IBM QRadar Vulnerability Manager
Version 7.4.0

Guide d'utilisation

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 143.

Ce document s'applique à IBM® QRadar Security Intelligence Platform version 7.4.0 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

© Copyright IBM France 2020. Tous droits réservés.

© Copyright International Business Machines Corporation 2012, 2020.

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.

© Copyright IBM Corp. 2012, 2020

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

Brevets

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

Assistance téléphonique

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

Présentation d'IBM QRadar Vulnerability Manager

Ces informations portent sur l'utilisation d'IBM QRadar Vulnerability Manager. QRadar Vulnerability Manager est une plateforme d'analyse qui permet d'identifier, de gérer et de hiérarchiser les vulnérabilités des actifs de réseau.

Ce guide contient des instructions pour configurer et utiliser QRadar Vulnerability Manager sur un IBM QRadar SIEM ou une console IBM QRadar Log Manager.

Utilisateurs concernés

Les administrateurs système responsables de la configuration d'IBM QRadar Vulnerability Manager doivent disposer d'un accès administratif à IBM QRadar SIEM ainsi qu'à tous vos périphériques réseau et pare-feu. Ils doivent également maîtriser votre réseau d'entreprise et connaître vos technologies de réseau.

Documentation technique

Pour savoir comment accéder à plus de documentation technique, aux notes techniques et aux notes sur l'édition, voir la note technique Accessing IBM Security Documentation (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

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

Bonnes pratiques de sécurité

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention, la détection et la réponse aux accès non autorisés au sein comme à l'extérieur de votre entreprise. Un accès non autorisé peut se traduire par la modification, la destruction, ou une utilisation inadéquate ou malveillante de vos systèmes, y compris l'utilisation de ces derniers pour attaquer d'autres systèmes. Aucun système ou produit informatique ne doit être considéré comme totalement sécurisé et aucun produit ou mesure de sécurité ne peut être à lui seul entièrement efficace pour empêcher un accès inapproprié. Les systèmes et les produits IBM sont conçus pour s'intégrer à une approche de sécurité complète, ce qui implique nécessairement des procédures opérationnelles supplémentaires, et ils peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, DES PRODUITS ET DES SERVICES, NI CELLE DE VOTRE ENTREPRISE, CONTRE LES CONDUITES MALVEILLANTES OU ILLICITES DE TIERS.

© Copyright IBM Corp. 2012, 2020

Chapitre 1. Nouveautés pour les utilisateurs de QRadar Vulnerability Manager version 7.4.0

QRadar Vulnerability Manager version 7.4.0 inclut désormais un nouveau paramètre de recherche permettant d'identifier les vulnérabilités controversées ainsi que les améliorations apportées aux exceptions de vulnérabilité.

Paramètres de recherche des vulnérabilités controversées

QRadar Vulnerability Manager version 7.4.0 inclut de nouveaux paramètres de recherche qui optimisent les données de vulnérabilité extraites de plusieurs scanners. Les paramètres **Trouvé par scanner** et **Non trouvé par scanner** offrent les avantages suivants :

- Réduction de la redondance d'ensemble de données via la suppression des vulnérabilités en double.
- Amélioration de la qualité des données en réduisant les faux positifs potentiels.
- Comparaison des vulnérabilités détectées par plusieurs scanners afin d'améliorer les techniques d'analyse et d'identifier les failles.

Amélioration des exceptions de vulnérabilité

Dans QRadar Vulnerability Manager version 7.4.0, la limitation qui permettait aux utilisateurs de créer des exceptions uniquement pour une instance de vulnérabilité d'une règle d'exception a été supprimée. Vous pouvez désormais créer des règles qui incluent des exceptions pour plusieurs vulnérabilités.

Pour plus d'informations, voir le document *IBM QRadar Vulnerability Manager - Guide d'utilisation*.

© Copyright IBM Corp. 2012, 2020

Chapitre 2. Installations et déploiements

En fonction du produit que vous installez et selon que vous décidez de mettre à niveau IBM QRadar ou d'installer un nouveau système, l'onglet **Vulnérabilités** peut ne pas s'afficher.

Vous pouvez accéder à IBM® Security QRadar Vulnerability Manager à l'aide de l'onglet Vulnérabilités :

- Si vous installez QRadar SIEM, l'onglet **Vulnérabilités** est activé par défaut avec une clé de licence temporaire.
- Si vous installez QRadar Log Manager, l'onglet **Vulnérabilités** n'est pas activé. Vous pouvez acheter la licence de QRadar Vulnerability Manager séparément ou l'activer à l'aide d'une clé de licence.

Pour plus d'informations sur la mise à niveau, voir le document *IBM QRadar - Guide de mise à niveau*.

Licence QRadar Vulnerability Manager

Pour utiliser QRadar Vulnerability Manager après une installation ou une mise à niveau, vous devez télécharger une clé de licence valide et l'allouer. Pour plus d'informations, voir le *Guide d'administration*. La licence QRadar Vulnerability Manager est appliquée et traitée en temps réel sur les actifs analysés de QRadar Vulnerability Manager ayant au moins une adresse IP. L'analyse QRadar Vulnerability Manager doit s'effectuer pendant la durée de conservation configurée pour l'adresse IP de l'actif.

1. Dans l'onglet **Admin**, cliquez sur **Configuration du profileur d'actif**
2. Recherchez la ligne **Conservation des IP d'actif (en jours)** pour éditer la valeur de conservation des adresses IP d'actifs.
3. Modifiez la valeur de conservation ou vérifiez qu'elle correspond à vos besoins. La valeur de conservation des adresses IP d'actifs par défaut est de 120 jours.

Licences QRadar Vulnerability Manager et QRadar Risk Manager

IBM QRadar Vulnerability Manager et IBM QRadar Risk Manager sont rassemblés sous la même offre et dépendent de la même licence de base. L'offre combinée fournit un flux de travaux intégré d'analyse réseau et de gestion des vulnérabilités. La licence de base vous autorise à utiliser QRadar Vulnerability Manager pour analyser jusqu'à 256 actifs. Vous pouvez intégrer à QRadar Risk Manager jusqu'à 50 sources de configuration standard. L'autorisation d'utiliser QRadar Vulnerability Manager ou QRadar Risk Manager vous donne automatiquement droit à la licence de base de l'autre produit. Vous devez être titulaire de licences supplémentaires pour analyser plus de 256 actifs ou intégrer plus de 50 sources de configuration.

Déploiement des composants d'analyse et de traitement des vulnérabilités

Lorsque vous installez QRadar Vulnerability Manager sous licence, un processeur de vulnérabilité est déployé automatiquement sur votre console QRadar. Ce déploiement n'a pas lieu si vous utilisez une clé d'activation logicielle sur votre console QRadar.

Le processeur de vulnérabilité fournit par défaut un composant d'analyse. Si nécessaire, vous pouvez déployer des programmes d'analyse supplémentaires vers des dispositifs de programmes d'analyse d'hôtes gérés QRadar Vulnerability Manager dédiés ou des hôtes gérés QRadar. Par exemple, vous pouvez déployer un scanner de vulnérabilité vers un Event Collector ou un QRadar QFlow Collector,

Si nécessaire, vous pouvez déplacer le processeur de vulnérabilité vers un autre hôte géré dans votre déploiement afin, par exemple, de conserver de l'espace disque sur votre console QRadar.

Restriction : Un seul processeur de vulnérabilité est autorisé dans votre déploiement. Vous pouvez déplacer le processeur de vulnérabilité uniquement vers un dispositif de processeur dédié QRadar Vulnerability Manager. Vous ne pouvez pas ajouter un processeur de vulnérabilité à l'appareil QRadar Flow Processor 1728.

© Copyright IBM Corp. 2012, 2020

Vous pouvez ajouter le processeur de vulnérabilité aux appareils suivants QRadar : 600, 700, 8099, 8024, 8000, 3124, 8026, 2100, 3199, 3126, 8021 et 3100.

Mises à jour automatiques et informations de vulnérabilité

L'exécution de la fonction de mise à jour automatique vous permet de disposer des métadonnées de vulnérabilité et des outils d'analyse les plus récents. Configurez vos mises à jour automatiques via une connexion Internet ou à partir d'un serveur hors ligne local. Généralement, les métadonnées de vulnérabilité et les outils d'analyse sont mis à jour une fois par semaine.

Nous vous recommandons d'exécuter les mises à jour automatiques après l'installation d'une mise à jour logicielle QRadar. Exécutez la mise à jour automatique sous l'onglet **Admin**, en cliquant sur l'icône **Mise à jour automatique**.

Pour en savoir plus sur l'installation des mises à jour automatiques de QRadar, voir le manuel *IBM QRadar Administration Guide*.

Concepts associés

Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager

Options de déplacement du processeur de vulnérabilité dans votre déploiement QRadar Vulnerability Manager

Processeur de vulnérabilité et clés d'activation de dispositif de programme d'analyse

Vous pouvez analyser et traiter vos vulnérabilités à l'aide de dispositifs d'hôtes gérés QRadar Vulnerability Manager dédiés.

Lorsque vous installez un processeur ou un dispositif d'hôte géré de programme d'analyse, vous devez entrer une clé d'activation valide.

Pour plus d'informations sur l'installation d'un dispositif hôte gérée, voir le *Guide d'administration* de votre produit.

La clé d'activation est une chaîne alphanumérique à quatre parties de 24 chiffres que vous recevez d'IBM. La clé d'activation indique les modules de logiciel qui s'appliquent à chaque type de dispositif :

- Le dispositif de processeur QRadar Vulnerability Manager inclut les composants de traitement et d'analyse des vulnérabilités.
- Le dispositif de programme d'analyse QRadar Vulnerability Manager inclut uniquement un composant d'analyse des vulnérabilités.

Vous pouvez obtenir la clé d'activation à partir des emplacements suivants :

- Si vous avez acheté un logiciel QRadar Vulnerability Manager ou téléchargé un dispositif virtuel, vous trouverez une liste des clés d'activation dans le document *Getting Started* joint à un e-mail de confirmation. Vous pouvez utiliser ce document pour établir un renvoi avec la référence du dispositif qui vous a été fourni.
- Si vous avez acheté un dispositif qui est préinstallé avec le logiciel QRadar Vulnerability Manager, la clé d'activation est incluse dans votre boîte ou CD d'expédition.

Sauvegarde et récupération des vulnérabilités

Vous pouvez utiliser les fonctions de sauvegarde et de reprise dans IBM QRadar SIEM pour sauvegarder et restaurer les données de vulnérabilité et de configuration d'IBM QRadar Vulnerability Manager.

Lorsque vous installez QRadar Vulnerability Manager, les sauvegardes nocturnes ou à la demande de QRadar SIEM incluent des profils d'analyse, des résultats d'analyse et des informations de configuration QRadar Vulnerability Manager.

Vous pouvez configurer des sauvegardes et des reprises de données ou de configuration dans l'onglet **Admin**.

Pour plus d'informations sur la sauvegarde et la reprise, voir *IBM QRadar Administration Guide*.

Ports utilisés pour la communication entre QRadar et les hôtes gérés QRadar Vulnerability Manager

QRadar Vulnerability Manager utilise des ports sécurisés pour se connecter aux hôtes gérés.

Ports utilisés pour la communication

Le tableau suivant décrit les ports qui sont utilisés pour la communication sécurisée entre QRadar et les hôtes gérés QRadar Vulnerability Manager.

Tableau 1. Ports de communication de QRadar Vulnerability Manager

Communication	Port	Protocole
QRadar Console au processeur QRadar Vulnerability Manager	22, 9999, 8989, 8844	TCP
QRadar Console au scanner QRadar Vulnerability Manager	22	TCP
Processeur QRadar Vulnerability Manager à la console QRadar Console	443	TCP
Scanner QRadar Vulnerability Manager au processeur QRadar Vulnerability Manager	9999	TCP

Options de déplacement du processeur de vulnérabilité dans votre déploiement QRadar Vulnerability Manager

Si nécessaire, vous pouvez déplacer le processeur de vulnérabilité de votre console QRadar vers un dispositif d'hôte géré QRadar Vulnerability Manager dédié.

