lancer une analyse immédiate pour QRadar Scan. Cette zone ne prend pas en charge l'utilisation du caractère perluète (&).
Policy Name	Nom d'une règle sur votre serveur Nessus pour lancer une analyse immédiate. La règle doit exister sur le serveur Nessus lorsque le système tente de lancer l'analyse. Si la règle n'existe pas, une erreur est affichée dans la colonne **Status**. Les systèmes peuvent avoir des noms de règle personnalisés, mais plusieurs noms de règle par défaut sont inclus. `External Network Scan`, `Internal Network Scan`, `Web App Tests`, `Prepare for PCI DSS audits` sont des noms de règles par défaut.

9. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
   a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
   b. Cliquez sur **Ajouter**.
10. Cliquez sur **Sauvegarder**.

Ajout d'une importation de rapport Nessus terminé à l'aide de l'API XMLRPC

Une importation de résultats planifiée utilisant l'API XMLRPC permet de télécharger des rapports de vulnérabilité terminés depuis le scanner Nessus.

Pourquoi et quand exécuter cette tâche

IBM Security QRadar se connecte au serveur Nessus et télécharge les données à partir des rapports complets qui correspondent aux filtres de nom et d'âge maximal des rapports. L'API Nessus XMLRPC est disponible sur les serveurs et les clients Nessus dotés de la version 4.2 jusqu'à la version 5.x.

Procédure

1. Ouvrez une session dans QRadar en tant qu'administrateur.
2. Cliquez sur l'onglet **Admin**.
3. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
4. Cliquez sur **Ajouter**.
5. Dans la zone **Nom du scanner**, entrez un nom identifiant votre serveur Nessus.
6. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
7. Dans la liste **Type**, sélectionnez **Scheduled Completed Report Import - XMLRPC AP**.
8. Dans la zone **Hostname**, entrez l'adresse IP ou le nom d'hôte du serveur Nessus contenant les vulnérabilités que vous souhaitez extraire avec l'API Nessus XMLRPC.
9. Dans la zone **Port**, entrez le numéro de port du serveur Nessus. La valeur par défaut du port d'API est 8834. .
10. Dans la zone **Username**, entrez le nom d'utilisateur requis pour accéder au serveur Nessus.
11. Dans la zone **Password**, entrez le mot de passe requis pour accéder au serveur Nessus.
12. Dans la zone **Report Name Pattern**, entrez l'expression régulière (regex) requise pour filtrer la liste de fichiers spécifiée dans le répertoire distant. Tous les fichiers correspondants sont inclus dans le traitement. Par défaut, la zone **Report Name Pattern** contient `.*` comme canevas d'expression régulière. Le canevas `.*` importe tous les fichiers au format Nessus dans le répertoire distant.
13. Dans la zone **Max Reports Age (Days)**, entrez l'âge maximal du fichier de résultats d'analyse. Les fichiers plus anciens que le nombre de jours et l'horodatage spécifiés dans le fichier de rapport sont exclus lorsque l'analyse planifiée est lancée. La valeur par défaut est 7 jours.
14. Configurez une plage CIDR pour le scanner .
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
15. Cliquez sur **Sauvegarder**.

Ajout d'une analyse immédiate Nessus avec l'API JSON

IBM Security QRadar peut utiliser l'API JSON pour commencer une analyse préconfigurée qui est basée sur un nom d'analyse et un nom de politique facultative sur le serveur Nessus.

Pourquoi et quand exécuter cette tâche

Pour démarrer une analyse opérationnelle depuis QRadar, vous devez indiquer le nom de l'analyse et le nom de la règle pour les données d'analyse opérationnelle que vous souhaitez récupérer. Comme l'analyse immédiate progresse, vous pouvez pointer votre souris sur le scanner Nessus dans la fenêtre Scan cheduling pour afficher le pourcentage d'analyse immédiate terminé. A la fin de l'analyse immédiate, QRadar utilise l'interface API JSON pour récupérer les données d'analyse et mettre à jour les informations de vulnérabilité de vos actifs.

L'API Nessus JSON n'est disponible que sur les serveurs et clients Nessus dont le logiciel correspond à la version v6.0 ou ultérieure.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Nessus.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Nessus Scanner**.
7. Dans la liste **Collection Type**, sélectionnez **Scheduled Live Scan - JSON API**.
8. Configurez les paramètres suivants :

Paramètre	Description
Hostname	Adresse IP ou nom d'hôte du serveur Nessus.
Port	Numéro de port du serveur Nessus.
Username	Nom d'utilisateur requis pour accéder au serveur Nessus.
Password	Votre mot de passe d'accès au serveur Nessus ne doit pas contenir de point d'exclamation (!) car ceci pourrait causer des échecs d'authentification.
Scan Name	Nom de l'analyse que vous voulez afficher lorsque l'analyse immédiate s'exécute sur le serveur Nessus. Si cette zone est vide, l'API tente de lancer une analyse immédiate pour QRadar Scan. Cette zone ne prend pas en charge l'utilisation du caractère perluète (&).
Policy Name	Nom d'une règle sur votre serveur Nessus pour lancer une analyse immédiate. La règle doit exister sur le serveur Nessus lorsque le système tente de lancer l'analyse. Si la règle n'existe pas, une erreur est affichée dans la colonne **Status**. Les systèmes peuvent avoir des noms de règle personnalisés, mais plusieurs noms de règle par défaut sont inclus. `External Network Scan`, `Internal Network Scan`, `Web App Tests`, `Prepare for PCI DSS audits` sont des noms de règles par défaut.
Scanner Name	S'il existe plusieurs scanners Nessus dans votre déploiement, indiquez le nom du scanner sur lequel vous souhaitez exécuter les analyses.

9. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
   a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
   b. Cliquez sur **Ajouter**.
10. Cliquez sur **Sauvegarder**.

Ajout d'une importation de rapport Nessus terminé à l'aide de l'API JSON

Une importation planifiée de résultats extrait des rapports d'analyse Nessus terminés depuis un emplacement externe à l'aide de l'API JSON.

Pourquoi et quand exécuter cette tâche

Un rapport de fin d'analyse peut être stocké sur un serveur Nessus ou un référentiel de fichiers. IBM Security QRadar se connecte au serveur Nessus, ou au référentiel de fichiers en utilisant l'API JSON puis importe les fichiers de rapport d'analyse terminée. Les rapports sont filtrés par une expression définie ou l'âge de rapport maximal.

L'API Nessus JSON n'est disponible que sur les serveurs et clients Nessus dont le logiciel correspond à la version v6.0 ou ultérieure.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Nessus.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Nessus Scanner**.
7. Dans la liste **Type de collection**, sélectionnez **Scheduled Completed Report Import - JSON API**.
8. Configurez les paramètres suivants :

Paramètre	Description
Hostname	Adresse IP ou nom d'hôte du serveur Nessus.
Port	Numéro de port du serveur Nessus.
Username	Nom d'utilisateur requis pour accéder au serveur Nessus.
Password	Mot de passe du serveur Nessus.
Report Name Filter	Filtre la liste des fichiers qui sont spécifiés dans le répertoire distant. Tous les fichiers correspondants sont inclus dans le traitement. Par défaut, la zone Report Name Pattern contient `.*` en tant que filtre.
Report Max Age (days)	Âge maximum du fichier pour votre fichier de résultats d'analyse. Les fichiers plus anciens que le nombre de jours et l'horodatage spécifiés dans le fichier de rapport sont exclus lorsque l'analyse planifiée est lancée. La valeur par défaut est 7 jours.

9. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
   a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
   b. Cliquez sur **Ajouter**.
10. Cliquez sur **Sauvegarder**.

16 Présentation du scanner netVigilance SecureScout

QRadar peut collecter des informations de vulnérabilité depuis une base de données sur le scanner SQL en s'enquérant de ces données via JDBC.

netVigilance SecureScout NX et SecureScout SP stockent les résultats d'analyse dans une base de données SQL. Il peut s'agir d'une base de données Microsoft MSDE ou SQL Server. Pour collecter des vulnérabilités, QRadar se connecte à la base de données distante pour localiser les derniers résultats d'analyse d'une adresse IP donnée. Les données renvoyées actualisent le profil de l'actif dans QRadar en incluant l'adresse IP de l'actif, les services détectés et les vulnérabilités identifiées. QRadar prend en charge la version 2.6 du scanner SecureScout.

Nous suggérons aux administrateurs de créer un utilisateur spécial dans votre base de données SecureScout afin que QRadar l'utilise pour rechercher des données de vulnérabilité.

L'utilisateur de base de données que vous créez doit disposer des autorisations de sélection pour les tables suivantes :

- HOST
- JOB
- JOB_HOST
- SERVICE
- TCRESULT
- TESTCASE
- PROPERTY
- PROP_VALUE
- WKS
- IPSORT - L'utilisateur de la base de données doit disposer de l'autorisation Execute pour cette table.

Pour ajouter une configuration de scanner, voir «Ajout d'un scanner netVigilance SecureScout».

Ajout d'un scanner netVigilance SecureScout

Les administrateurs peuvent ajouter un scanner SecureScout pour interroger les données de vulnérabilité via JDBC.

Avant de commencer

Pour interroger les données de vulnérabilité, QRadar doit disposer des droits d'administration appropriés pour interroger le scanner SecureScout via JDBC. Les administrateurs doivent également s'assurer que les pare-feux, y-compris celui sur l'hôte SecureScout, permettent une connexion depuis l'hôte chargé de l'analyse au scanner SecureScout.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre serveur SecureScout.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.

6. Dans la liste **Type**, sélectionnez **SecureScout Scanner**.
7. Dans la zone **Database Hostname**, entrez l'adresse IP ou le nom d'hôte du serveur de base de données SecureScout qui contient le serveur SQL.
8. Dans la zone **Login Name**, entrez le nom d'utilisateur requis pour accéder à la base de données SQL du scanner SecureScout.
9. Facultatif. Dans la zone **Login Password**, entrez le mot de passe requis pour accéder à la base de données SQL du scanner SecureScout.
10. Dans la zone **Database Name**, entrez `SCE`.
11. Dans la zone **Database Port**, entrez le port TCP dont le serveur SQL doit surveiller les connexions. La valeur par défaut est 1433.
12. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
13. Cliquez sur **Sauvegarder**.
14. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

17 Présentation du scanner Nmap

QRadar utilise SSH pour communiquer avec le serveur Nmap, pour lancer des analyses Nmap à distance ou pour télécharger les résultats d'analyses Nmap terminées.

Restriction : Même si chaque hôte QRadar dispose d'un NMap binaire, celui-ci est uniquement destiné à un usage interne de QRadar. La configuration d'un scanner de vulnérabilité NMap dans le but d'utiliser une console QRadar Console ou un hôte géré QRadar en tant que scanner NMap distant n'est pas prise en charge et peut entraîner des instabilités.

Lorsque les administrateurs configurent une analyse Nmap, un compte utilisateur Nmap spécifique peut être créé pour le système QRadar. Un compte utilisateur unique garantit que QRadar dispose des données d'identification requises pour se connecter et communiquer avec le serveur Nmap. Une fois le compte utilisateur créé, les administrateurs peuvent tester la connexion depuis QRadar au client Nmap avec SSH pour vérifier les données d'identification de l'utilisateur. Ce test garantit que chaque système peut communiquer avant que le système ne tente de télécharger les données d'analyse des vulnérabilités ou de lancer une analyse ponctuelle.

Les options suivantes sont disponibles pour la collecte de données d'informations de vulnérabilité depuis des scanners Nessus.

- Analyse immédiate distante. Les analyses immédiates utilisent le fichier binaire Nmap pour lancer des analyses à distance. Au terme de l'analyse immédiate, les données sont importées via SSH. Voir «Ajout d'une analyse immédiate Nmap distante», à la page 55.
- Importation de résultats à distance. Les données de résultat d'une analyse complétée auparavant sont importées via SSH. Voir «Ajout d'une importation de résultats Nmap distants»

Ajout d'une importation de résultats Nmap distants

Une importation de résultats distants extrait des rapports d'analyse Nmap terminés via SSH.

Pourquoi et quand exécuter cette tâche

Les analyses doivent être générées au format XML en spécifiant l'option `-oX` sur votre scanner Nmap. Après avoir ajouté votre scanner Nmap, vous devez définir une planification d'analyse spécifiant la fréquence d'importation des données de vulnérabilité depuis le scanner.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Nmap.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Nessus Scanner**.
7. Dans la liste **Collection Type**, sélectionnez **Remote Results Import**.
8. Dans la zone **Server Hostname**, entrez le nom d'hôte ou l'adresse IP du système distant hébergeant le client Nmap. Il est recommandé que les administrateurs hébergent Nmap sur un système UNIX sur lequel SSH est activé.
9. Choisissez l'une des options d'authentification suivantes :

Option	Description
Login Username	Pour s'authentifier avec un nom d'utilisateur et un mot de passe, procédez comme suit : 1. Dans la zone **Server Username**, entrez le nom d'utilisateur requis pour accéder au système distant hébergeant le client Nmap. 2. Dans la zone **Login Password**, entrez le mot de passe associé au nom d'utilisateur. Le mot de passe ne doit pas contenir le ! car ce caractère peut provoquer des échecs d'authentification avec SSH. Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH qui se connecte à QRadar doit prendre en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification par SSH du scanner échoue. Vérifiez que la ligne suivante figure dans votre fichier `/etc/ssh/sshd_config` : `PasswordAuthentication yes`. Si le serveur de votre scanner n'utilise pas OpenSSH, consultez dans la documentation de son fournisseur les informations de configuration du scanner.
Enable Key Authorization	Pour s'authentifier avec un fichier d'authentification basé clés, procédez comme suit : 1. Cochez la case **Enable Key Authentication**. 2. Dans la zone **Private Key File**, entrez le chemin de répertoire du fichier de clés. Par défaut, il s'agit de `/opt/qradar/conf/vis.ssh.key`. Si un fichier de clés n'existe pas, vous devez créer le fichier vis.ssh.key.

10. Dans la zone **Remote Folder**, entrez l'emplacement du répertoire des fichiers de résultat de l'analyse.
11. Dans la zone **Remote File Pattern**, entrez l'expression régulière (regex) requise pour filtrer la liste de fichiers spécifiée dans le dossier distant. Tous les fichiers correspondants sont inclus dans le traitement. Le canevas regex par défaut pour extraire des résultats Nmap est `.*\.xml`. Le canevas `.*\.xml` importe tous les fichiers de résultat XML dans le dossier distant. Les rapports d'analyse importés et traités ne sont pas supprimés du dossier distant. Il est conseillé de planifier une tâche périodique pour supprimer les rapports d'analyse déjà traités.
12. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
13. Cliquez sur **Sauvegarder**.
14. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83

Ajout d'une analyse immédiate Nmap distante

QRadar surveille l'état de l'analyse immédiate en cours et attend que le serveur Nmap termine l'analyse. Au terme de l'analyse, les résultats de vulnérabilités sont téléchargés via SSH.

Pourquoi et quand exécuter cette tâche

Plusieurs types d'analyse de port Nmap requièrent que Nmap s'exécute en tant qu'utilisateur root. Par conséquent, QRadar doit avoir accès en tant que root ou vous devez désélectionner la case **OS Detection**. Pour exécuter des analyses Nmap avec l'option OD Detection sélectionnée, vous devez attribuer à QRadar des données d'identification disposant de droits d'accès root lorsque vous ajoutez le scanner. Ou bien vous pouvez demander à votre administrateur de configurer le fichier binaire Nmap avec les droits setuid root. Consultez votre administrateur Nmap pour plus d'informations.

Restriction : Même si chaque hôte QRadar dispose d'un NMap binaire, celui-ci est uniquement destiné à un usage interne de QRadar. La configuration d'un scanner de vulnérabilité NMap dans le but d'utiliser une console QRadar Console ou un hôte géré QRadar en tant que scanner NMap distant n'est pas prise en charge et peut entraîner des instabilités.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Nmap.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Nmap Scanner**.
7. Dans la liste **Scan Type**, sélectionnez **Remote Live Scan**.
8. Dans la zone **Server Hostname**, entrez l'adresse IP ou le nom d'hôte du serveur Nmap.
9. Choisissez l'une des options d'authentification suivantes :

Option	Description
Server Username	Pour s'authentifier avec un nom d'utilisateur et un mot de passe, procédez comme suit : 1. Dans la zone **Server Username**, entrez le nom d'utilisateur requis pour accéder au système distant hébergeant le client Nmap utilisant SSH. 2. Dans la zone **Login Password**, entrez le mot de passe associé au nom d'utilisateur. Si la case **OS Detection** est cochée, l'utilisateur doit disposer de privilèges root.

Option	Description
Enable Key Authorization	Pour s'authentifier avec un fichier d'authentification basé clés, procédez comme suit : 1. Cochez la case **Enable Key Authentication**. 2. Dans la zone **Private Key File**, entrez le chemin de répertoire du fichier de clés. Le répertoire par défaut du fichier de clés est : `/opt/qradar/conf/vis.ssh.key`. Si un fichier de clés n'existe pas, vous devez créer le fichier vis.ssh.key. Si le scanner est configuré pour utiliser un mot de passe, le serveur du scanner SSH qui se connecte à QRadar doit prendre en charge l'authentification par mot de passe. Si ce n'est pas le cas, l'authentification par SSH du scanner échoue. Vérifiez que la ligne suivante figure dans votre fichier `/etc/ssh/sshd_config` : `PasswordAuthentication yes`. Si le serveur de votre scanner n'utilise pas OpenSSH, consultez dans la documentation de son fournisseur les informations de configuration du scanner.