Par exemple, vous pouvez déplacer la fonction de traitement des vulnérabilités vers un hôte géré afin de réduire l'impact de l'espace disque sur votre console QRadar.

Restriction : Un seul processeur de vulnérabilité est autorisé dans votre déploiement. Par ailleurs, son déploiement n'est permis que sur une console QRadar ou un dispositif de processeur d'hôte géré QRadar Vulnerability Manager.

Pour déplacer le processeur de vulnérabilité, choisissez l'une des options suivantes :

Option 1 : Déploiement d'un dispositif de processeur QRadar Vulnerability Manager dédié

Pour déployer un dispositif de processeur, vous devez exécuter les tâches suivantes :

1. Installez un dispositif de processeur QRadar Vulnerability Manager dédié.
2. Ajoutez le dispositif de processeur d'hôte géré à votre console QRadar Console à l'aide de l'outil **Gestion du système et de la licence** dans l'onglet **Admin**.

   Lorsque vous sélectionnez l'option d'hôte géré, le processeur est automatiquement supprimé de la console QRadar.

Option 2 : Déplacement du processeur de vulnérabilités de la console vers l'hôte géré

Si le processeur de vulnérabilité est installé sur votre console QRadar, vous pouvez le déplacer vers un dispositif de processeur d'hôte géré QRadar Vulnerability Manager précédemment installé.

Vous pouvez à tout moment ramener le processeur de vulnérabilité sur votre console QRadar.

Déploiement d'un dispositif de processeur QRadar Vulnerability Manager dédié

Vous pouvez déployer un dispositif de processeur dédié QRadar Vulnerability Manager en tant qu'hôte géré.

Lorsque vous déployez votre processeur de vulnérabilité sur un hôte géré, toutes les vulnérabilités sont traitées sur l'hôte géré.

Restriction : Une fois que le processeur a été déployé sur un hôte géré QRadar Vulnerability Manager dédié, les profils ou résultats d'analyse qui sont associés à un processeur de la console QRadar ne sont pas affichés. Vous pouvez continuer la recherche et l'affichage des données de vulnérabilité sur les pages **Gérer les vulnérabilités**.

Avant de commencer

Assurez-vous qu'un hôte géré QRadar Vulnerability Manager dédié est installé et qu'une clé d'activation du dispositif de processeur valide est appliquée. Pour plus d'informations, voir le *Guide d'installation* de votre produit.

Procédure

1. Connectez-vous à la console QRadar Console en tant qu'administrateur :

   `https://`*`Adresse_IP_QRadar`*

   Le nom d'utilisateur par défaut est `admin`. Le mot de passe est le mot de passe du compte de l'utilisateur root qui a été entré lors de l'installation.
2. Dans le menu de navigation (☰), cliquez sur **Admin**.
3. Dans le panneau **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. A partir de la table d'hôte, cliquez sur l'hôte QRadar Console et cliquez sur **Actions de déploiement** > **Ajouter l'hôte**.
5. Entrez l'adresse IP et le mot de passe de l'hôte.
6. Pour créer un tunnel SSH sur le port 22, sélectionnez **Chiffrer les connexions hôtes**.
7. Pour activer la compression de chiffrement pour des communications avec un hôte, sélectionnez **Compression de chiffrement**.
8. Pour activer la conversion d'adresse réseau (NAT) pour un hôte géré, sélectionnez **Conversion d'adresses réseau** puis ajoutez les informations suivantes :

Tableau 2. Configuration NAT

Zone	Description
Groupe NAT	Si l'hôte géré se trouve sur le même sous-réseau que la console QRadar Console, sélectionnez la console QRadar Console se trouvant sur le réseau avec conversion d'adresses réseau. Si l'hôte géré ne se trouve pas sur le même sous-réseau que la console QRadar Console, sélectionnez l'hôte géré se trouvant sur le réseau avec conversion d'adresses réseau.

Tableau 2. Configuration NAT (suite)	
Zone	**Description**
Adresse IP publique	L'hôte géré utilise cette adresse IP pour communiquer avec d'autres hôtes gérés sur différents réseaux utilisant la conversion NAT.

Le réseau avec conversion d'adresses réseau doit utiliser la conversion statique d'adresses réseau.

9. Cliquez sur **Ajouter**.

   Remarque : Ne fermez pas la fenêtre tant que le processus d'ajout d'hôte n'est pas terminé.
10. Fermez la fenêtre **Gestion du système et de la licence**.
11. Dans la barre d'outils de l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.
12. Cliquez sur **OK**.

Concepts associés

Processeur de vulnérabilité et clés d'activation de dispositif de programme d'analyse

Tâches associées

Vérification du déploiement d'un processeur de vulnérabilité

Déplacement de votre processeur de vulnérabilité sur un hôte géré ou une console

Si nécessaire, vous pouvez déplacer votre processeur de vulnérabilité entre un dispositif d'hôte géré QRadar Vulnerability Manager et votre console QRadar.

Avant de commencer

Assurez-vous qu'un hôte géré QRadar Vulnerability Manager dédié est installé et qu'une clé d'activation du dispositif de processeur valide est appliquée.

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
3. Cliquez sur **Activer le processeur**.
4. Sélectionnez l'hôte géré ou la console dans la liste **Processeur**.

   Si votre processeur se trouve sur l'hôte géré, vous ne pouvez sélectionner que la console QRadar.
5. Cliquez sur **Sauvegarder**.
6. Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.
7. Cliquez sur **OK**.

   Après avoir modifié le déploiement de votre processeur de vulnérabilité, vous devez attendre la fin de la configuration de votre déploiement. Sur la page **Profils d'analyse**, le message suivant s'affiche : **QVM is in the process of being deployed.**

Concepts associés

Processeur de vulnérabilité et clés d'activation de dispositif de programme d'analyse

Vérification du déploiement d'un processeur de vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez vérifier que votre processeur de vulnérabilité est déployé sur une console QRadar ou un hôte géré QRadar Vulnerability Manager.

Procédure

1. Connectez-vous à la console QRadar.

2. Dans le menu de navigation (☰), cliquez sur **Admin**.
3. Cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
4. Vérifiez que le processeur est affiché sur la liste **Processeurs**.

Suppression d'un processeur de vulnérabilité d'une console ou d'un hôte géré

Si nécessaire, vous pouvez supprimer le processeur de vulnérabilité à partir d'une console QRadar ou d'un hôte géré QRadar Vulnerability Manager.

Procédure

1. Connectez-vous à la console QRadar.
2. Dans le menu de navigation (☰), cliquez sur **Admin**.
3. Cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gestion du déploiement de vulnérabilité**.
4. Cochez la case **Activer le processeur** pour la désélectionner.
5. Cliquez sur **Retirer**.
6. Cliquez sur **Sauvegarder**.
7. Fermez la fenêtre **Gestion du système et de la licence**.
8. Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.
9. Cliquez sur **OK**.

Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager

Si vous disposez d'un grand réseau qui nécessite des options d'analyse souples, vous pouvez ajouter des programmes d'analyse supplémentaires à votre déploiement IBM QRadar Vulnerability Manager.

Votre processeur QRadar Vulnerability Manager est automatiquement déployé avec un composant d'analyse. En déployant davantage de programmes d'analyse, vous bénéficiez d'une plus grande flexibilité pour effectuer vos opérations d'analyse. Par exemple, vous pouvez analyser des zones spécifiques de votre réseau avec des programmes d'analyse distincts et à des heures planifiées différentes.

Analyses de vulnérabilité dynamiques

Il peut arriver que les programmes d'analyse des vulnérabilités déployés n'aient pas accès à toutes les zones de votre réseau. Dans QRadar Vulnerability Manager, vous pouvez affecter différents programmes d'analyse aux plages CIDR réseau. Lors d'une analyse, chaque actif de la plage CIDR à analyser est associée dynamiquement au programme d'analyse approprié.

Pour ajouter d'autres programmes d'analyse des vulnérabilités, choisissez l'une des options suivantes :

Déployez un dispositif de programme d'analyse d'hôte géré QRadar Vulnerability Manager dédié.
Vous pouvez rechercher les vulnérabilités à l'aide d'un dispositif de scanner d'hôte géré QRadar Vulnerability Manager dédié.

Pour déployer un dispositif de scanner, vous devez exécuter les tâches suivantes :

1. Installez un dispositif de scanner d'hôte géré QRadar Vulnerability Manager dédié.
2. Ajoutez le dispositif de scanner d'hôte géré à votre console QRadar Console à l'aide de l'outil **Gestion du système et de la licence** dans l'onglet **Admin**.

Déployez un programme d'analyse QRadar Vulnerability Manager à la console ou à l'hôte géré QRadar.

Si vous déplacez votre processeur de vulnérabilité de votre console QRadar vers un hôte géré QRadar Vulnerability Manager, vous pouvez ajouter un scanner sur votre console.

Vous pouvez également ajouter un scanner de vulnérabilité à un des hôtes gérés QRadar suivants : QRadar Console, Event Processor, Flow Processor, Combo Processor, Event Collector, QFlow Collector et Data Node.

Remarque : Le scanner de vulnérabilité peut pas être ajouté à App Host, App Node et à QRadar Network Insights.

Exécutez une mise à jour automatique lorsque vous ajoutez un scanner ou d'autres hôtes gérés avec des fonctions d'analyse. Pour en savoir plus sur les mises à jour automatiques, voir le *Guide d'administration* d'*IBM Security QRadar*.

Configurez l'accès à un programme d'analyse hébergé par IBM et analysez votre zone démilitarisée.

Vous pouvez configurer l'accès à un scanner hébergé IBM et analyser les actifs de votre zone démilitarisée.

Concepts associés

Analyses de vulnérabilité dynamiques

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse afin d'utiliser certains programmes d'analyse des vulnérabilités pour des plages CIDR spécifiques dans votre réseau. Par exemple, vos programmes d'analyse pourraient n'avoir accès qu'à certaines zones de votre réseau.

Tâches associées

Association de programmes d'analyse des vulnérabilités à des plages CIDR

Dans IBM QRadar Vulnerability Manager, pour effectuer une analyse dynamique, vous devez associer des programmes d'analyse des vulnérabilités à différents segments de votre réseau.

Analyse de plages CIDR avec différents programmes d'analyse des vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez analyser des zones de votre réseau avec différents programmes d'analyse des vulnérabilités.

Déploiement d'un dispositif de programme d'analyse QRadar Vulnerability Manager dédié

Vous pouvez déployer un dispositif de programme d'analyse d'hôte géré QRadar Vulnerability Manager dédié.

Avant de commencer

Assurez-vous qu'un dispositif de programme d'analyse d'hôte géré QRadar Vulnerability Manager dédié est installé et qu'une clé d'activation du dispositif valide est appliquée.

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Ajouter un hôte géré**.
3. Entrez l'adresse IP de l'hôte et le mot de passe du dispositif de scanner de l'hôte géré QRadar Vulnerability Manager.
4. Cliquez sur **Ajouter**.

   Vous devez attendre quelques minutes que l'hôte géré soit ajouté.
5. Fermez la fenêtre **Gestion du système et de la licence**.
6. Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.
7. Cliquez sur **OK**.

Concepts associés

Processeur de vulnérabilité et clés d'activation de dispositif de programme d'analyse

Déploiement d'un scanner de vulnérabilité vers une console ou un hôte géré QRadar

Vous pouvez déployer un scanner QRadar Vulnerability Manager vers une console QRadar ou un hôte géré QRadar. Par exemple, vous pouvez déployer un scanner sur un collecteur de flux, un processeur de flux, un collecteur d'événements, un processeur d'événements ou un nœud de données.

Avant de commencer

Dans un déploiement All-in-One, le contrôleur est utilisé comme scanner intégré. Vous ne pouvez pas ajouter de dispositif de scanner distinct à une console QRadar Console lorsque le processeur QRadar Vulnerability Manager se trouve sur la console QRadar Console. Dans un déploiement autre qu'un déploiement All-in-One, il est recommandé de déplacer le processeur QRadar Vulnerability Manager sur un dispositif dédié lorsque vous analysez plus de 50000 actifs.

Pour déployer un programme d'analyse sur votre console QRadar, assurez-vous que le processeur de vulnérabilité a été déplacé vers un dispositif d'hôte géré QRadar Vulnerability Manager dédié.