10. Dans la zone **Nmap Executable**, entrez le chemin d'accès complet du répertoire et le nom de fichier du fichier binaire Nmap. Le chemin de répertoire par défaut du fichier binaire est : `/usr/bin/Nmap`.
11. Sélectionnez une option pour la case à cocher **Disable Ping**. Dans certains réseaux, le protocole ICMP est partiellement ou complètement désactivé. Si ICMP n'est pas activé, vous pouvez sélectionner cette case pour désactiver des commandes PING ICMP afin d'affiner l'analyse. Par défaut, la case est décochée.
12. Sélectionnez une option pour la case à cocher **OS Detection**:
    - Cochez cette case pour activer la détection du système d'exploitation dans Nmap. Vous devez accorder au scanner des privilèges root pour utiliser cette option.
    - Décochez cette case pour recevoir les résultats Nmap sans détection du système d'exploitation.
13. Dans la liste **Max RTT Timeout**, sélectionnez une valeur de délai d'attente. Le délai d'attente détermine si une analyse doit être arrêtée ou réexécutée en raison du temps d'attente entre le scanner et la cible d'analyse. La valeur par défaut est de 300 millisecondes (ms). Si vous spécifiez un délai d'expiration de 50 millisecondes, nous suggérons que les périphériques analysés résident sur le réseau local. Les dispositifs sur des réseaux distants peuvent utiliser une valeur de délai d'expiration d'1 seconde.
14. Sélectionnez une option dans la liste **Timing Template**. Les options incluent :
    - Paranoid - Cette option produit une évaluation lente et non intrusive.
    - Sneaky - Cette option produit une évaluation lente et non intrusive, mais patiente 15 secondes entre les analyses.
    - Polite - Cette option est plus lente que la normale et destinée à alléger la charge sur le réseau.
    - Normal - Cette option est le comportement d'analyse standard.
    - Aggressive - Cette option st plus rapide que la normale et plus gourmande en ressources.
    - Insane - Cette option n'est pas aussi précise que les analyses plus lentes et ne convient qu'aux réseaux très rapides.
    -
15. Dans la zone **CIDR Mask**, entrez la taille du sous-réseau analysé. La valeur spécifiée pour le masque représente la portion la plus large du sous-réseau que le scanner peut analyser à un moment donné. Le masque segmente l'analyse afin d'optimiser les performances de l'opération.

16. Pour configurer une plage CIDR pour votre scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
17. Cliquez sur **Sauvegarder**.
18. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83

18 Présentation du scanner de vulnérabilité Outpost24

IBM Security QRadar utilise le protocole HTTPS pour communiquer avec l'API du scanner de vulnérabilité Outpost24 et télécharger des données d'actif et de vulnérabilité dans des analyses précédemment effectuées.

Le tableau suivant répertorie les spécifications concernant le scanner de vulnérabilité Outpost24 :

Tableau 3. Spécifications du scanner de vulnérabilité Outpost24

Spécification	**Valeur**
Nom du scanner	Scanner de vulnérabilité Outpost24
Versions prises en charge	HIAB V4.1 OutScan V4.1
Type de connexion	HTTPS
Informations complémentaires	Site de Outpost24 (http://www.outpost24.com/)

Certificats serveur

Avant d'ajouter un scanner, un certificat serveur est requis pour prendre en charge les connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : `.crt`, `.cert` ou `.der`. Pour copier un certificat dans le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat dans le répertoire `/opt/qradar/conf/trusted_certificates` via SCP (Secure Copy) ou SFTP (Secure File Transfer Protocol).
- Pour télécharger automatiquement le certificat dans le répertoire `/opt/qradar/conf/trusted_certificates`, connectez-vous via SSH à la console ou à l'hôte géré et saisissez la commande suivante :

  `/opt/qradar/bin/getcert.sh <adresse_IP_ou_nom_hôte> <port_facultatif_(valeur_par_défaut_443)>`.

Installation de Java Cryptography Extension illimité

Les certificats par défaut utilisés par OUTSCAN et HIAB ont recours à des clés de 2048 Bits. Par conséquent, vous devez modifier la cryptographie Java lorsque vous utilisez ces certificats. Pour plus d'informations, voir «Installation du module Java Cryptography Extension Unlimited», à la page 1.

Etapes de configuration

Pour configurer QRadar et télécharger des données d'actif et de vulnérabilité dans un scanner de vulnérabilité Outpost24, procédez comme suit.

1. Si les mises à jour automatiques ne sont pas activées, téléchargez et installez la plus récente version du RPM du scanner de vulnérabilité Outpost 24 sur votre système QRadar.
2. Sur celui-ci, créez un jeton d'application pour QRadar.
3. Sur QRadar Console, ajoutez le scanner. Configurez tous les paramètres requis et utilisez le tableau suivant pour identifier les valeurs spécifiques à Outpost24 :

Tableau 4. Paramètres du scanner de vulnérabilité Outpost24

Paramètre	**Valeur**
Type	Scanner de vulnérabilité Outpost24

Tableau 4. Paramètres du scanner de vulnérabilité Outpost24 (suite)

Paramètre	Valeur
Server Hostname	Nom d'hôte ou adresse IP du scanner de vulnérabilité Outpost24.
Port	443
API token	Le jeton d'API créé sur le scanner Outpost24 doit être utilisé.

4. Planifiez une analyse.

Tâches associées:

«Création d'un jeton d'authentification d'API Outpost24 pour QRadar»
Pour activer IBM Security QRadar afin d'utiliser l'API Outpost24 et télécharger des données d'actif et de vulnérabilité, créez un jeton d'accès à une application sur le scanner de vulnérabilité Outpost24.

24, «Planification d'une analyse de vulnérabilité», à la page 83
Les planifications d'analyse sont des intervalles affectés aux scanners et qui déterminent quand des données d'évaluation de vulnérabilités doivent être importées depuis vos dispositifs d'analyse sur votre réseau. Les planifications d'analyse peuvent également définir les plages CIDR ou les sous-réseaux à inclure dans l'importation des données lors de l'importation des données de vulnérabilité.

Création d'un jeton d'authentification d'API Outpost24 pour QRadar

Pour activer IBM Security QRadar afin d'utiliser l'API Outpost24 et télécharger des données d'actif et de vulnérabilité, créez un jeton d'accès à une application sur le scanner de vulnérabilité Outpost24.

Procédure

1. Connectez-vous au scanner de vulnérabilité Outpost24.
2. Sélectionnez **Settings > Account**.
3. Cliquez sur l'onglet **Security Policy**.
4. Dans le panneau Application Access Tokens, cliquez sur **New**.
5. Dans la fenêtre Maintaining App Access Token, vérifiez que la case **Active** est sélectionnée.
6. Entrez un nom pour l'application, comme par exemple QRadar.
7. Configurez les restrictions IP ainsi que les droits d'accès utilisateur.
8. Cliquez sur **Save**.
9. Copiez le jeton d'authentification à 64 caractères dans un fichier.

Que faire ensuite

Sur le système QRadar, ajoutez le scanner de vulnérabilité Outpost24.

19 Positive Technologies MaxPatrol

Vous pouvez ajouter un scanner Positive Technologies MaxPatrol à votre déploiement IBM Security QRadar.

A chaque intervalle déterminé par une planification d'analyse, QRadar importe des résultats de fichiers XML qui contiennent des vulnérabilités MaxPatrol. Le scanner MaxPatrol importe des fichiers d'un serveur distant qui contient les données d'analyse exportées.

Le tableau suivant fournit des détails sur le scanner Positive Technologies MaxPatrol :

Tableau 5. Détails du scanner Positive Technologies MaxPatrol

Fournisseur	Positive Technologies
Nom du scanner	MaxPatrol
Versions prises en charge	Version 8.24.4 et versions suivantes

Utilisez les procédures ci-après pour intégrer Positive Technologies MaxPatrol à QRadar.

1. Configurez votre scanner Positive Technologies MaxPatrol pour l'exportation des rapports d'analyse. Activez les exportations de vulnérabilité de fichier XML compatible QRadar. Pour obtenir les fichiers nécessaires et les procédures de configuration, contactez le support client de Positive Technologies.
2. Sur votre console QRadar, ajoutez un scanner Positive Technologies MaxPatrol.
3. Sur votre console QRadar, créez une planification d'analyse pour importer vos données de résultats d'analyse.

Intégration de Positive Technologies MaxPatrol à QRadar

Procédures qui sont requises pour intégrer Positive Technologies MaxPatrol à QRadar.

Procédure

1. Configurez votre scanner Positive Technologies MaxPatrol pour l'exportation des rapports d'analyse. Activez les exportations de vulnérabilité de fichier XML compatible QRadar. Pour obtenir les fichiers nécessaires et les procédures de configuration, contactez le support client de Positive Technologies.
2. Sur votre console QRadar, ajoutez un scanner Positive Technologies MaxPatrol.
3. Sur votre console QRadar, créez une planification d'analyse pour importer vos données de résultats d'analyse.

Ajout d'un scanner Positive Technologies MaxPatrol

Ajoutez un scanner Positive Technologies MaxPatrol à votre déploiement IBM Security QRadar.

Avant de commencer

Assurez-vous que les prérequis suivants sont respectés : .

- Le système Positive Technologies MaxPatrol est configuré pour l'exportation des rapports de vulnérabilité XML compatible QRadar.
- Un partage SFTP ou SMB est configuré et contient les rapports de vulnérabilité XML exportés.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les paramètres de scanner Positive Technologies MaxPatrol lorsque vous sélectionnez SFTP comme méthode d'importation :

Tableau 6. Propriétés SFTP du scanner Positive Technologies MaxPatrol

Paramètre	Description
Remote Hostname	Adresse IP ou nom d'hôte du serveur qui a le fichier de résultats d'analyse.
Login Username	Nom d'utilisateur que QRadar utilise pour la connexion au serveur.
Enable Key Authentication	Indique que QRadar s'authentifie avec un fichier d'authentification par clé.
Remote directory	Emplacement des fichiers de résultat d'analyse.
Private Key File	Chemin d'accès complet au fichier qui contient la clé privée. Si un fichier de clés n'existe pas, vous devez créer le fichier `vis.ssh.key`.
File Name Pattern	Expression régulière (regex) requise pour filtrer la liste de fichiers spécifiée dans le répertoire distant. Le canevas `.*\.xml` importe tous les fichiers XML dans le répertoire distant.

Le tableau suivant décrit les paramètres de scanner Positive Technologies MaxPatrol lorsque vous sélectionnez SMB Share comme méthode d'importation :

Tableau 7. Propriétés SMB Share du scanner Positive Technologies MaxPatrol

Paramètre	Description
Hostname	Adresse IP ou nom d'hôte de SMB Share.
Login Username	Nom d'utilisateur que QRadar utilise pour la connexion à SMB Share.
Domain	Domaine qui est utilisé pour la connexion à SMB Share.
SMB Folder Path	Chemin d'accès complet au partage depuis a racine de l'hôte SMB. Utilisez les barres obliques, par exemple `/share/logs/`.
File Name Pattern	Expression régulière (regex) requise pour filtrer la liste de fichiers spécifiée dans le répertoire distant. Le canevas `.*\.xml` importe tous les fichiers xml dans le répertoire distant.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant le scanner Positive Technologies MaxPatrol.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner.
6. Dans la liste **Type**, sélectionnez **Positive Technologies MaxPatrol Scanner**.
7. Configurez les paramètres ci-après.
8. Configurez une plage CIDR pour le scanner.
9. Cliquez sur **Sauvegarder**.

10. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Pour plus d'informations sur la création d'une planification d'analyse, voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

20 Présentation du scanner Qualys

QRadar peut extraire des informations sur les vulnérabilités via l'API Host Detection List de QualysGuard ou télécharger directement des rapports d'analyse directement depuis un dispositif QualysGuard. Vous pouvez intégrer QRadar à des dispositifs QualysGuard qui utilisent la version 4.7 jusqu'à la version 8.1.

Scanners Qualys Detection

Ajoutez un scanner de détection Qualys si vous voulez utiliser l'interface de programme d'application (API) Host Detection List de QualysGuard pour analyser plusieurs rapports d'analyse afin de collecter les données de vulnérabilité des actifs. Les données retournées par la requête contiennent les vulnérabilités comme les numéros d'identification, que QRadar compare à la base de connaissances de vulnérabilités Qualys la plus récente. Le scanner de détection Qualys ne gère pas les analyses immédiates mais peut extraire des informations de vulnérabilités agrégées de rapports d'analyse multiples. QRadar prend en charge les paramètres de recherche clés permettant de filtrer les informations que vous voulez collecter. Vous pouvez aussi configurer la fréquence à laquelle QRadar extrait et met en cache la base de connaissances de vulnérabilités Qualys.

Scanners Qualys

Ajoutez un scanner Qualys si vous voulez importer des rapports immédiats ou importés spécifiques qui incluent des données d'analyse ou d'actif. Lorsque vous ajoutez un scanner Qualys, vous avez le choix entre les types de collection suivants :

- Rapport d'analyse planifiée immédiate.
- Importation planifiée de rapport de données d'actif
- Importation planifiée de rapport d'analyse

Installation du certificat Qualys

Avant de pouvoir vous connecter à Qualys, vous devez télécharger le certificat Qualys dans IBM Security QRadar.

Pourquoi et quand exécuter cette tâche

Un certificat serveur est requis pour prendre en charge les connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : .crt, .cert ou .der. Des certificats peuvent être copiés manuellement dans le répertoire `/opt/qradar/conf/trusted_certificates` de QRadar via SCP ou SFTP. Toutefois, vous pouvez également télécharger le certificat Qualys à partir d'une URL client.

Procédure

1. Contactez Qualys pour obtenir une URL client et vos données d'identification de connexion. Pour plus d'information sur la connexion à Qualys, voir www.qualys.com/support (https://www.qualys.com/support/faq/login/).
2. Téléchargez le certificat en tapant la commande suivante :
   `/opt/qradar/bin/getcert.sh <URL_client>`
3. Copiez le certificat téléchargé dans le répertoire `/opt/qradar/conf/trusted_certificates`.

Ajout d'un scanner de détection Qualys

Ajoute un scanner de détection Qualys pour l'utilisation d'une API permettant d'interroger plusieurs rapports d'analyse afin de collecter les données de vulnérabilité pour les actifs. Le scanner de détection Qualys utilise l'interface de programme d'application (API) QualysGuard Host Detection List.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner de détection Qualys.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner.
6. Dans la liste **Type**, sélectionnez **Qualys Detection Scanner**.
7. Configurez les paramètres suivants :

Paramètre	Description
Qualys Server Host Name	Nom de domaine complet ou adresse IP de la console de gestion QualysGuard. Si vous entrez le nom de domaine complet, le nom d'hôte et non l'URL, par exemple, saisissez `qualysapi.qualys.com` ou `qualysapi.qualys.eu`.
Qualys Username	L'utilisateur que vous indiquez doit disposer d'un accès pour télécharger Qualys KnowledgeBase. Pour plus d'informations sur la mise à jour de l'abonnement Qualys, reportez-vous à la documentation Qualys.
Qualys Password	Mot de passe de connexion à Qualys
Operating System Filter	Expression régulière (regex) permettant de filtrer les données d'analyse par système d'exploitation.
Asset Group Names	Liste séparée par des virgules pour interroger les adresses IP d'après le nom de groupe.
Host Scan Time Filter (Days)	Les dates antérieures au nombre de jours spécifié sont exclues des résultats renvoyés par Qualys.
Qualys Vulnerability Retention Period (Days)	Nombre de jours pendant lequel QRadar doit stocker la base de connaissances de vulnérabilités Qualys. Si une analyse est planifiée après l'expiration de la période de conservation, le système télécharge une mise à jour.
Force Qualys Vulnerability Update	Force le système à mettre à jour la base de connaissances de vulnérabilités Qualys la plus récente pour chaque analyse planifiée.

8. Pour configurer un proxy, cochez la case **Use Proxy** et configurez les données d'identification pour le serveur proxy.
9. Pour configurer un certificat client, cochez la case **Use Client Certificate** et configurez la zone **Certificate File Path** et les zones **Certificate Password**.
10. Pour configurer une plage CIDR pour votre scanner, configurez les paramètres de plage CIDR et cliquez sur **Add**.

    Restriction : L'API QualysGuard Host Detection List n'accepte les plages CIDR que dans la limite d'une seule classe A ou /8 et ne doit pas englober l'adresse IP de l'hôte local (127.0.0.1) ou 0.0.0.0.
11. Cliquez sur **Sauvegarder**.
12. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**. Les changements apportés à la configuration de proxy requièrent une opération **Déployer la configuration entière**.

Ajout d'une analyse planifiée Qualys immédiate

Ajoutez une analyse en continu planifiée pour lancer les analyses préconfigurées sur le scanner Qualys, puis collectez les résultats d'analyse terminés.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Qualys.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner.
6. Dans la liste **Type**, sélectionnez **Qualys Scanner**.
7. Configurez les paramètres suivants :

Paramètre	Description
Qualys Server Host Name	Nom de domaine complet ou adresse IP de la console de gestion QualysGuard. Si vous entrez le nom de domaine complet, le nom d'hôte et non l'URL, par exemple, saisissez `qualysapi.qualys.com` ou `qualysapi.qualys.eu`.
Qualys Username	L'utilisateur que vous indiquez doit disposer d'un accès pour télécharger Qualys KnowledgeBase. Pour plus d'informations sur la mise à jour de l'abonnement Qualys, reportez-vous à la documentation Qualys.
Qualys Password	Mot de passe de connexion à Qualys

8. Facultatif : Pour configurer un proxy, cochez la case **Use Proxy** et configurez les données d'identification pour le serveur proxy.
9. Facultatif : Pour configurer un certificat client, sélectionnez la case à cocher **Use Client Certificate** et configurez la zone **Certificate File Path** et les zones **Certificate Password**.
10. Dans la liste **Collection Type**, sélectionnez **Scheduled Live - Scan Report**.
11. Configurez les paramètres suivants :

Paramètre	Description
Scanner Name	Pour obtenir le nom du scanner, contactez votre administrateur réseau. Le dispositif d'analyse publique doit effacer le nom de cette zone.
Option Profiles	Nom du profil d'option qui détermine l'analyse en continu qui est lancée. Les analyses opérationnelles prennent en charge un nom de profil d'option pour chaque configuration de scanner.

12. Facultatif : Pour configurer une plage CIDR pour votre scanner, configurez les paramètres de plage CIDR et cliquez sur **Ajouter**.
13. Facultatif : Pour permettre à QRadar de créer des vulnérabilités personnalisées depuis les données d'analyse en continu, cochez la case **Enable Custom Vulnerability Creation** et choisissez les options que vous voulez inclure.
14. Cliquez sur **Sauvegarder**.
15. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**. Les changements apportés à la configuration de proxy requièrent une opération **Déployer la configuration entière**.