Avant de déployer des programmes d'analyse sur des hôtes gérés QRadar, vérifiez d'abord que ces hôtes existent. Pour plus d'informations, voir le *Guide d'installation* de votre produit.

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
3. Cliquez sur **Ajouter des scanners de vulnérabilité supplémentaires**.
4. Cliquez sur l'icône **+**.
5. Dans la liste **Hôte**, sélectionnez l'hôte ou la console géré QRadar.

   Restriction : L'ajout d'un programme d'analyse à une console QRadar n'est pas autorisé si le processeur de vulnérabilité réside sur la console. Vous devez déplacer le processeur de vulnérabilité sur un hôte géré QRadar Vulnerability Manager.
6. Cliquez sur **Sauvegarder**.
7. Fermez la fenêtre **Gestion du système et de la licence**.
8. Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.
9. Cliquez sur **OK**.
10. Vérifiez la liste **Serveur d'analyse** dans la page **Scan Profiles Configuration** pour vous assurer que le scanner est ajouté.

    Pour plus d'informations, voir «Création d'un profil d'analyse», à la page 39.

Que faire ensuite

Exécutez une mise à jour automatique après avoir ajouté le scanner ou d'autres hôtes gérés avec des fonctions d'analyse. Vous pouvez également procéder à une analyse après que la mise à jour automatique quotidienne s'est exécutée. Si les mises à jour automatiques d'autres scanners ont déjà été effectuées, les mises à jour automatiques de tous les scanners peuvent ne pas être complètement synchronisées avant la prochaine mise à jour quotidienne.

Tâches associées

Déplacement de votre processeur de vulnérabilité sur un hôte géré ou une console

Analyse des actifs de votre zone démilitarisée

Dans IBM QRadar Vulnerability Manager, vous pouvez vous connecter à un programme d'analyse externe et analyser les actifs de votre zone démilitarisée afin de détecter des vulnérabilités.

Pour analyser les actifs dans DMZ afin de détecter des vulnérabilités, il n'est pas nécessaire de déployer un programme d'analyse dans votre DMZ. Vous devez configurer QRadar Vulnerability Manager à l'aide d'un programme d'analyse IBM hébergé qui se trouve à l'extérieur de votre réseau.

Les vulnérabilités détectées sont traitées par le processeur sur votre console QRadar ou sur un hôte géré QRadar Vulnerability Manager.

Procédure

1. Configurez votre réseau et vos actifs pour les analyses externes.
2. Configurez QRadar Vulnerability Manager pour analyser vos actifs externes.

Information associée

QRadar Vulnerability Manager - Nouvelle analyse externe / Adresses d'analyse de zone démilitarisée

Configuration de votre réseau et de vos actifs pour des analyses externes

Pour analyser les actifs d'un réseau de zone démilitarisée, vous devez configurer votre réseau et indiquer à IBM quels actifs vous souhaitez analyser.

Pourquoi et quand exécuter cette tâche

Pour analyser les actifs d'un réseau de zone démilitarisée, vous devez effectuer les actions suivantes :

1. Configurer le réseau.
2. Envoyer les caractéristiques du réseau requises à l'équipe externe en charge de l'analyse.

Configuration du réseau pour les analyses externes

Pour analyser les actifs d'un réseau de zone démilitarisée, vous devez tout d'abord configurer votre réseau pour les analyses externes.

Procédure

1. Vérifiez que le processeur QRadar Vulnerability Manager dispose d'un accès Internet pour permettre les communications avec le programme d'analyse de zone démilitarisée.

   Remarque : Une adresse IP statique est requise.
2. Vérifiez que chaque actif qui doit être analysé par le programme d'analyse de zone démilitarisée dispose d'un accès Internet.
3. Configurez une règle de pare-feu sortant pour le port 443 afin d'autoriser une connexion au programme d'analyse de zone démilitarisée.

   Conseil : Les connexions entrantes ne sont pas requises.
4. Placez sur liste blanche `external-scanner.qradar.ibmcloud.com` dans les systèmes d'intrusion réseau afin de permettre la transparence de certificat de bout en bout entre le processeur QRadar Vulnerability Manager et le programme d'analyse de zone démilitarisée.

Envoi des caractéristiques du réseau requises à l'équipe externe en charge de l'analyse

Une fois que vous avez configuré votre réseau pour les analyses externes, vous devez indiquer à IBM les actifs que vous souhaitez analyser.

Procédure

Envoyez les caractéristiques du réseau suivantes à l'équipe externe en charge de l'analyse, à l'adresse QRadar-QVM-Hosted-Scanner@hursley.ibm.com.

Option	Description
Adresse IP de passerelle	Adresse IP externe/publique du processeur QRadar Vulnerability Manager (provenance de l'analyse). Si vous utilisez un serveur proxy, indiquez à la place l'adresse IP du serveur proxy.
Equilibreurs de charge (élément facultatif)	Si vous utilisez des équilibreurs de charge, une liste explicite ou la plage de tous les équilibreurs de charge est requise.
Plage/liste d'adresse IP	Plage/liste explicite de tous les actifs à analyser.

Restriction : Les analyses externes/de zone démilitarisée n'aboutissent pas tant que les informations demandées ne sont pas envoyées à QRadar-QVM-Hosted-Scanner@hursley.ibm.com et qu'aucun message de confirmation n'est reçu.

Information associée

QRadar Vulnerability Manager - Nouvelle analyse externe / Adresses d'analyse de zone démilitarisée

Configuration de QRadar Vulnerability Manager pour analyser vos actifs externes

Pour analyser les actifs dans votre zone démilitarisée, vous devez configurer QRadar Vulnerability Manager à l'aide de l'outil **Gestion du système et de la licence** dans l'onglet **Admin**.

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Cliquez sur **Configuration système**.
3. Cliquez sur **Gestion du système et de la licence**.
4. Dans le menu **Afficher**, sélectionnez **Systèmes**.
5. Cliquez sur **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
6. Cliquez sur **Utiliser le scanner externe**.
7. Dans la zone **IP de la passerelle**, entrez l'adresse IP externe.

   Restriction : Vous ne pouvez pas analyser les actifs externes tant que votre adresse IP externe n'est pas configurée. Vérifiez que vous avez bien envoyé les informations détaillées de votre adresse IP externe à IBM.
8. Si votre réseau est configuré pour utiliser un serveur proxy, cliquez sur **Activer le serveur proxy**, entrez les détails de votre serveur.
9. Cliquez sur **Enregistrer**, puis sur **Fermer**.
10. Dans la barre d'outils de l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.
11. Cliquez sur **OK**.

    Remarque : Aucune analyse authentifiée n'est effectuée depuis le scanner externe.

Information associée

QRadar Vulnerability Manager - Nouvelle analyse externe / Adresses d'analyse de zone démilitarisée

Navigateurs Web pris en charge

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

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

Tableau 3. Navigateurs Web pris en charge par les produits QRadar

Navigateur Web	Versions prises en charge
Mozilla Firefox 64 bits	60 Extended Support Release et versions ultérieures
Microsoft Edge 64 bits	38.14393 et versions ultérieures
Google Chrome 64 bits	Dernière version disponible

Le navigateur Web Microsoft Internet Explorer n'est plus pris en charge depuis QRadar version 7.4.0.

Certificats et exceptions de sécurité

Si vous utilisez le navigateur Web Mozilla Firefox, vous devez ajouter une exception à Mozilla Firefox pour pouvoir vous connecter à QRadar SIEM. Pour plus d'informations, voir la documentation de votre navigateur Web Mozilla Firefox.

Navigation dans l'application Web

Lorsque vous utilisez QRadar, utilisez les options de navigation disponibles dans l'interface utilisateur de QRadar au lieu du bouton **Retour** de votre navigateur.

Activation du mode document et du mode navigateur dans Internet Explorer

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

Procédure

1. Dans votre navigateur Web Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre des **Developer Tools**.
2. Cliquez sur **Browser Mode** et sélectionnez la version de votre navigateur Web.
3. Cliquez sur **Document Mode** et sélectionnez **Internet Explorer standards** pour votre version d'Internet Explorer.

Analyses à haute disponibilité QRadar Vulnerability Manager

Utilisez un déploiement à haute disponibilité (HA) QRadar pour gérer votre planning d'analyse des vulnérabilités, en cas d'échec du déploiement de QRadar.

Le système à haute disponibilité version 2 est pris en charge dans QRadar Vulnerability Manager.

Vous devez utiliser des dispositifs identiques avec des configurations logicielles identiques dans votre système à haute disponibilité. Pour plus d'informations sur la configuration d'un déploiement à haute disponibilité, voir le document *IBM QRadar High Availability Guide*.

Analyses à haute disponibilité

Les dispositifs suivants sont pris en charge dans un déploiement à haute disponibilité QRadar Vulnerability Manager :

- Console
- Dispositif de scanner (610)
- Dispositif de processeur (600)

Remarques importantes

Prenez en compte les informations suivantes lorsque vous déployez une analyse de la vulnérabilité à haute disponibilité (HA) :

- Annulez et redémarrez les analyses après un basculement si ces dernières étaient au cours au moment du basculement.
- Si vous remplacez un dispositif dans votre environnement d'analyse à haute disponibilité, il peut ne pas apparaître dans le déploiement. Vous devez ajouter à nouveau le dispositif au déploiement à haute disponibilité puis déployer les modifications.
- Utilisez des configurations et des dispositifs identiques dans votre configuration à haute disponibilité.
- Les mises à jour automatiques interrompues ne reprennent pas après un basculement. Vous devez exécuter une mise à jour automatique dans une configuration active ininterrompue.

Extension de la période de licence temporaire QRadar Vulnerability Manager

Par défaut, lorsque vous installez IBM QRadar SIEM, vous pouvez voir l'onglet **Vulnérabilités** car une clé de licence temporaire est également installée. Lorsque la licence temporaire expire, vous pouvez prolonger de quatre semaines supplémentaires.

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Cliquez sur l'icône **Vulnerability Manager** dans la zone **Essayer**.
3. Pour accepter le contrat de licence d'utilisateur final, cliquez sur **OK**.

   Lorsque la période de licence étendue est terminée, vous devez attendre six mois avant de pouvoir activer à nouveau la licence temporaire. Pour avoir un accès permanent à QRadar Vulnerability Manager, vous devez acheter une licence.

Analyses à haute disponibilité QRadar Vulnerability Manager

Utilisez un déploiement à haute disponibilité (HA) QRadar pour gérer votre planning d'analyse des vulnérabilités, en cas d'échec du déploiement de QRadar.

Le système à haute disponibilité version 2 est pris en charge dans QRadar Vulnerability Manager.

Vous devez utiliser des dispositifs identiques avec des configurations logicielles identiques dans votre système à haute disponibilité. Pour plus d'informations sur la configuration d'un déploiement à haute disponibilité, voir le document *IBM QRadar High Availability Guide*.

Analyses à haute disponibilité

Les dispositifs suivants sont pris en charge dans un déploiement à haute disponibilité QRadar Vulnerability Manager :

- Console
- Dispositif de scanner (610)
- Dispositif de processeur (600)

Remarques importantes

Prenez en compte les informations suivantes lorsque vous déployez une analyse de la vulnérabilité à haute disponibilité (HA) :

- Annulez et redémarrez les analyses après un basculement si ces dernières étaient au cours au moment du basculement.
- Si vous remplacez un dispositif dans votre environnement d'analyse à haute disponibilité, il peut ne pas apparaître dans le déploiement. Vous devez ajouter à nouveau le dispositif au déploiement à haute disponibilité puis déployer les modifications.
- Utilisez des configurations et des dispositifs identiques dans votre configuration à haute disponibilité.
- Les mises à jour automatiques interrompues ne reprennent pas après un basculement. Vous devez exécuter une mise à jour automatique dans une configuration active ininterrompue.

Chapitre 3. Présentation de QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager est une plateforme d'analyse de réseau qui détecte les vulnérabilités des applications, des systèmes et des dispositifs de votre réseau ou dans votre zone démilitarisée.

QRadar Vulnerability Manager utilise le renseignement de sécurité pour vous aider à gérer et à hiérarchiser les vulnérabilités de votre réseau. Par exemple, vous pouvez utiliser QRadar Vulnerability Manager pour surveiller les vulnérabilités en continu, améliorer la configuration des ressources et identifier les correctifs logiciels. Vous pouvez également hiérarchiser les failles de sécurité en corrélant les données de vulnérabilité aux flux réseau, données de journal, pare-feu et données du système de prévention des intrusions.

Vous pouvez gérer une visibilité en temps réel des vulnérabilités détectées par le programme d'analyse QRadar Vulnerability Manager intégré et d'autres programmes d'analyse tiers. Les programmes d'analyse tiers sont intégrés à QRadar et incluent IBM BigFix, Guardium, AppScan, Nessus, nCircle et Rapid 7.

Remarque : Lors du déploiement, QRadar Vulnerability Manager met à jour automatiquement le bloc de construction **BB:Host Definition: VA Scanner Source IP** par défaut afin d'inclure les emplacements de tous les processeurs QVM. Ce comportement est normal.

Sauf indication contraire, toutes les références à QRadar Vulnerability Manager se réfèrent à IBM QRadar Vulnerability Manager. Toutes les références à QRadar se réfèrent à IBM QRadar SIEM et à IBM QRadar Log Manager, et toutes les références à SiteProtector se réfèrent à IBM Security SiteProtector.

Analyse des vulnérabilités

Dans IBM QRadar Vulnerability Manager, l'analyse des vulnérabilités est gérée par la configuration des profils d'analyse. Chaque profil d'analyse définit les actifs à examiner et la planification de l'analyse.

Processeur de vulnérabilité

Lorsque vous faites l'acquisition d'une licence pour QRadar Vulnerability Manager, un processeur de vulnérabilité est déployé automatiquement sur votre console QRadar. Ce processeur contient un composant d'analyse QRadar Vulnerability Manager.

Options de déploiement

Vous pouvez déployer l'analyse de vulnérabilité de plusieurs façons. Par exemple, vous pouvez déployer la fonction d'analyse sur un dispositif de programme d'analyse d'hôte géré QRadar Vulnerability Manager ou sur un hôte géré QRadar.

Options de configuration

Les administrateurs peuvent configurer les analyses des façons suivantes :

- Planifier les analyses afin qu'elles s'exécutent à des moments opportuns pour vos actifs de réseau.
- Spécifier les périodes pendant lesquelles les analyses ne doivent pas avoir lieu.
- Spécifier les actifs à exclure des analyses, tant globalement que pour chaque analyse.
- Configurer les analyses des correctifs authentifiés pour les systèmes d'exploitation Linux, UNIX ou Windows.
- Configurer plusieurs protocoles d'analyse ou spécifier les plages de ports à analyser.

© Copyright IBM Corp. 2012, 2020

Catégories des vérifications de vulnérabilité QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager recherche plusieurs types de vulnérabilité dans votre réseau.

Les différentes vulnérabilités sont classées dans les catégories suivantes :

- Paramètres par défaut à risque
- Fonctions logicielles
- Configuration incorrecte
- Failles de fournisseur

Paramètres par défaut à risque

En conservant certains paramètres par défaut, vous pouvez rendre votre réseau vulnérable aux attaques. Vous trouverez ci-dessous des exemples de situation rendant votre réseau vulnérable :

- Conservation de pages ou de scripts exemple dans une installation IIS
- Conservation du mot de passe par défaut sur un concentrateur/commutateur 3Com
- Conservation du nom de communauté SNMP "public" ou "private" sur un périphérique SNMP
- Absence de mot de passe de connexion SA sur un serveur MS-SQL

Fonctions logicielles

Certains paramètres logiciels pour les systèmes ou les applications sont conçus pour une meilleure convivialité mais ces paramètres peuvent devenir des facteurs de risque pour votre réseau. Par exemple; le protocole NetBIOS de Microsoft est utile dans les réseaux internes mais s'il est exposé sur Internet ou sur un segment réseau non sécurisé, il présente des risques pour votre réseau.

Vous trouverez ci-dessous des exemples de commandes ou de fonctions logicielles pouvant présenter des risques pour votre réseau :

- Demandes de masque de réseau ou d'horodatage ICMP
- Commandes Sendmail expand ou verify
- Services du protocole Ident qui identifient le propriétaire d'un processus en cours d'exécution.

Configuration incorrecte

QRadar Vulnerability Manager identifie les configurations incorrectes des paramètres par défaut mais il peut également identifier un ensemble plus étendu de configurations incorrectes, par exemple dans les cas suivants :

- Relais SMTP
- Partage de fichiers NetBios non restreint
- Transferts de zone DNS
- Répertoires inscriptibles FTP
- Comptes d'administration par défaut n'ayant aucun mot de passe
- Répertoires pouvant être exportés NFS

Failles de fournisseur

Cette catégorie générale inclut divers événements, tels que des dépassements de mémoire tampon, des problèmes de format de chaîne, des attaques de traversée de répertoire et des scripts intersite. Les vulnérabilités nécessitant un correctif ou un correctif de mise à jour sont inclus dans cette catégorie.

Vérifications effectuées par QRadar Vulnerability Manager

QRadar Vulnerability Manager utilise un ensemble de vérifications actives qui implique l'envoi de paquets et d''envois-tests distants, ainsi que des vérifications de corrélations passives. La base de données QRadar Vulnerability Manager couvre environ 70 000 vulnérabilités de couche d'application, de système d'exploitation et de réseau.

Vous pouvez effectuer dans l'ensemble de la bibliothèque d'analyse une recherche par CVE, plage de dates, nom de fournisseur, nom de produit, version de produit et nom d'exposition dans la fenêtre de recherche de l'onglet **Vulnérabilités**.

Tests QRadar Vulnerability Manager

Les exemples suivants correspondent à des catégories testées par QRadar Vulnerability Manager :

- Vérifications de base de données
- Vérifications de serveur Web
- Vérifications de serveur d'applications Web
- Vérifications de scripts Web communs
- Vérifications d'application Web personnalisée
- Vérifications de serveur DNS
- Vérifications de serveur de messagerie
- Vérifications de serveur d'applications
- Vérifications de point d'accès sans fil
- Vérification de service commun
- Systèmes et logiciels obsolètes

Le tableau suivant décrit certaines vérifications effectuées par QRadar Vulnerability Manager.

Tableau 4. Types de vérification QRadar Vulnerability Manager

Type de vérification	Description
Analyse de port	Recherche les hôtes actifs ainsi que les ports et les services ouverts sur chaque hôte actif. Renvoie l'adresse MAC si l'hôte se trouve sur le même sous-réseau que le scanner. Renvoie des informations de système d'exploitation.

Tableau 4. Types de vérification QRadar Vulnerability Manager (suite)

Type de vérification	Description
Analyse des applications Web	Vérifie chaque application et page sur un serveur Web en utilisant les méthodes suivantes : Téléchargement de fichier Parcours de répertoire HTTP CWE-22 - Limitation incorrecte d'un nom de chemin à un répertoire restreint (path traversal) Fichier intéressant/apparaissant dans les journaux Indication automatique du mot de passe dans le navigateur Configuration incorrecte dans les fichiers par défaut Divulgation d'informations Formulaire de connexion non chiffré Répertoire indexable : vérifie s'il est possible de parcourir les répertoires du serveur Action HTTP PUT autorisée : vérifie si l'option PUT est activée pour les répertoires du serveur Existence de fichiers obsolètes Analyse CGI : vérifications de page Web commune Injection (XSS/script/HTML) Extraction de fichier distant (au niveau du serveur) Exécution de commande à partir du shell distant Injection SQL, incluant le contournement de l'authentification, l'identification logicielle et la source distante Options d'optimisation inverse, à l'exception des options spécifiées. **Remarque :** L'analyse d'application Web authentifiée n'est pas prise en charge. Par exemple, si une authentification est requise pour accéder au site, vous ne pouvez pas exécuter de tests d'application Web.
Système d'exploitation	Divulgation de nom d'utilisateur et de mot de passe Accès aux systèmes de fichiers Noms d'utilisateur et mots de passe par défaut Escalade de privilège Refus de service Exécution de commande à distance Attaques par script intersite (Microsoft)
Base de données	Exploitations et accès ouvert aux bases de données. Bases de données par défaut Noms d'utilisateur et mot de passe découverts Refus de service Droits d'administration

Tableau 4. Types de vérification QRadar Vulnerability Manager (suite)	
Type de vérification	**Description**
Serveur Web	Vulnérabilités connues, exploitations et problèmes de configuration sur les serveurs Web. Refus de service Mots de passe d'administration par défaut Possibilité d'affichage du système de fichiers Attaques par script intersite
Scripts Web communs	Scripts Web généralement détectés (CGI, par exemple) Scripts liés au commerce électronique ASP PHP
Serveur DNS	Chiffrement de mot de passe non fiable Refus de service Détermination de noms de compte Envoi de messages électroniques Lecture arbitraire de messages électroniques et d'informations de compte confidentielles Obtention d'accès administrateur
Point d'accès sans fil	Mot de passe par défaut du compte d'administration Noms de communauté SNMP par défaut Stockage du mot de passe en texte normal Refus de service
Services communs	Système DNS (Domain name system - système de nom de domaine) Protocole FTP (File Transfer Protocol) Protocole SMTP (Simple Mail Transfer Protocol)
Serveur d'applications	Contournement d'authentification Refus de service Divulgation d'informations Noms d'utilisateur et mots de passe par défaut Autorisations d'accès aux fichiers vulnérables Attaques par script intersite
OVAL	Vulnérabilités côté client sous IE, Chrome, Skype, etc.
Test de mot de passe	Test de mot de passe par défaut
Analyse des correctifs Windows	Rassemble des entrées de clé de registre, des services Windows, des applications Windows installées et des bogues Microsoft corrigés.
Analyse des correctifs UNIX	Collecte des détails relatifs aux RPM installés

Analyse des applications Web

QRadar Vulnerability Manager utilise l'analyse non authentifiée pour l'analyse d'application Web principale. La liste suivante décrit les vérifications de vulnérabilité Web QRadar Vulnerability Manager :

- Vulnérabilités d'injection SQL

  Il existe des vulnérabilité d'injection SQL lorsque des programmes mal conçus acceptent des données fournies par l'utilisateur dans une requête de base de données sans valider l'entrée se trouvant sur des pages Web avec du contenu dynamique. En recherchant des vulnérabilités d'injection SQL, QRadar Vulnerability Manager garantit que l'autorisation requise est établie afin d'éviter ces exploitations.
- Vulnérabilités de script intersite (XSS)

  En profitant de vulnérabilités de script intersite, des utilisateurs malveillants peuvent injecter du code (scripts côté client et HTML, par exemple) dans des pages Web consultées par d'autres utilisateurs. Une vulnérabilité de script intersite exploitée peut être utilisée par des attaquants pour contourner les contrôles d'accès (politique de même origine, par exemple). QRadar Vulnerability Manager recherche différentes vulnérabilités de script intersite persistantes ou non afin de s'assurer que l'application Web n'est pas concernée par cette menace.
- Infrastructure d'application Web

  QRadar Vulnerability Manager inclut des milliers d'actions qui vérifient les configurations par défaut, les scripts cgi, l'application installée et de prise en charge, les périphériques et les systèmes d'exploitation sous-jacents.
- Erreurs de page Web

Pour une analyse d'application Web approfondie, QRadar Vulnerability Manager est intégré à IBM Security AppScan pour une meilleure visibilité des vulnérabilités d'application Web.

Analyse de périphérique réseau

QRadar Vulnerability Manager inclut les plug-in suivants qui prennent en charge l'analyse des périphériques réseau :

- SNMP

  QRadar Vulnerability Manager prend en charge SNMP V1 et SNMP V2. SNMP V3 n'est pas pris en charge. QRadar Vulnerability Manager utilise un dictionnaire des valeurs par défaut de communauté connues pour divers périphériques SNMP. Vous pouvez personnaliser le dictionnaire.
- Analyse OVAL

  QRadar Vulnerability Manager utilise OVAL pour détecter et signaler les vulnérabilités connues. Le plug-in d'analyse OVAL QRadar Vulnerability Manager fonctionne uniquement avec les périphériques Cisco.