Ajout d'une importation planifiée de rapport sur les actifs de Qualys

Ajoutez une importation de données de rapport sur les actifs afin de planifier l'extraction par QRadar d'un rapport unique sur les actifs à partir de votre scanner Qualys.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Qualys.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner.
6. Dans la liste **Type**, sélectionnez **Qualys Scanner**.
7. Configurez les paramètres suivants :

Paramètre	Description
Qualys Server Host Name	Nom de domaine complet ou adresse IP de la console de gestion QualysGuard. Si vous entrez le nom de domaine complet, le nom d'hôte et non l'URL, par exemple, saisissez `qualysapi.qualys.com` ou `qualysapi.qualys.eu`.
Qualys Username	L'utilisateur que vous indiquez doit disposer d'un accès pour télécharger Qualys KnowledgeBase. Pour plus d'informations sur la mise à jour de l'abonnement Qualys, reportez-vous à la documentation Qualys.
Qualys Password	Mot de passe de connexion à Qualys

8. Facultatif : Pour configurer un proxy, cochez la case **Use Proxy** et configurez les données d'identification pour le serveur proxy.
9. Facultatif : Pour configurer un certificat client, sélectionnez la case à cocher **Use Client Certificate** et configurez la zone **Certificate File Path** et les zones **Certificate Password**.
10. Dans la liste **Collection Type**, sélectionnez **Scheduled Import - Asset Data Report**.
11. Configurez les paramètres suivants :

Paramètre	Description
Report Template Title	Titre du modèle de rapport remplaçant le titre de rapport de données d'actif par défaut.
Max Reports Age (Days)	Les fichiers plus anciens que le nombre de jours et l'horodatage spécifiés dans le fichier de rapport sont exclus lorsque l'analyse planifiée est lancée.
Import File	Chemin de répertoire pour le téléchargement et l'importation d'un rapport d'actif unique depuis Qualys. Si vous spécifiez un emplacement de fichier d'importation, QRadar télécharge le contenu du fichier d'actif depuis Qualys vers un répertoire local et importe le fichier. Si vous laissez cette zone vide ou si le fichier ou le répertoire est introuvable, le scanner Qualys utilise l'API pour extraire le rapport sur les actifs à l'aide de la valeur de la zone **Report Template Title**.

12. Facultatif : Pour configurer une plage CIDR pour votre scanner, configurez les paramètres de plage CIDR et cliquez sur **Ajouter**.
13. Facultatif : Pour permettre à QRadar de créer des vulnérabilités personnalisées depuis les données d'analyse en continu, cochez la case **Enable Custom Vulnerability Creation** et choisissez les options que vous voulez inclure.

14. Cliquez sur **Sauvegarder**.
15. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**. Les changements apportés à la configuration de proxy requièrent une opération **Déployer la configuration entière**.

Ajout d'une importation planifiée de rapport d'analyse Qualys

Ajoutez une importation de données de rapport d'analyse pour planifier l'extraction par QRadar de rapports d'analyse depuis votre scanner Qualys.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner Qualys.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré qui gère l'importation du scanner.
6. Dans la liste **Type**, sélectionnez **Qualys Scanner**.
7. Configurez les paramètres suivants :

Paramètre	Description
Qualys Server Host Name	Nom de domaine complet ou adresse IP de la console de gestion QualysGuard. Si vous entrez le nom de domaine complet, le nom d'hôte et non l'URL, par exemple, saisissez `qualysapi.qualys.com` ou `qualysapi.qualys.eu`.
Qualys Username	L'utilisateur que vous indiquez doit disposer d'un accès pour télécharger Qualys KnowledgeBase. Pour plus d'informations sur la mise à jour de l'abonnement Qualys, reportez-vous à la documentation Qualys.
Qualys Password	Mot de passe de connexion à Qualys

8. Facultatif : Pour configurer un proxy, cochez la case **Use Proxy** et configurez les données d'identification pour le serveur proxy.
9. Facultatif : Pour configurer un certificat client, sélectionnez la case à cocher **Use Client Certificate** et configurez la zone **Certificate File Path** et les zones **Certificate Password**.
10. Dans la liste **Collection Type**, sélectionnez **Scheduled Import - Scan Report**.
11. Configurez les paramètres suivants :

Paramètre	Description
Option Profiles	Nom du profil d'option pour déterminer l'analyse à lancer. QRadar récupère les données complètes de l'analyse opérationnelle après que celle-ci soit terminée. Les analyses opérationnelles prennent en charge un nom de profil d'option par configuration de scanner.
Scan Report Name Pattern	Expression régulière (regex) requise pour filtrer la liste des rapports d'analyse.
Max Reports Age (Days)	Les fichiers plus anciens que le nombre de jours et l'horodatage spécifiés dans le fichier de rapport sont exclus lorsque l'analyse planifiée est lancée.

Paramètre	Description
Import File	Chemin de répertoire pour le téléchargement et l'importation d'un rapport d'analyse unique depuis Qualys, par exemple, `/qualys_logs/test_report.xml`. Si vous spécifiez un emplacement de fichier d'importation, QRadar télécharge le contenu du fichier d'actif depuis Qualys vers un répertoire local et importe le fichier. Si vous laissez cette zone à blanc ou si le fichier ou répertoire est introuvable, le scanner Qualys utilise l'API pour extraire le rapport d'actif à l'aide de la valeur de la zone **Options Profile**.

12. Facultatif : Pour configurer une plage CIDR pour votre scanner, configurez les paramètres de plage CIDR et cliquez sur **Ajouter**.
13. Facultatif : Pour permettre à QRadar de créer des vulnérabilités personnalisées depuis les données d'analyse en continu, cochez la case **Enable Custom Vulnerability Creation** et choisissez les options que vous voulez inclure.
14. Cliquez sur **Sauvegarder**.
15. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**. Toute modification du proxy requiert une opération **Déployer la configuration entière**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

21 Présentation du scanner Rapid7 Nexpose

Les scanners Rapid7 Nexpose peuvent fournir à QRadar des rapports de données sur des sites afin d'importer les vulnérabilités identifiées sur votre réseau.

Les options suivantes sont disponibles pour collecter des informations de vulnérabilité depuis des scanners Rapid7 Nexpose :

- Importation d'un rapport ad hoc sur des sites via l'API Rapid7. Voir «Ajout d'une importation des résultats d'un scanner Rapid7 Nexpose sur des sites via une API», à la page 72.
- Importation d'un fichier local sur un site. Voir «Ajout d'une importation de fichier local de scanner Rapid7 Nexpose»
- Importation d'un fichier distant sur un site. Voir «Ajout d'une importation de fichier distant de scanner Rapid7 Nexpose», à la page 73

Ajout d'une importation de fichier local de scanner Rapid7 Nexpose

QRadar utilise des fichiers locaux pour importer les données de vulnérabilité de votre scanner Rapid7 Nexpose.

Avant de commencer

Avant d'ajouter ce scanner, vérifiez que vous possédez un certificat serveur qui prend en charge les connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : *.crt, *.cert ou *.der. Pour copier un certificat vers le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat vers le répertoire `/opt/qradar/conf/trusted_certificates` via SCP ou SFTP.
- Utilisez SSH pour vous connecter à la console ou à l'hôte géré et extrayez le certificat à l'aide de la commande suivante : `/opt/qradar/bin/getcert.sh <adresse IP ou nom d'hôte> <port facultatif - 443 par défaut>`. Un certificat est alors téléchargé du nom d'hôte ou de l'IP spécifié, et placé dans le répertoire `/opt/qradar/conf/trusted_certificates` dans le format approprié.

Pourquoi et quand exécuter cette tâche

Les importations de fichier local collectent des vulnérabilités concernant un site depuis un fichier local qui est téléchargé. Le fichier XML Rapid7 Nexpose contenant les informations sur le site et les vulnérabilités détectées doit être copié depuis votre dispositif Rapid7 Nexpose vers la console ou l'hôte géré que vous avez spécifié lors de l'ajout du scanner à QRadar. Le répertoire de destination sur l'hôte géré ou la console doit exister pour que le dispositif Rapid7 Nexpose puisse copier les rapports du site. Les fichiers du site peuvent être copiés sur l'hôte géré ou la console via SCP (Secure Copy) ou SFTP (Secure File Transfer Protocol).

Vous devez définir l'utilisateur VIS comme propriétaire du répertoire d'importation créé sur l'hôte géré ou QRadar Console avec les droits appropriés dans QRadar. Par exemple, la commande `chown -R vis:qradar <chemin_répertoire_importation>` et `chmod 755 <chemin_répertoire_importation>` définit l'utilisateur VIS comme propriétaire du chemin de répertoire d'importation avec les droits read-write-execute appropriés.

Remarque : Les fichiers de site importés ne sont pas supprimés du dossier d'importation mais renommés en `.processed0`. Les administrateurs peuvent créer un travail périodique (cron) pour supprimer les fichiers de site déjà traités.

Procédure

1. Cliquez sur **Admin** > **Configuration système**.
2. Cliquez sur l'icône **Scanners VA**. puis cliquez sur **Ajouter**.
3. Tapez un **nom du scanner** pour identifier votre scanner Rapid7 Nexpose.
4. Sélectionnez l'**hôte géré** de votre déploiement QRadar qui gère l'importation de scanner.
5. Dans la liste **Type**, sélectionnez **Rapid7 Nexpose Scanner**.
6. Dans la liste **Import Type**, sélectionnez **Import Site Data - Local File**.
7. Dans la zone **Import Folder**, entrez le chemin de répertoire des données de vulnérabilité XML. Si vous spécifiez un dossier d'importation, vous devez déplacer vos données de vulnérabilité depuis votre scanner Rapid7 Nexpose vers QRadar.
8. Dans la zone **Import File Pattern**, entrez l'expression régulière (regex) requise pour déterminer les fichiers XML Rapid7 Nexpose à inclure dans le rapport d'analyse. Tous les noms de fichier correspondant au masque regex sont inclus lors de l'importation du rapport d'analyse de vulnérabilité. Vous devez spécifier un masque regex valide dans cette zone. La valeur par défaut, `.*\.xml`, importe tous les fichiers depuis le répertoire d'importation.
9. Entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
10. Cliquez sur **Sauvegarder**.
11. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

Ajout d'une importation des résultats d'un scanner Rapid7 Nexpose sur des sites via une API

Les importations via une API permettent à QRadar d'importer des rapports ad hoc de données de vulnérabilité sur vos sites depuis des scanners Rapid7 Nexpose. Les données de site importées dépendent du nom du site.

Avant de commencer

Avant d'ajouter ce scanner, vous devez posséder un certificat serveur qui prend en charge les connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : .crt, .cert ou .der. Pour copier un certificat vers le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat vers le répertoire `/opt/qradar/conf/trusted_certificates` via SCP ou SFTP.
- Lancez SSH sur la console ou l'hôte géré et extrayez le certificat à l'aide de la commande suivante : `/opt/qradar/bin/getcert.sh <IP ou nom d'hôte> <port facultatif - 443 par défaut>`. Un certificat est alors téléchargé du nom d'hôte ou de l'IP spécifié, et placé dans le répertoire `/opt/qradar/conf/trusted_certificates` dans le format approprié.

Procédure

1. Cliquez sur **Admin** > **Configuration système**.
2. Cliquez sur l'icône **Scanners VA**. puis cliquez sur **Ajouter**.
3. Tapez un **nom du scanner** pour identifier votre scanner Rapid7 Nexpose.
4. Sélectionnez l'**hôte géré** de votre déploiement QRadar qui gère l'importation de scanner.
5. Dans la liste **Type**, sélectionnez **Rapid7 Nexpose Scanner**.

6. Dans la liste **Import Type**, sélectionnez l'une des options suivantes :
   - **Import Site Data - Asset and Vulnerability data via SQL API** - Option par défaut. Choix recommandé pour l'importation des résultats.
   - **Import Site Data - Adhoc Report via API**
7. Dans la zone **Remote Hostname**, entrez l'adresse IP ou le nom d'hôte du scanner Rapid7 Nexpose.
8. Dans la zone **Login Username**, entrez le nom d'utilisateur utilisé pour accéder au scanner Rapid7 Nexpose. Les informations de connexion doivent correspondre à un utilisateur valide. Le *nom d'utilisateur* peut être obtenu depuis l'interface utilisateur Rapid7 Nexpose ou auprès de l'administrateur Rapid7 Nexpose.
9. Dans la zone **Login Password**, entrez le mot de passe requis pour accéder au scanner Rapid7 Nexpose.
10. Dans la zone **Port**, entrez le port utilisé pour se connecter à la console de sécurité de Rapid7 Nexpose. Le numéro de port est le même que celui qui est utilisé pour se connecter à l'interface utilisateur de Rapid7 Nexpose.
11. Dans la zone **Site Name Pattern**, entrez l'expression régulière (regex) requise pour déterminer les sites Rapid7 Nexpose à inclure dans l'analyse. Tous les sites qui correspondent au masque sont inclus lorsque le programme d'analyse démarre. La valeur par défaut de l'expression régulière est `.*`, ce qui importe tous les noms de site.
12. Dans la zone **Cache Timout (Minutes)**, indiquez la durée pendant laquelle les données du dernier rapport d'analyse généré doivent être conservées en cache. Si le délai d'expiration de conservation en cache a expiré, de nouvelles données de vulnérabilité sont réclamées à l'API lorsque l'analyse planifiée est lancée.
13. Entrez le chemin du répertoire local à utiliser pour stocker les rapports XML téléchargés.
14. Pour configurer une plage CIDR pour le scanner, procédez comme suit :
    a. Dans la zone, entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
15. Cliquez sur **Sauvegarder**.
16. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

Ajout d'une importation de fichier distant de scanner Rapid7 Nexpose

QRadar utilise des fichiers distants pour importer les données de vulnérabilité du scanner Rapid7 Nexpose.

Avant de commencer

Avant d'ajouter ce scanner, vérifiez que vous possédez un certificat serveur qui prend en charge les connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : .crt, .cert ou .der. Pour copier un certificat dans le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat vers le répertoire `/opt/qradar/conf/trusted_certificates` via SCP ou SFTP.
- Utilisez SSH pour vous connecter à la console ou à l'hôte géré et extrayez le certificat à l'aide de la commande suivante : `/opt/qradar/bin/getcert.sh <adresse IP ou nom d'hôte> <port facultatif - 443 par défaut>`. Un certificat est alors téléchargé du nom d'hôte ou de l'IP spécifié, et placé dans le répertoire `/opt/qradar/conf/trusted_certificates` dans le format approprié.

Pourquoi et quand exécuter cette tâche

Les importations de fichier distant collectent des vulnérabilités d'un site depuis un fichier distant téléchargé. Le fichier XML Rapid7 Nexpose contenant les informations sur le site et les vulnérabilités détectées doit être copié depuis votre dispositif Rapid7 Nexpose vers la console ou l'hôte géré que vous avez spécifié lors de l'ajout du scanner à QRadar. Le répertoire de destination sur l'hôte géré ou la console doit exister pour que le dispositif Rapid7 Nexpose puisse copier les rapports du site. Les fichiers du site peuvent être copiés sur l'hôte géré ou la console via SCP (Secure Copy) ou SFTP (Secure File Transfer Protocol).

Vous devez définir l'utilisateur VIS comme propriétaire du répertoire d'importation créé sur l'hôte géré ou QRadar Console avec les droits appropriés dans QRadar. Par exemple, la commande `chown -R vis:qradar <chemin_répertoire_importation>` et `chmod 755 <chemin_répertoire_importation>` définit l'utilisateur VIS comme propriétaire du chemin de répertoire d'importation avec les droits read-write-execute appropriés.

Remarque : Les fichiers de site importés ne sont pas supprimés du dossier d'importation mais renommés en `.processed0`. Les administrateurs peuvent créer un travail périodique (cron) pour supprimer les fichiers de site déjà traités.

Procédure

1. Cliquez sur **Admin** > **Configuration système**.
2. Cliquez sur l'icône **Scanners VA**. puis cliquez sur **Ajouter**.
3. Tapez un **nom du scanner** pour identifier votre scanner Rapid7 Nexpose.
4. Sélectionnez l'**hôte géré** de votre déploiement QRadar qui gère l'importation de scanner.
5. Dans la liste **Type**, sélectionnez **Rapid7 Nexpose Scanner**.
6. Dans la liste **Import Type**, sélectionnez **Import Site Data - Remote File**.
7. Entrez le **nom d'hôte distant** du serveur qui possède les fichiers de résultats d'analyse et le **port distant** du serveur SSH distant.
8. Entrez le nom d'utilisateur et le mot de passe du serveur SSH distant.
9. Facultatif : Activez l'authentification par clé, puis entrez le chemin local complet de la clé privée SSH.
10. Indiquez l'emplacement du répertoire distant qui contient les résultats d'analyse du serveur SSH distant.
11. Dans la zone **File Name Pattern**, entrez l'expression régulière (regex) requise pour déterminer les fichiers XML Rapid7 Nexpose à inclure dans le rapport d'analyse. Tous les noms de fichier correspondant au masque regex sont inclus lors de l'importation du rapport d'analyse de vulnérabilité. Vous devez spécifier un masque regex valide dans cette zone. La valeur par défaut, `.*\.xml`, importe tous les fichiers depuis le répertoire d'importation.
12. Entrez le nombre maximal de jours pour l'utilisation du fichier de rapport. Les fichiers antérieurs à ce nombre de jours ne sont pas traités. Indiquez 0 si souhaitez désactiver la vérification de la date du rapport.
13. Configurez une plage CIDR pour le scanner :
    a. Dans la zone, entrez la plage CIDR que ce scanner doit prendre en compte ou cliquez sur **Parcourir** pour sélectionner une plage CIDR dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
14. Cliquez sur **Sauvegarder**.
15. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

22 Présentation du scanner SAINT

Les administrateurs peuvent intégrer leurs scanners de vulnérabilité SAINT (Security Administrator's Integrated Network Tool) avec QRadar dans le cas de dispositifs SAINT avec niveau de logiciel V7.4.x.

Les administrateurs peuvent ajouter des scanners SAINT à QRadar pour collecter des données de vulnérabilité SAINT sur des hôtes, y-compris des informations sur les adresses Mac, les ports et les services concernés. Le scanner SAINT identifie des vulnérabilités compte tenu du niveau d'analyse spécifié et utilise SAINTwriter pour générer des rapports personnalisés. Par conséquent, votre système peut inclure un modèle de rapport SAINTwriter personnalisé et des analyses qui s'exécutent régulièrement pour garantir que ses résultats sont à jour.

Les types de collecte de données suivants sont pris en charge pour les configurations de scanner SAINT :

- Analyse immédiate - Lance une analyse à distance sur le scanner SAINT. L'analyse immédiate génère un rapport de vulnérabilité basé sur le nom de la session et ce rapport est importé à l'issue de l'analyse.
- Rapport uniquement - Importe du scanner SAINT des rapports terminés basés sur le nom de la session.