Vérifications du scanner externe

Le scanner externe analyse les énumérations CWE (Common Weakness Enumerations) d'OWASP (Open Web Application Security Project) suivantes :

- Directory Listing
- Path Traversal, Windows File Parameter Alteration, UNIX File Parameter Alteration, Poison Null Byte Windows Files Retrieval, Poison Null Byte UNIX Files Retrieval
- Cross-Site Scripting, DOM-Based Cross-Site Scripting
- SQL Injection, Blind SQL Injection, Blind SQL Injection (Time Based)
- Autocomplete HTML Attribute Not Disabled for Password Field
- Unencrypted Login Request, Unencrypted Password Parameter
- Remote Code Execution, Parameter System Call Code Injection, File Parameter Shell Command Injection, Format String Remote Command Execution

Analyse de base de données

QRadar Vulnerability Manager détecte les vulnérabilités sur les principales bases de données en utilisant l'analyse authentifiée des hôtes cible. De plus, QRadar Vulnerability Manager cible plusieurs bases de données en utilisant des plug-in.

Vérifications de système d'exploitation

Tableau 5. Vérifications de système d'exploitation

Système d'exploitation	Analyse des vulnérabilités	Analyse des correctifs	Configuration
Windows	Oui	Oui	Oui
AIX UNIX	Oui	Oui	Non
CentOS Linux	Oui	Oui	Non
Debian Linux	Oui	Oui	Non
Fedora Linux	Oui	Oui	Non
Red Hat Linux	Oui	Oui	Non
Sun Solaris	Oui	Oui	Non
HP-UX	Oui	Oui	Non
Suse Linux	Oui	Oui	Non
Ubuntu Linux	Oui	Oui	Non
CISCO	Non	Non	Non
AS/400 / iSeries	Non	Non	Non

OVAL et systèmes d'exploitation

Les définitions OVAL sont prises en charge dans les systèmes d'exploitation suivants :

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- CentOS versions 3 - 7
- IBM AIX versions 4-7
- RHEL versions 3 - 7
- SUSE versions 10 - 11
- Ubuntu versions 6-14
- Red Hat 9

- Solaris versions 2.6, 7 - 10

Tableau de bord de gestion des vulnérabilités

Vous pouvez afficher les informations de vulnérabilité dans votre tableau de bord QRadar.

IBM QRadar Vulnerability Manager est distribué avec un tableau de bord des vulnérabilités par défaut qui vous permet de voir rapidement les risques pour votre organisation.

Vous pouvez créer un tableau de bord, gérer vos tableaux de bord existants et modifier les configurations d'affichage de chaque élément de tableau de bord de vulnérabilité.

Pour plus d'informations sur les tableaux de bord, voir le *Guide d'utilisation* de votre produit.

Révision des données de vulnérabilité sur le tableau de bord de gestion des vulnérabilités par défaut

Vous pouvez afficher les informations de gestion des vulnérabilités par défaut sur le tableau de bord QRadar.

Le tableau de bord de gestion des vulnérabilités par défaut contient des informations relatives aux risques, aux vulnérabilités et aux analyses.

Vous pouvez configurer votre propre tableau de bord pour qu'il contienne d'autres éléments, tels que les recherches enregistrées.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la barre d'outils, dans la liste **Afficher le tableau de bord**, sélectionnez **Gestion des vulnérabilités**.

Création d'un tableau de bord de gestion des vulnérabilités personnalisé

Dans QRadar, vous pouvez créer un tableau de bord de gestion des vulnérabilités qui est personnalisé à vos besoins.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la barre d'outils, cliquez sur **Nouveau tableau de bord**.
3. Entrez un nom et une description pour le tableau de bord des vulnérabilités.
4. Cliquez sur **OK**.
5. Dans la barre d'outils, sélectionnez **Ajouter un article** > **Gestion des vulnérabilités**, puis choisissez parmi les options suivantes :
   - Si vous souhaitez présenter les recherches enregistrées par défaut sur votre tableau de bord, sélectionnez **Recherches de vulnérabilités**.
   - Si vous souhaitez présenter les liens de site Web pour accéder à des informations sur la sécurité et les vulnérabilités, sélectionnez **Articles sur la sécurité**, **Recommandations de sécurité** ou **Dernières vulnérabilités publiées**.
   - Si vous souhaitez afficher des informations sur les analyses terminées ou en cours d'exécution, sélectionnez **Analyses terminées** ou **Analyses en cours**.

Création d'un tableau de bord pour la conformité d'actif

Créez un tableau de bord qui indique le correctif le plus efficace pour remédier aux vulnérabilités détectées sur le réseau.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la barre d'outils, cliquez sur **Nouveau tableau de bord**.
3. Entrez un nom et une description pour le tableau de bord des vulnérabilités.
4. Cliquez sur **OK**.
5. Dans la barre d'outils, sélectionnez **Ajouter un article** > **Gestion des vulnérabilités** > **Recherche de vulnérabilités** et choisissez la recherche sauvegardées par défaut que vous voulez afficher sur votre tableau de bord.
6. Dans l'en-tête du nouvel article de tableau de bord, cliquez sur l'icône **Paramètres** jaune.
7. Sélectionnez **Correctif** dans la liste **Grouper par** et sélectionnez l'une des options suivantes dans la liste **Par graphique**:
   - Si vous voulez voir combien d'actifs sont nécessaires pour qu'un correctif soit appliqué, sélectionnez **Nombre d'actifs**.
   - Si vous voulez voir le score du risque cumulé par correctif, sélectionnez **Score de risque**.
   - Si vous souhaitez voir le nombre de vulnérabilités qui sont couvertes par un correctif, sélectionnez **Nombre de vulnérabilités**.
8. Cliquez sur **Sauvegarder**.
9. Pour afficher les détails de la vulnérabilité dans la page **Gérer les vulnérabilités** > **Par vulnérabilité** sous l'onglet **Vulnérabilités**, cliquez sur le lien **Afficher dans Par vulnérabilité** au bas de l'article de tableau de bord.

Chapitre 4. Stratégie d'analyse des vulnérabilités et recommandations

Une bonne planification est essentielle pour la configuration d'un système d'analyse IBM QRadar Vulnerability Manager stable et efficace dans votre réseau.

Analysez la structure de votre réseau et définissez la meilleure configuration d'analyse pour votre réseau, du point de vue du matériel et des performances d'analyse.

Prenez en compte les informations ci-dessous qui offrent des recommandations sur la configuration de votre déploiement d'analyse QRadar Vulnerability Manager :

- Types de politique d'analyse

  Choisissez le type de politique d'analyse qui répond à vos besoins en analyse et tenez compte du temps et des ressources qui sont nécessaires pour effectuer l'analyse.
- Durée d'analyse et ports à analyser

  Décidez si vous avez besoin d'analyser tous les ports TCP et UDP. Les ports UDP sont plus longs à analyser que les ports TCP.
- Optimisation de votre reconnaissance d'actifs.

  Optimisez votre reconnaissance d'actifs pour gérer la durée et l'efficacité de la reconnaissance d'actifs.
- Optimisation des performances pour la reconnaissance d'actifs.

  Optimisez la vitesse et la précision de reconnaissance des actifs dans votre réseau.
- Positionnement du scanner dans votre réseau

  Placez les scanners prêt des actifs que vous analysez et tenez compte de l'impact du temps d'attente des réseaux sur vos durées d'analyse.
- Analyse des applications Web

  Cette analyse peut prendre un temps considérable et peut nécessiter une grande quantité de ressources. Si vous n'avez pas besoin d'exécuter cette analyse dans le cadre d'une analyse complète, vous pouvez l'exclure.
- Analyse dynamique

  Vous pouvez gagner du temps en implémentant une analyse dynamique.
- Définition de la bande passante du réseau

  Ajustez les paramètres relatifs à la bande passante du réseau conformément à la bande passante de votre réseau et au nombre d'actifs que vous pouvez analyser simultanément.
- Cartes d'interface réseau sur les scanners

  Utilisez les cartes d'interface réseau pour segmenter l'analyse de votre réseau.
- Gestion des vulnérabilités pour les propriétaires d'actifs

  Affectez des propriétaires à vos actifs.
- Notification des propriétaires d'actifs sur les temps d'analyse.

  Assurez-vous que les propriétaires d'actifs sont informés de la durée des analyses.
- Déclenchements d'analyses des nouveaux actifs

  Déclenchez des analyses des nouveaux actifs lorsqu'ils sont ajoutés à la base de données d'actifs.
- Configuration du risque environnemental pour un actif

  Utilisez le score environnemental CVSS pour manipuler et définir la priorité du score de risque pour les actifs sélectionnés.

© Copyright IBM Corp. 2012, 2020

- Analyse externe - Foire aux questions

  Ce que vous devez savoir sur la configuration d'une analyse externe.

Types de politique d'analyse

IBM QRadar Vulnerability Manager fournit plusieurs types de politique d'analyse par défaut. Vous pouvez également définir vos propres analyses à partir des modèles d'analyse.

Les modèles d'analyse suivants sont les modèles les plus couramment utilisés :

Discovery scan policy (Politique d'analyse de reconnaissance)
Détecte les actifs réseau puis analyse les ports afin d'identifier les principales caractéristiques des actifs, comme par exemple le système d'exploitation, le type de périphérique, et les services. Les vulnérabilités ne sont pas analysées.

Analyse simple sans données d'identification qui recherche un espace adresse pour les adresses IP actives puis analyse leurs ports. Elle exécute les recherches DNS et NetBIOS pour détecter le système d'exploitation, les services ouverts et les noms des réseaux.

Si possible, exécutez cette analyse sans données d'identification une fois par semaine pour offrir une bonne visibilité du réseau. Cette analyse est très utile pour identifier les nouveaux actifs et les modifications par rapports aux actifs analysés auparavant.

Remarque : Utilisez la recherche sauvegardée **actifs détectés au cours des 14 derniers jours mais non analysés** de l'onglet **Actifs** pour identifier les nouveaux actifs détectés par QRadar de manière passive au cours des 14 derniers jours.

Full scan policy (Politique d'analyse complète)
Détecte les actifs réseau à l'aide d'une plage de port à analyse rapide. Exécute une analyse de port configurable par l'utilisateur et une analyse non authentifiée des services détectés tels que le FTP, le Web, le SSH, et la base de données. Une analyse authentifiée est exécutée lorsque des données d'identification sont fournies.

Exécute la suite complète des tests de QRadar Vulnerability Manager.

Une analyse complète comprend les phases suivantes :

1. Analyse de reconnaissance.
2. Analyse sans données d'identification.

   Vérifie les services n'ayant pas besoin de données d'identification, par exemple la lecture des bannières et des réponses en vue d'obtenir des informations de version, la date d'expiration des certificats SSL, le test des comptes par défaut et le test des réponses en vue de détecter les vulnérabilités.
3. Analyse avec données d'identification.

   QRadar Vulnerability Manager se connecte à l'actif et collecte des informations sur l'inventaire d'application installé et sur la configuration requise et augmente ou supprime les vulnérabilités. Les analyses authentifiées sont préférables aux analyses non authentifiées. Les analyses non authentifiées donnent un aperçu utile de l'état de vulnérabilité du réseau. Cependant, l'analyse sans données d'identification est essentielle pour un programme de gestion des vulnérabilités efficace et complet.

   Vous ne pouvez pas modifier les politiques intégrées, mais vous pouvez les copier pour créer votre propre politique d'analyse personnalisée.

   Conseil : Les analyses complètes peuvent parfois verrouiller certains comptes d'administration, par exemple SQL Server, lorsque QRadar Vulnerability Manager teste plusieurs données d'identification par défaut sur les comptes. Pour désactiver ces tests de connexion, procédez comme suit :

   a. Cliquez sur l'onglet **Vulnérabilités**.

b. Dans la fenêtre **Politique d'analyse**, cliquez sur **Politiques d'analyse**.

c. Cliquez sur la politique **Analyse complète**, puis sur **Editer**.

d. Cliquez sur l'onglet **Outils**.

Par défaut, la liste **Included** est affichée.

e. Dans le menu **Filter**, sélectionnez **Default Logons (Dos Risk)**.

f. Cliquez sur **Exclude All** pour supprimer les coches en regard des éléments de la liste.

g. Cliquez sur **Save**.

h. Vérifiez que les outils **Default Logons (Dos Risk)** sont dans la liste **Excluded**.