Pour configurer un modèle pour votre rapport, voir «Configuration d'un modèle SAINTwriter».

Configuration d'un modèle SAINTwriter

Un modèle doit être configuré dans SAINTwriter avant que les administrateurs puissent ajouter et importer des vulnérabilités depuis un scanner SAINT.

Procédure

1. Connectez-vous à l'interface utilisateur SAINT.
2. Dans le menu de navigation, sélectionnez **Data** > **SAINTwriter**.
3. Cliquez sur **Report Type**.
4. Dans la liste **Type**, sélectionnez **Custom**.
5. Dans la zone **File Name**, entrez le nom d'un fichier de configuration.

   Le nom du fichier de configuration créé doit être utilisé lorsque vous ajoutez le scanner SAINT à QRadar.
6. Dans la liste **Template Type**, sélectionnez **Technical Details**.
7. Cliquez sur **Continue**.
8. Sélectionnez **Lists**.
9. Dans la liste **Columns to include in host**, modifiez toutes les colonnes indiquant None par **MAC address**.
10. Dans la liste **Columns to include in vulnerability**, modifiez toutes les colonnes indiquant None par **Port**.
11. Dans la liste **Columns to include in vulnerability**, modifiez toutes les colonnes indiquant None par **Service**.
12. Cliquez sur **Save**.

Que faire ensuite

Vous pouvez à présent ajouter une configuration d'analyse à QRadar pour le scanner SAINT. Voir «Ajout d'une analyse de vulnérabilité SAINT», à la page 78.

Ajout d'une analyse de vulnérabilité SAINT

Les administrateurs peuvent ajouter une configuration de scanner SAINT afin de collecter des rapports spécifiques ou de lancer des analyses sur le scanner distant.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant votre scanner SAINT.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **SAINT Scanner**.
7. Dans la zone **Remote Hostname**, entrez l'adresse IP ou le nom d'hôte du scanner SAINT.
8. Choisissez l'une des options d'authentification suivantes :

Option	Description
Login Username	Pour s'authentifier avec un nom d'utilisateur et un mot de passe, procédez comme suit : 1. Dans la zone **Login Username**, entrez un nom d'utilisateur autorisé à accéder à l'hôte distant. 2. Dans la zone **Login Password**, entrez le mot de passe associé au nom d'utilisateur.
Enable Key Authorization	Pour s'authentifier avec un fichier d'authentification basé clés, procédez comme suit : 1. Cochez la case **Enable Key Authentication**. 2. Dans la zone **Private Key File**, entrez le chemin de répertoire du fichier de clés. Le répertoire par défaut du fichier de clés est : `/opt/qradar/conf/vis.ssh.key`. Si un fichier de clés n'existe pas, vous devez créer le fichier vis.ssh.key.

9. Dans la zone **SAINT Base Directory**, entrez le chemin du répertoire d'installation du scanner SAINT.
10. Dans la zone **Scan Type**, sélectionnez l'une des options suivantes :
    - Live Scan - Lance une analyse de vulnérabilité pour générer des données de rapport basées sur le nom de la session.
    - Report Only - Génère un rapport d'analyse basé sur le nom de la session.
11. Pour les configurations **Live Scan**, sélectionnez une option pour la case à cocher **Ignore Existing Data**.
    - Cochez cette case pour forcer l'analyse immédiate à collecter de nouvelles données de vulnérabilité depuis le réseau. Cette option supprime toutes les données du dossier de session avant que l'analyse immédiate ne débute.
    - Décochez cette case pour permettre à l'analyse immédiate d'utiliser les données existantes dans le dossier de session.
12. Dans la liste **Scan Level**, sélectionnez un niveau d'analyse. Les options incluent :
    - Vulnerability Scan - analyse de toutes les vulnérabilités.
    - Port Scan - analyse des services TCP ou UDP à l'écoute sur le réseau.
    - PCI Compliance Scan - analyse des ports et des services avec accent sur la conformité DSS PCI.

- SANS Top 20 Scan - analyse des 20 vulnérabilités de sécurité les plus graves.
- FISMA Scan - analyse de toutes les vulnérabilités, couvrant également toutes les analyses personnalisées et tous les niveaux PCI.

13. Dans la zone **Session Name**, entrez le nom de session pour la configuration du scanner SAINT.
14. Dans la zone **SAINT Writer Config**, entrez le nom du fichier de configuration SAINTwriter.
15. Pour configurer une plage CIDR pour le scanner, procédez comme suit :
    a. Dans la zone de texte, entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
16. Cliquez sur **Sauvegarder**.
17. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

23 Présentation du scanner Tenable SecurityCenter

Un scanner Tenable SecurityCenter peut être utilisé pour planifier et extraire des rapports d'analyses de vulnérabilités ouvertes depuis des scanners de vulnérabilité Nessus sur votre réseau.

Pour configurer un scanner Tenable SecurityCenter, voir «Ajout d'un scanner Tenable SecurityCenter».

Ajout d'un scanner Tenable SecurityCenter

Vous pouvez ajouter un scanner Tenable SecurityCenter pour permettre à IBM Security QRadar de collecter des informations sur les hôtes et la vulnérabilité via l'API Tenable.

Avant de commencer

Vérifiez l'emplacement de l'API sur votre serveur Tenable SecurityCenter.

Un certificat serveur est requis pour prendre en charge les connexions HTTPS. QRadar prend en charge les certificats possédant les extensions de fichier suivantes : .crt, .cert ou .der. Pour copier un certificat vers le répertoire `/opt/qradar/conf/trusted_certificates`, choisissez l'une des options suivantes :

- Copiez manuellement le certificat vers le répertoire `/opt/qradar/conf/trusted_certificates` via SCP ou SFTP.
- Lancez SSH sur la console ou l'hôte géré et extrayez le certificat à l'aide de la commande suivante : `/opt/qradar/bin/getcert.sh <IP ou nom d'hôte> <port facultatif - 443 par défaut>`. Un certificat est alors téléchargé du nom d'hôte ou de l'IP spécifié, et placé dans le répertoire `/opt/qradar/conf/trusted_certificates` dans le format approprié.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Scanners d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la zone **Nom du scanner**, entrez un nom identifiant le scanner.
5. Dans la liste **Hôte géré**, sélectionnez l'hôte géré de votre déploiement QRadar qui gère l'importation de scanner.
6. Dans la liste **Type**, sélectionnez **Tenable SecurityCenter**.
7. Dans la zone **Server Address**, entrez l'adresse IP du serveur Tenable SecurityCenter.
8. Dans la zone **API Location**, entrez le chemin d'accès à l'API sur le serveur Tenable SecurityCenter.

   Le chemin par défaut du fichier API pour SecurityCenter version 4 est `sc4/request.php`.

   Le chemin par défaut du fichier API pour SecurityCenter version 5 est `rest`.
9. Dans la liste **API Version**, sélectionnez la version de votre SecurityCenter. Par exemple, **Version 4** ou **Version 5**.
10. Dans la zone **User Name**, entrez le nom d'utilisateur requis pour accéder à l'API Tenable SecurityCenter.
11. Dans la zone **Password**, entrez le mot de passe requis pour accéder à l'API Tenable SecurityCenter.
12. Configurez une plage CIDR pour le scanner.
    a. Dans la zone des plages CIDR, entrez la plage CIDR pour l'analyse ou cliquez sur **Parcourir** pour la sélectionner dans la liste des réseaux.
    b. Cliquez sur **Ajouter**.
13. Cliquez sur **Sauvegarder**.

14. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Que faire ensuite

Vous pouvez à présent créer une planification d'analyse. Voir 24, «Planification d'une analyse de vulnérabilité», à la page 83.

24 Planification d'une analyse de vulnérabilité

Les planifications d'analyse sont des intervalles affectés aux scanners et qui déterminent quand des données d'évaluation de vulnérabilités doivent être importées depuis vos dispositifs d'analyse sur votre réseau. Les planifications d'analyse peuvent également définir les plages CIDR ou les sous-réseaux à inclure dans l'importation des données lors de l'importation des données de vulnérabilité.

Pourquoi et quand exécuter cette tâche

Des planifications d'analyse sont créées pour chaque produit de scanner dans votre réseau et sont utilisés pour extraire des données de vulnérabilités. Il n'y a aucune limite au nombre de planifications d'analyse que vous pouvez créer. Il est souvent utile de créer plusieurs analyses de vulnérabilités dans votre réseau. Les importations de données de vulnérabilité volumineuses peuvent prendre beaucoup de temps et sollicitent intensément les ressources système. Une analyse ne peut être planifiée qu'après que le scanner a été ajouté.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Planifier un scanner d'analyse des vulnérabilités**.
3. Cliquez sur **Ajouter**.
4. Dans la liste **Scanners d'analyse des vulnérabilités**, sélectionnez le scanner pour lequel vous souhaitez établir une planification d'analyse.
5. Choisissez l'une des options suivantes :

Option	Description
CIDR réseau	Sélectionnez cette option pour définir une plage CIDR pour l'importation des données. Si un scanner inclut plusieurs configurations CIDR, la plage CIDR peut être sélectionnée dans la liste.
Sous-réseau/CIDR	Sélectionnez cette option pour définir un sous-réseau ou une plage CIDR pour l'importation des données. La valeur de sous-réseau/CIDR définie par l'administrateur doit correspondre à un CIDR réseau accessible au scanner.

6. Dans la liste **Priorité**, sélectionnez le niveau de priorité à affecter à l'analyse.

Option	Description
Faible	Indique que l'analyse a une priorité normale. La priorité basse est la valeur d'analyse par défaut.
Elevée	Indique que l'analyse a une priorité élevée. Les analyses de priorité élevée sont toujours placées au-dessus des analyses de priorité basse dans la file d'attente des analyses.

7. Dans la zone **Ports**, entrez les ports inclus dans la planification d'analyse. Les ports ne faisant pas partie du planning ne sont pas inclus dans les données de vulnérabilité. L'administrateur peut

spécifier n'importe quel numéro de port compris entre 1 et 65536. Les valeurs de port individuelles peuvent être spécifiés sous forme de valeurs séparées par des virgules, de pair avec les plages de ports. Par exemple, 21,443, 445, 1024-2048.

8. Sélectionnez l'heure de début du planning.
9. Dans la zone **Intervalle**, entrez un intervalle indiquant la fréquence de répétition de cette analyse. Les planifications d'analyse peuvent contenir des intervalles en heures, jours, semaines ou mois.
10. Sélectionnez **Effacez les ports de vulnérabilité** pour supprimer toutes les vulnérabilités détectées sur chaque ressource et remplacez les données signalées lors de l'exécution d'analyse suivante.
11. Cliquez sur **Sauvegarder**.

25 Affichage de l'état d'une analyse de vulnérabilité

La fenêtre des planifications d'analyse fournit aux administrateurs une vue indiquant pour chaque scanner son calendrier de collecte de données d'évaluation des vulnérabilités pour des actifs du réseau.

Pourquoi et quand exécuter cette tâche

Le nom de chaque analyse est affiché, avec la plage CIDR, le port ou la plage de ports, la priorité, l'état et l'heure de la prochaine exécution.

Tableau 8. Etat de la planification d'analyse

Nom de la colonne	Description
Scanner d'analyse des vulnérabilités	Affiche le nom de l'analyse planifiée.
CIDR	Affiche les plages d'adresses CIDR incluses dans l'importation de données de vulnérabilité lorsque la planification d'analyse est lancée.
Ports	Affiche les plages de ports incluses dans l'importation de données de vulnérabilité lorsque la planification d'analyse est lancée. Les planifications d'analyse peuvent lancer une analyse distante sur un dispositif de vulnérabilité distant de fournisseurs spécifiques. Par exemple, NMap ou Nessus, ou Nessus Scan Results Importer. Les ports mentionnés dans la colonne Ports sont alors ceux contenus dans l'analyse. Pour la plupart des scanners, la plage de ports n'est pas prise en compte lors de la demande d'informations d'actifs auprès d'un scanner. Par exemple, les scanners nCircle IP360 et Qualys rapportent des vulnérabilités sur tous les ports mais exigent que vous indiquiez des informations de port adéquates afin de récupérer le rapport complet à afficher dans l'interface utilisateur.
Priorité	Affiche la priorité de l'analyse. Les analyses planifiées ayant une priorité élevée sont placées en tête de liste et sont effectuées avant celles avec un faible priorité.
Etat	Affiche l'état actuel de l'analyse. Chaque zone d'état affiche des informations uniques sur l'état de l'analyse. • Les nouvelles analyses peuvent être modifiées tant que leur état n'a pas été modifié. • Les analyses en attente doivent attendre qu'un nouvelle analyse soit terminée. • Les analyses en cours indiquent le pourcentage réalisé avec une infobulle d'informations sur l'importation des données. • Les analyses terminées fournissent un récapitulatif des vulnérabilités importées ou des importations partielles de données qui se sont produites. • Les analyses ayant échoué fournissent un message d'erreur indiquant pourquoi l'importation des vulnérabilités a échoué.
Dernière heure de fin	Indique la dernière fois où l'analyse est parvenue à importer des enregistrements de vulnérabilités pour le planning.
Heure de la prochaine exécution	Affiche le prochain calendrier d'importation de données de vulnérabilité. Les planifications d'analyse indiquant *Never* dans l'interface utilisateur sont des analyses qui ne sont effectuées qu'une seule fois.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Planifier un scanner d'analyse des vulnérabilités**.
3. Examinez la colonne Etat pour déterminer l'état de vos sources de journal.

   La colonne Etat de chaque scanner contient un message d'état indiquant l'aboutissement ou l'échec de chaque importation de vulnérabilité.

26 Scanners de vulnérabilité pris en charge

Les données de vulnérabilité peuvent être collectées via plusieurs fournisseurs et vendeurs de produits de sécurité. Si le scanner déployé dans votre réseau n'est pas répertorié dans ce document, vous pouvez contacter votre ingénieur commercial pour déterminer la prise en charge de votre dispositif.

Tableau 9. Scanners de vulnérabilité pris en charge

Fournisseur	Nom du scanner	Versions prises en charge	Nom de la configuration	Type de connexion
Beyond Security	Automated Vulnerability Detection System (AVDS)	AVDS Management V12 (version mineure 129) et au-dessus	Beyond Security AVDS Scanner	Importation de fichier de données de vulnérabilité avec SFTP
Digital Defense Inc	AVS	N/A	Digital Defense Inc AVS	HTTPS
eEye Digital Security	eEye REM	REM V3.5.6	eEye REM Scanner	Programme d'écoute d'alerte SNMP
	Retina CS eEye	Retina CS V3.0 à V4.0		Requêtes de base de données via JDBC
Générique	Axis	N/A	Axis Scanner	Importation de fichier de données de vulnérabilité avec SFTP
IBM	IBM AppScan Enterprise	Version 8.6	Scanner IBM AppScan	Service Web IBM REST avec HTTP ou HTTPS
IBM	InfoSphere Guardium	Version 9.0 et versions suivantes	Scanner IBM Guardium SCAP	Importation de fichier de données de vulnérabilité avec SFTP
IBM	BigFix	V8.2x à V9.5.2	IBM BigFix Scanner	API SOAP avec HTTP ou HTTPS
IBM	InfoSphere SiteProtector	Version 2.9.x	Scanner IBM SiteProtector	Requêtes de base de données via JDBC
IBM	Tivoli Endpoint Manager Désormais appelé IBM BigFix			
Juniper Networks	NetScreen Security Manager (NSM) Profiler	2007.1r2	Juniper NSM Profiler Scanner	Requêtes de base de données via JDBC
		2007.2r2		
		2008.1r2		
		2009r1.1		
		2010.x		
McAfee	Vulnerability Manager	V6.8	McAfee Vulnerability Manager	API SOAP avec HTTPS
		V7.0		Importation de fichier XML
		V7.5		
Microsoft	Microsoft System Center Configuration Manager (SCCM)	Microsoft Windows	Microsoft SCCM	DCOM doit être configuré et activé
nCircle ou Tripwire	IP360	VnE Manager V6.5.2 à V6.8.28	nCircle ip360 Scanner	Importation de fichier de données de vulnérabilité avec SFTP
netVigilance	SecureScout	V2.6	SecureScout Scanner	Requêtes de base de données via JDBC
Open source	NMap	V3.7 à V6.0	NMap Scanner	Importation de fichier de données de vulnérabilité via SFTP avec exécution de commande SSH
Outpost24	Outpost24	HIAB V4.1 OutScan V4.1	Outpost24	API sur HTTPS
Positive Technologies	MaxPatrol	Version 8.24.4 et versions suivantes	Positive Technologies MaxPatrol	SFTP ou SMB Share
Qualys	QualysGuard	V4.7 à V8.1	Scanner Qualys	APIv2 sur HTTPS
Qualys	QualysGuard	V4.7 à V8.1	Scanner Qualys Detection	API de liste de détection d'hôte via HTTPS
Rapid7	NeXpose	V4.x à V6.3.3	Scanner Rapid7 NeXpose	Appel de procédure à distance via HTTPS
				Importation dans un répertoire local de fichier XML via SCP ou SFTP

Tableau 9. Scanners de vulnérabilité pris en charge (suite)

Fournisseur	Nom du scanner	Versions prises en charge	Nom de la configuration	Type de connexion
Saint Corporation	Security Administrator's Integrated Network Tool (SAINT)	V7.4.x	Saint Scanner	Importation de fichier de données de vulnérabilité via SFTP avec exécution de commande SSH
Tenable Network Security	SecurityCenter	Version 4 et Version 5	Tenable SecurityCenter	Requête JSON avec HTTPS
Tenable Network Security	Nessus	Linux V4.0.2 à V4.4.x Microsoft Windows V4.2 à V4.4.x	Nessus Scanner	Importation de fichiers via SFTP avec exécution de commande SSH
		Linux V4.2 à V5.x Microsoft Windows V4.2 à V5.x		XML-RPC API sur HTTPS

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 éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

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

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance 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 de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

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

Dispositions pour la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Domaine d'application

Ces dispositions s'ajoutent aux conditions d'utilisation relatives au site Web IBM.

Usage personnel

Vous pouvez reproduire ces informations 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.

Usage commercial

Vous pouvez reproduire, distribuer et publier ces informations uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces informations en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement express d'IBM.

Droits

Excepté les droits d'utilisation expressément accordés dans le présent document, aucun autre droit, licence ou autorisation, implicite 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 session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

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

Politique de confidentialité

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 session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

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

Index