Exécutez une analyse complète tous les 2 à 3 mois pour obtenir une évaluation détaillée et précise des vulnérabilités de votre réseau. L'analyse complète consomme une grande quantité de ressources, de sorte que la planification et l'allocation des ressources sont importantes pour obtenir des performances optimales.

Politique d'analyse de correctif

Explore le réseau pour découvrir les actifs puis exécute une analyse de port rapide et une analyse avec données d'identification des actifs.

Les analyses de correctifs sont utilisées pour déterminer quels correctifs et produits sont installés ou manquants sur le réseau.

Une analyse de correctifs comporte deux phases principales :

1. analyse de reconnaissance
2. Analyse avec données d'identification

Exécutez cette analyse toutes les 1 à 4 semaines pour déterminer quels correctifs et produits sont installés ou manquants sur votre réseau. L'analyse de correctif représente seulement une charge minimale sur votre réseau et les tests actifs sont maintenus à un niveau faible.

Politique d'analyse de PCI

Analyse tous les ports TCP et UDP 0 à 65535.

Vous n'êtes pas obligé d'analyser tous les ports UDP pour la conformité PCI. En règle générale, vous analysez les ports UDP les plus courants pour la conformité PCI, mais la liste des ports peut varier légèrement dans le temps, conformément aux normes de sécurité PCI.

Si vous analysez tous les ports UDP, l'analyse peut prendre un certain temps et ne pas se terminer dans le délai d'expiration sur les grands segments de réseau. Cela entraîne certains cas de vulnérabilité `Scan Interference Detected - Scan Potentially Incomplete`.

Vous pouvez créer votre propre politique d'analyse PCI personnalisée en copiant cette politique, en la renommant et en modifiant les ports d'analyse UDP en fonction de vos exigences.

Politique d'analyse de base de données

Analyse les ports 523, 1433, 1521 et 3306 de la base de données pour rechercher des services de bases de données populaires.

Utilisez l'analyse de base de données sans données d'identification pour analyser les ports DB2 (523), Microsoft SQL (1433), MySQL (3306), Oracle (1521) et Informix (1526) afin de détecter des services de bases de données populaires.

Exécutez cette analyse régulièrement si l'activité de votre base de données est élevée.

Concepts associés

Politiques d'administration d'analyse

Durées d'analyse et analyse des ports

La gestion de la configuration de vos analyses réseau dépend du nombre d'actifs présents dans votre réseau, de l'infrastructure de votre réseau et des durées de réalisation des analyses.

L'analyse d'un réseau important peut prendre beaucoup de temps et vous avez donc besoin d'une stratégie d'analyse qui optimise vos ressources d'analyse.

Conseil : Il est recommandé d'utiliser des fenêtres opérationnelles pour effectuer des analyses à des périodes en dehors des sauvegardes nocturnes ou des sauvegardes automatiques.

Stratégie d'analyse des ports

Votre stratégie d'analyse dépend du nombre d'hôtes que vous souhaitez analyser : s'il s'agit d'un réseau de classe C de 256 hôtes ou d'un réseau de classe B de 65.536 hôtes. Votre durée d'analyse totale peut être affectée de manière significative si vous augmentez le nombre d'hôtes que vous souhaitez analyser. Pour que la durée d'analyse totale soit acceptable, vous pouvez réduire la durée d'analyse par hôte.

Par exemple, si vous effectuez une analyse de reconnaissance réseau sur un réseau de classe B et que la reconnaissance du port TCP prend 1 seconde :

- L'analyse d'un port sur 65536 hôtes à 1 seconde par hôte prend 18 heures.
- Si vous analysez un port supplémentaire sur chacun des 65.536 hôtes et autorisez 1 seconde par hôte, l'analyse de ce port supplémentaire prend 18 heures supplémentaires.

Cet exemple montre bien l'impact que peut avoir le fait d'ajouter un port d'analyse supplémentaire sur un réseau de grande envergure. Si vous analysez un grand nombre d'hôtes, déterminez quels services sont importants et exposés à des vulnérabilités à haut risque afin de pouvoir configurer vos politiques d'administration d'analyse en conséquence lors de l'analyse de reconnaissance. Avant d'implémenter vos politiques d'administration d'analyse, exécutez des analyses test à l'aide de différentes politiques d'administration d'analyse et estimez le temps et les ressources nécessaires pour réaliser ces analyses.

Conseil : La politique d'administration d'analyse de reconnaissance par défaut de QRadar exécute une analyse rapide Nmap des ports TCP et UDP et vous pouvez l'utiliser pour analyser un nombre d'hôtes plus limité.

L'analyse du port UDP est plus longue que celle du port TCP car il s'agit d'un protocole sans connexion. L'analyse de tous les ports UDP peut prendre un temps considérable et faire appel à une grande quantité de ressources. Déterminez si vous avez besoin d'analyser tous les ports UDP ou si vous pouvez analyser ces ports moins souvent que les ports TCP.

Les ports suivants constituent les ports UDP prioritaires que vous devriez analyser régulièrement :

- Services d'authentification tels que RADIUS et Kerberos
- Portes dérobées et applications à accès distant
- Applications de sauvegarde
- Serveurs de base de données
- DNS (Domain Name System)
- NetBIOS et CIFS (Common Internet File System)
- NFS (Network File System)
- NTP (Network Time Protocol)
- P2P (peer-to-peer) et application de dialogue en ligne
- Protocole de routage, y compris RIP (Routing Information Protocol)
- RPC (Remote Procedure Call) et mappage des noeuds finaux RPC
- SNMP (Simple Network Management Protocol) et alerte SNMP
- Syslog
- TFTP (Trivial File Transfer Protocol)

- VPNs, y compris ISAKMP (Internet Security Association and Key Management Protocol), L2TP (Layer Two Tunneling Protocol) et NAT-T (NAT Traversal).
- Les ports connus pour être associés à une activité malveillante.

Durées d'analyse typiques

Le tableau ci-dessous offre des renseignements sur les durées d'analyse.

Tableau 6. Durées d'analyse pour les appareils QRadar

Application QRadar	**Durées d'analyse**
QRadar 2100/3100 All-in-One	Une analyse complète par défaut de 2000 à 4000 actifs prend 2 à 3 jours.
QRadar Vulnerability Manager sur les hôtes gérés suivants : 610 1200 1300 1400 1500	Une analyse complète par défaut de 2000 à 4000 actifs prend 2 à 3 jours. Un processeur QRadar Vulnerability Manager externe sur un hôte géré (600) est requis lorsque plus de 50.000 actifs sont analysés régulièrement ou lorsque des analyses sont exécutées pendant de longues périodes sur la console QRadar Console.

Optimisation de votre configuration de reconnaissance d'actifs

Optimisez votre reconnaissance d'actifs pour gérer la durée et l'efficacité de la reconnaissance d'actifs.

Optimisez votre reconnaissance d'actifs dans l'onglet **Asset Discovery** de votre politique d'analyse. Vous pouvez utiliser la configuration par défaut comme un moyen rapide et efficace de reconnaître vos actifs. Les pings ICMP et les paquets TCP SYN sont activés par défaut.

Utilisez les options suivantes pour optimiser votre reconnaissance d'actifs :

- Envoi de commandes ping ICMP.

  Les commandes pings sont envoyées aux adresses IP configurées dans le profil d'analyse qui utilise cette politique d'analyse.
- Envoi de paquets TCP SYN aux ports.

  Cette option est une option rapide et fiable activée pour les ports préconfigurés.
- Envoi de paquets UDP aux ports.

  Sélectionnez cette option pour envoyer des paquets UDP vers les ports préconfigurés. UDP est plus lent que TCP. Si vous envoyez un paquet UDP vers une adresse IP inactive, l'envoi peut prendre plusieurs secondes en raison des tentatives multiples.
- Activation de la détection de la fonction Traceroute.

  La détection de Traceroute nécessite davantage de ressources et une durée d'analyse plus longue.
- Activation de la détection ICMP.

  La détection d'ICMP nécessite davantage de ressources et une durée d'analyse plus longue.
- Empreintes digitales de système d'exploitation et de service

  Interroger les ports pour les informations du système d'exploitation et de service. Si vous sélectionnez cette option, les temps d'analyse augmentent.

Vous pouvez configurer des options de reconnaissance personnalisées. Les options que vous choisissez dépendent de vos besoins et de la structure de votre réseau. Testez différentes options pour découvrir une configuration de reconnaissance optimale qui correspond à vos besoins.

Optimisation des performances pour la reconnaissance d'actifs

Optimisez la vitesse et la précision de reconnaissance des services sur vos actifs.

Optimisez les performances de reconnaissance dans l'onglet **Discovery Performance** de votre politique d'analyse. Vous pouvez utiliser la configuration par défaut comme un moyen rapide et efficace de reconnaître vos actifs.

Utilisez les options suivantes afin d'optimiser vos performances pour la reconnaissance d'actifs :

- **Maximum retries**

  Les analyses peuvent durer plus longtemps lorsque la valeur indiquée pour le nombre maximal de tentatives est élevée mais l'indication d'une valeur trop faible peut avoir des conséquence sur la précision des résultats de l'analyse.

- **Minimum timeout interval**

  L'intervalle de délai pour les analyses est réduit au niveau minimal configuré lorsque le réseau est fiable.

- **Initial timeout interval**

  Nmap définit la valeur du délai en réponse aux envois-tests précédents. Si le temps d'attente augmente, la valeur de délai d'attente est également augmentée. Si vous réduisez de manière trop importante à la fois le délai d'attente d'origine et les intervalles de délai d'attente maximum, les analyses peuvent être plus rapides mais il est probable qu'une nouvelle transmission soit nécessaire.

- **Scan delay**

  Utilisez ce paramètre pour définir le délai entre plusieurs envois-tests d'analyse. Si vos périphériques utilisent une limitation de débit, vous pouvez alors synchroniser le délai d'analyse avec la valeur de limitation de débit afin d'avoir des temps d'analyse optimisés.

- **Minimum packets per second**

  Nmap envoie des paquets en utilisant le débit le plus élevé possible toléré par votre réseau (compris entre le débit **Minimum packets per second** et la valeur de l'option **Maximum packets per second rate**).

- **Maximum packets per second**

  Par défaut, cette zone est vide car Nmap définit dynamiquement une vitesse de paquet appropriée pour votre réseau. Si vous le souhaitez, vous pouvez configurer votre propre débit.

Analyse des applications Web

Les analyses Web peuvent être lentes si vous possédez des applications Web complexes. Tous les ports exécutant des services HTTP ou HTTPS, y compris les ports RPC HTTP Microsoft, sont analysés.

Une partie d'une analyse complète ou d'une analyse Web comporte une phase qui utilise des techniques consommatrices de ressources similaires au balayage du Web (en anglais : web crawling ou spidering). Si le scanner doit balayer plusieurs pages Web contenant plusieurs liens, l'analyse peut être lente et consommer un grand nombre de ressources. Les analyses Web recherchent les vulnérabilités du Web et déterminent par exemple si une version de serveur HTTP présente des vulnérabilités, des certificats SSL arrivés à expiration ou des chiffrements SSL faibles. L'analyse Web recherche également les vulnérabilités OWASP (Open Web Application Security Project) comme l'injection SQL, le script intersite (XSS), et les configurations de sécurité défaillantes.

Si vous n'avez pas besoin d'analyser vos applications Web, créez une politique d'administration d'analyse personnalisée complète et excluez l'outil d'analyse **http – CGI scanner** qui se trouve sur l'onglet **Outils** de votre politique d'administration d'analyse.

Positionnement du scanner dans votre réseau

Les opérations d'analyse sont plus efficaces lorsque les scanners ont une bonne connectivité avec les actifs qui sont analysés et ne sont pas bloqués par des pare-feu ou d'autres périphériques ayant un impact sur le flux des données d'analyse. Vous pouvez déployer un nombre illimité de scanners sur votre réseau, mais vous devez disposer d'une licence logicielle pour chaque hôte géré QRadar que vous déployez en tant que scanner.

Tenez compte des facteurs suivants avant de placer des scanners dans votre réseau :

- Evitez d'analyser les actifs à travers des pare-feu pour les raisons suivantes :
  - Les pare-feu ralentissent le processus d'analyse et bloquent certains ports qui sont requis pour réaliser l'analyse.
  - Lorsque vous analysez des actifs à travers un pare-feu, des événements sont créés dans IBM QRadar et le nombre d'événements par seconde (EPS) augmente, ce qui peut avoir un impact sur votre licence EPS.
  - Les pare-feu avec état peuvent entraîner la création d'actifs par QRadar par erreur. Les pare-feu avec état répondent aux paquets TCP hors séquence et peuvent faire penser au scanner qu'un hôte existe.
- N'analysez pas les connexions des réseaux longue distances à faible bande passante.
- Si la durée de ping du scanner à l'actif dépasse 40 ms, placez le scanner plus prêt de l'actif.
- Ne scannez pas à travers un équilibreur de charge car il est plus difficile pour le scanner de gérer l'analyse lorsque le trafic réseau est équilibré auprès de différents serveurs.
- Evitez de configurer votre scanner pour analyser des plages d'adresses ID qui ne sont pas utilisées. Durant la phase de détection d'une analyse, un scanner met plus longtemps à déterminer qu'une adresse IP n'est pas utilisée qu'à déterminer si une adresse IP est active.
- Déployez plusieurs scanners plutôt que d'exécuter plusieurs analyses simultanées à partir du même scanner. A mesure que vous ajoutez des analyses simultanées à un même scanner, les ressources deviennent plus étendues et chaque analyse met plus de temps à s'exécuter.

Analyse dynamique

Utilisez l'analyse dynamique dans IBM QRadar Vulnerability Manager pour associer les scanners individuels à une adresse IP, à des plages CIDR, à des plages d'adresses IP ou à un domaine que vous spécifiez dans le profil d'analyse. L'analyse dynamique est particulièrement utile lorsque vous déployez plusieurs scanners. Par exemple, si vous déployez plus de 5 scanners, vous pouvez gagner du temps en utilisant l'analyse dynamique.

Les avantages offerts par l'implémentation d'une analyse dynamique dépendent de l'infrastructure de votre réseau et du nombre de scanners disponibles. Par exemple, si vous avez 10 scanners QRadar Vulnerability Manager et si vous n'utilisez pas l'analyse dynamique, vous devez configurer 10 travaux d'analyse individuels. QRadar Vulnerability Manager sélectionne le scanner approprié pour chaque adresse IP analysée.

Si l'analyse dynamique est utilisée dans votre profil d'analyse et si vous associez 2 scanners à un actif, le scanner qui inclut l'actif dans le plus petit sous-réseau correspondant obtient la priorité pour analyser l'actif en premier.

Par exemple, votre adresse IP d'actif est 10.2.2.3, le scanner A est assigné à la plage d'adresses CIDR 10.2.2.0/24 et le scanner B est assigné à l'adresse CIDR 10.2.2.3/32. Le scanner B est prioritaire pour analyser l'actif par rapport au scanner A car le sous-réseau (/32) constitue une correspondance exacte pour l'actif.

Avant d'activer l'analyse dynamique, exécutez des analyses test puis évaluez l'impact sur les ressources de votre réseau, la performance d'analyse et les durées d'analyse.

Tâches associées

Création d'un profil d'analyse

Bande passante du réseau pour les analyses d'actifs simultanées

En ajustant la configuration de la bande passante du réseau, vous pouvez modifier le nombre d'actifs pouvant être analysés simultanément et le nombre d'outils de vulnérabilité pouvant être utilisés simultanément pour analyser les actifs. Certaines analyses utilisent plusieurs outils de vulnérabilité pour analyser, ce qui affecte le nombre d'actifs pouvant être analysés en même temps.

La configuration de la bande passante du réseau peut aller d'une valeur basse de 200 Kbps à une valeur haute de 5000 Kbps. Configurez la définition de la bande passante dans l'onglet Détails d'un profil d'analyse. La définition par défaut de la bande passante du réseau est moyenne, à savoir 1000 Kbps.

Ajustez la bande passante conformément aux scénarios suivants :

- Réglez la bande passante du réseau sur 5000 Kbps (valeur haute) pour analyser les correctifs de jusqu'à 50 actifs à la fois ou conservez la configuration de 1000 Kbps (valeur moyenne) pour analyser les correctifs de 10 actifs à la fois.
- Utilisez la valeur de 5000 Kbps (valeur haute) si la bande passante de votre réseau est importante.
- N'utilisez pas la valeur 5000 Kbps en cas de connexion WAN lente.
- Si vous analysez à travers un pare-feu et qu'il s'agit d'une source de journal, le trafic d'analyse crée des événements et vous devez éventuellement réduire la bande passante du réseau pour éviter de dépasser votre seuil de licence EPS (événements par seconde).

Tâches associées

Création d'un profil d'analyse

Cartes d'interface réseau sur les scanners

Dans IBM QRadar Vulnerability Manager, l'analyse ne dépend pas des cartes d'interface réseau (NIC) configurées sur l'application du scanner.

Vous pouvez configurer plusieurs cartes d'interface réseau, en sachant que 4 ou 5 cartes correspondent à une configuration typique. QRadar Vulnerability Manager utilise des protocoles TCP/IP standard pour analyser une unité ayant une adresse IP. Si plusieurs cartes réseau (NIC) sont définies, l'analyse suit la configuration réseau standard sur un dispositif.

Si les actifs de destination que vous analysez appartiennent à des réseaux différents, configurez des cartes d'interface réseau individuelles pour la connexion aux différents réseaux.

Cette segmentation des réseaux à l'aide des cartes d'interface réseau permet au scanner de se connecter directement à différents réseaux. Par exemple, une interface Ethernet peut être configurée pour se connecter au réseau 10.100.85.0/24 et une deuxième interface Ethernet peut être configurée pour se connecter au réseau 192.168.0.0/24.

Gestion des vulnérabilités pour les propriétaires d'actifs

Assignez des propriétaires à vos actifs de manière à leur assigner les vulnérabilités détectées. Les vulnérabilités sont assignées avec une date d'échéance qui est calculée en fonction du niveau de risque de la vulnérabilité.

Configurez les rapports de résolutions que vous souhaitez envoyer aux propriétaires d'actifs en mettant en évidence les informations suivantes :

- Les correctifs qu'ils ont besoin d'installer.
- Les étapes requises pour résoudre la vulnérabilité.
- Les actifs dont les vulnérabilités sont arrivées à échéance.
- Les nouvelles vulnérabilités qui ont été détectées depuis la dernière analyse.

Les rapports de résolution standard sont disponibles dans l'onglet **E-mail** de la page **Configuration du profil d'analyse**. Vous pouvez créer des rapports client supplémentaires à l'aide des recherches QRadar Vulnerability Manager.

Sous l'onglet **Rapports**, vous pouvez créer un rapport de vulnérabilité et l'assigner à un groupe de rapports d'analyse. Vous pouvez configurer des destinataires pour ce rapport dans un profil d'analyse que vous pouvez afficher dans la fenêtre **Rapports disponibles** de l'onglet **Contenu de l'e-mail** de l'écran **Configuration du profil d'analyse**.

Utilisez les critères de recherche pour vous assurer que vos rapports se concentrent sur les activités de résolution des vulnérabilités qui répondent le mieux à vos besoins commerciaux et de conformité.

Pour faciliter la création de rapports de résolution, utilisez QRadar Vulnerability Manager pour créer automatiquement des vulnérabilités d'actifs et des rapports de vulnérabilité pour chaque propriétaire d'actif à partir d'une seule définition de rapport.

Lorsque les actifs sont réanalysés, les vulnérabilités résolues sont automatiquement détectées et signalées comme corrigées. Elles sont supprimées des rapports et des vues, à moins que la configuration ne spécifie le contraire. Les vulnérabilités précédemment corrigées et à nouveau détectées sont automatiquement rouvertes.

Tâches associées

Affectation d'un utilisateur technique comme propriétaire des groupes d'actifs

Envoi d'un e-mail aux propriétaires d'actif lors du démarrage et de l'arrêt des analyses de vulnérabilité
Envoyez un e-mail aux propriétaires techniques d'actif afin de les informer de la planification de l'analyse. Vous pouvez aussi envoyer des rapports aux propriétaires d'actif .

Recherche des données de vulnérabilité

Notifications des analyses de vulnérabilité

Pour éviter les fausses alarmes lorsque l'activité d'analyse est élevée, communiquez les durées d'analyse aux propriétaires des actifs.

Certains outils d'analyse QRadar Vulnerability Manager comme les outils Web peuvent générer une grande quantité de trafic. Par exemple, une analyse Web peut envoyer 500 requêtes HTTP par seconde à des serveurs HTTP. Si les propriétaires des actifs observent une augmentation anormale du trafic, ils peuvent penser que l'actif scanné fait l'objet d'une attaque DOS ou d'une attaque similaire.

Configurez les profils d'analyse pour envoyer des courriers électroniques aux propriétaires d'actifs et aux autres parties intéressées avant et après une analyse afin que les propriétaires des actifs sachent qu'une quantité anormale de trafic réseau ou de chargement peut se produire sur leur réseau. Une autre manière de leur communiquer les durées d'analyse des actifs est de planifier des heures d'analyse avec eux.

Configurez la notification par courrier électronique dans l'onglet **E-mail** du profil d'analyse.

Déclenchements d'analyses des nouveaux actifs

Utilisez des événements traitées par le moteur CRE (Custom Rules Engine) pour déclencher des analyses des nouveaux actifs lorsque de nouvelles adresses IP leur sont affectées.

Avant de commencer

Créez un profil d'analyse avec l'option d'**analyse à la demande** activée.

Procédure

1. Depuis l'onglet **Activité du journal**, cliquez sur **Règles** > **Règles**.

   Vous pouvez aussi accéder au menu de règles depuis les onglets **Infractions** et **Activité réseau**.
2. Depuis le menu **Actions** , cliquez sur **Nouvelle règle d'événement**.
3. Cliquez sur **Evénements**, puis sur **Suivant** pour continuer.
4. Ajoutez des tests à votre liste de règles.
   a) Cliquez sur l'icône d'ajout (**+**) en regard du test **when the events were detected by one or more of these log sources**.
   b) Cliquez sur l'icône d'ajout (**+**) en regard du test **when the event QID is one of the following QIDs**.
   c) Cliquez sur l'icône d'ajout (**+**) en regard du test **and when the source IP is one of the following IP addresses**.
5. Dans le volet **Règle**, éditez chaque valeur de règle.
   a) Pour la première règle, cliquez **these log sources** et ajoutez l'élément Profileur d'actif de la liste.
   b) Pour la seconde règle, cliquez sur **QID**, puis recherchez les QID qui sont décrits dans le tableau suivant et ajoutez-les à votre règle.

   Tableau 7. Noms et descriptions QID à ajouter à la règle

QID	Nom	Description
68750030	**Adresse IP d'actif créée**	Cet événement se produit lorsqu'un nouvel enregistrement d'adresse IP est créé pour un actif.
68750013	**Actif créé**	Cet événement se produit lorsqu'un nouvel actif est créé.

   c) Pour la troisième règle, cliquez sur **and** afin de choisir **and NOT**, puis cliquez sur **Adresses IP** et ajoutez 127.0.0.1

   Voici un exemple de sortie de cette configuration de règle :

   and NOT when the source IP is one of the following 127.0.0.1
6. Dans la zone de texte **Appliquer**, saisissez un nom unique pour cette règle, conservez **Local** comme paramètre système par défaut, puis cliquez sur **Suivant**.
7. Dans la section **Réponse à la règle**, cliquez sur **Déclencher l'analyse**.
   a) Dans le menu **Profil d'analyse à utiliser comme modèle**, sélectionnez le profil d'analyse que vous voulez utiliser.

   Vous devez sélectionner l'option d'**analyse à la demande** dans le profil d'analyse que vous voulez utiliser avec cette règle.
   b) Cliquez sur **Source** en regard de l'option **Environnements locaux à analyser**.
   c) Entrez des valeurs pour le paramètre **Limiteur de réponse**.

   Configurez des intervalles appropriés afin d'éviter une surcharge possible sur votre système.
   d) Si vous ne voulez pas commencer tout de suite à surveiller les événements, désélectionnez l'option **Activer la règle**, puis cliquez sur **Terminer**.

Configuration du risque environnemental pour un actif

Utilisez le score environnemental CVSS pour manipuler et définir la priorité du score de risque pour les actifs sélectionnés. Si vous configurez les paramètres **CVSS, poids et conformité** pour un actif, vous pouvez appliquer des scores de risque plus élevés pour les actifs qui sont plus importants ou critiques.

Pourquoi et quand exécuter cette tâche

Si vous avez des actifs importants ou critiques et des actifs moins importants ayant les mêmes vulnérabilités, vous pouvez définir une valeur plus élevée pour le score environnemental CVSS des actifs importants ou critiques. En procédant ainsi, vous mettez en évidence les actifs plus importants dans vos résultats d'analyse.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Cliquez deux fois sur l'actif à modifier puis cliquez sur **Modifier un actif**.
4. Cliquez sur **CVSS, poids et conformité** dans la fenêtre **Editer le profil d'actif**.
5. Configurez les paramètres dans le panneau **CVSS, poids et conformité**.

   Le tableau suivant présente les paramètres disponibles dans le panneau **CVSS, poids et conformité**.

Paramètre	Description
Dommages collatéraux potentiels	Risque de danger de mort ou de perte d'actifs physiques par endommagement ou vol. Si vous modifiez la valeur définie pour **Dommages collatéraux potentiels** (en remplaçant **Faible** par **Elevé**), la valeur calculée pour **Score CVSS** augmente. Le paramètre **Dommages collatéraux potentiels** est directement lié au paramètre **Poids**. Si vous changez un paramètre, cela a des conséquences sur l'autre paramètre.
Exigences de confidentialité	Impact en matière de confidentialité pour cet actif lorsqu'une vulnérabilité est exploitée. Si vous modifiez la valeur définie pour les exigences de confidentialité (en remplaçant **Faible** par **Elevé**, par exemple), la valeur calculée de **Score CVSS** augmente.
Exigences de disponibilité	Impact pour la disponibilité de l'actif lorsqu'une vulnérabilité est exploitée. Les attaques qui consomment de la bande passante réseau, des cycles de processeur ou de l'espace disque ont un impact sur la disponibilité d'un actif. Si vous modifiez la valeur définie pour les exigences de disponibilité (en remplaçant **Faible** par **Elevé**, par exemple), la valeur calculée de **Score CVSS** augmente.

Paramètre	Description
Exigences d'intégrité	Impact pour l'intégrité de l'actif lorsqu'une vulnérabilité est exploitée. L'intégrité fait référence à la fiabilité et la véracité des informations. Si vous modifiez la valeur définie pour les exigences d'intégrité (en remplaçant **Faible** par **Elevé**, par exemple), la valeur calculée de **Score CVSS** augmente.
Poids	Le paramètre **Poids** est lié au paramètre **Dommages collatéraux potentiels**. Si vous sélectionnez 10 pour le paramètre **Poids**, la valeur **Elevé** est attribuée à **Dommages collatéraux potentiels**.

6. Cliquez sur **Sauvegarder**.

Analyse externe - Foire aux questions

Analysez les actifs de votre DMZ ou périmètre réseau du cloud à l'aide d'un scanner externe hébergé par IBM. Exécutez des analyses sans données d'identification depuis l'extérieur de votre réseau afin de disposer d'une défense supplémentaire pour protéger vos actifs d'une attaque externe.

Quelles informations devez-vous fournir ?

Vous devez adresser un e-mail à QRadar-QVM-Hosted-Scanner@hursley.ibm.com avec les informations suivantes :

- Adresse IP externe de votre organisation.
- Si vous utilisez des équilibrages de charge, vous devez fournir les adresses IP qui sont utilisées par ces derniers.
- Plage d'adresse IP des actifs dans votre DMZ.

Remarque : Vous devez disposer d'une installation locale de QRadar Vulnerability Manager.

L'équipe QRadar vérifie-t-elle la plage CIDR qui est fournie ?

La plage CIDR ainsi que la propriété sont vérifiés avant d'exécuter une analyse.

Quel est l'impact de l'analyse externe sur les serveurs (serveurs Web, par exemple) ?

L'analyse n'est pas intrusive mais elle exerce une certaine charge sur vos systèmes. Exécutez l'analyse lorsque les serveurs ne sont pas très actifs.

Comment les résultats de l'analyse sont-ils envoyés du cloud vers le processeur QRadar Vulnerability Manager ?

Le scanner externe envoie les résultats d'analyse du cloud vers le processeur QRadar Vulnerability Manager via une connexion sécurisée.

Quel est le rôle de App Scan dans le scanner externe ?

App Scan analyse le script intersite (XSS) et les vulnérabilités OWASP (Open Web Application Security Project) sur les serveurs Web. Vous devez fournir les noms des domaines virtuels.

Faut-il utiliser un scanner interne en plus du scanner externe pour analyser le DMZ ?
La plupart des attaques réseau proviennent de l'extérieur, le scanner externe cible donc toutes les zones d'attaques externes d'un point de vue extérieur.

Il est conseillé d'exécuter des analyses externes et des analyses authentifiées en interne dans votre DMZ car les pare-feux restreignent parfois l'accès à des vulnérabilités, des ports, des services et des hôtes.

Si vous utilisez un programme d'équilibrage de charge pour le trafic entrant, il est possible que le scanner externe n'ait accès qu'à un seul des serveurs connectés au programme d'équilibrage de charge. Dans ce cas, vous devrez peut-être configurer une route d'accès de sorte que le scanner externe puisse analyser tous les serveurs. Vous pouvez aussi utiliser un scanner interne pour analyser ces serveurs dans votre DMZ.

Chapitre 5. Configuration des analyses

Dans IBM QRadar Vulnerability Manager, toutes les analyses de réseau sont contrôlées par les profils d'analyse que vous créez. Vous pouvez créer plusieurs profils d'analyse et configurer chaque profil différemment en fonction des exigences spécifiques de votre réseau.

Profils d'analyse

Utilisez les profils d'analyse pour exécuter les tâches suivantes :

- Spécifiez les noeuds, les domaines ou les domaines virtuels du réseau à analyser.
- Spécifiez les actifs réseau à exclure des analyses.
- Créez des fenêtres opérationnelles, qui définissent les heures auxquelles les analyses peuvent être effectuées.
- Exécutez manuellement les profils d'analyses ou planifiez l'exécution d'une analyse à une date ultérieure.
- Exécutez, suspendez, reprenez, annulez ou supprimez une seule ou plusieurs analyses.
- Utilisez les données d'identification centralisées pour exécuter des systèmes d'exploitation Windows, UNIX ou Linux.
- Analysez les actifs d'une recherche d'actifs enregistrée.

Concepts associés

Ensembles de données d'identification centralisés

Création d'un profil d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer les profils d'analyse pour spécifier comment et quand les actifs de votre réseau seront analysés en vue de détecter des vulnérabilités.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. En outre, vous pouvez également configurer les paramètres facultatifs suivants.

   - Si vous avez ajouté d'autres scanners à votre déploiement QRadar Vulnerability Manager, sélectionnez un scanner de la liste **Serveur d'analyse**. Cette étape n'est pas nécessaire si vous souhaitez utiliser l'analyse dynamique.
   - Pour activer ce profil pour l'analyse à la demande, cliquez sur la case à cocher **Analyse à la demande activée**.

     En sélectionnant cette option, vous mettez à disposition le profil à utiliser si vous voulez déclencher une analyse en réponse à un événement de règle personnalisée. Elle permet également une analyse de vulnérabilité à la demande en utilisant le menu contextuel sur la page **Actifs**.
   - En sélectionnant la case **Sélection de serveur dynamique**, vous pouvez choisir le scanner disponible le plus approprié. Assurez-vous que vous définissez les scanners dans la page **Administrative** > **Scanners**.

© Copyright IBM Corp. 2012, 2020

Les profils de sécurité doivent être mis à jour avec un domaine associé. Les restrictions de niveau domaine ne sont pas appliquées tant que les profils de sécurité ne sont pas mis à jour et les modifications ne sont pas déployées.

- Pour analyser votre réseau en utilisant un jeu prédéfini de critères d'analyse, sélectionnez un type d'analyse dans la liste **Politiques d'administration d'analyse**.
- Si vous avez configuré des données d'identification centralisées pour les actifs, sélectionnez la case à cocher **Utiliser les données d'identification centralisées**. Pour plus d'informations, voir *IBM QRadar Administration Guide*.

4. Cliquez sur **Sauvegarder**.

Concepts associés

Bande passante du réseau pour les analyses d'actifs simultanées
En ajustant la configuration de la bande passante du réseau, vous pouvez modifier le nombre d'actifs pouvant être analysés simultanément et le nombre d'outils de vulnérabilité pouvant être utilisés simultanément pour analyser les actifs. Certaines analyses utilisent plusieurs outils de vulnérabilité pour analyser, ce qui affecte le nombre d'actifs pouvant être analysés en même temps.

Analyse dynamique
Utilisez l'analyse dynamique dans IBM QRadar Vulnerability Manager pour associer les scanners individuels à une adresse IP, à des plages CIDR, à des plages d'adresses IP ou à un domaine que vous spécifiez dans le profil d'analyse. L'analyse dynamique est particulièrement utile lorsque vous déployez plusieurs scanners. Par exemple, si vous déployez plus de 5 scanners, vous pouvez gagner du temps en utilisant l'analyse dynamique.

Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager

Politiques d'administration d'analyse

Analyses de vulnérabilité dynamiques
Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse afin d'utiliser certains programmes d'analyse des vulnérabilités pour des plages CIDR spécifiques dans votre réseau. Par exemple, vos programmes d'analyse pourraient n'avoir accès qu'à certaines zones de votre réseau.

Tâches associées

Association de programmes d'analyse des vulnérabilités à des plages CIDR
Dans IBM QRadar Vulnerability Manager, pour effectuer une analyse dynamique, vous devez associer des programmes d'analyse des vulnérabilités à différents segments de votre réseau.

Nouvelle analyse d'un actif à l'aide de l'option de menu contextuel

Configuration d'une politique d'analyse
Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une politique d'analyse pour répondre à toutes les exigences spécifiques de vos analyses de vulnérabilité. Vous pouvez copier et renommer une politique d'analyse préconfigurée ou vous pouvez ajouter une nouvelle politique d'analyse. Vous ne pouvez pas modifier une politique d'analyse préconfigurée.

Création d'un profil d'analyse de scanner externe

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer des profils d'analyse afin d'utiliser un scanner hébergé pour analyser des actifs dans votre zone démilitarisée.

Avant de commencer

QRadar Vulnerability Manager doit être configuré avec un scanner hébergé. Pour plus d'informations, voir «Analyse des actifs de votre zone démilitarisée», à la page 10.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.

Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. Pour créer un profil de scanner externe, vous devez également suivre les étapes restantes de cette procédure.

4. Sélectionnez un scanner externe dans la liste **Serveur d'analyse**.
5. Sélectionnez **Analyse complète** ou **Analyse Web** dans la liste **Politiques d'administration d'analyse**.
6. Cliquez sur l'onglet concernant le **domaine et l'application Web**. Dans le panneau des **toiles virtuelles**, entrez les informations relatives au domaine et à l'adresse IP pour les sites Web et les applications que vous voulez analyser.
7. Cliquez sur **Sauvegarder**.

Remarque : Aucune analyse authentifiée n'est effectuée depuis le scanner externe.

Création d'un profil de test de performances

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

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter un benchmark**.
4. Si vous voulez utiliser des données d'identification prédéfinies, sélectionnez la case à cocher **Utiliser les données d'identification centralisées**.

   Les données d'identification qui sont utilisées pour l'analyse des systèmes Linux doivent disposer de droits root. Les données d'identification qui sont utilisées pour l'analyse des systèmes Windows doivent disposer de droits d'administrateur.
5. Si vous n'utilisez pas l'analyse dynamique, sélectionnez le scanner QRadar Vulnerability Manager dans la liste **Serveur d'analyse**.
6. Pour activer l'analyse dynamique, cliquez sur la case **Sélection de serveur dynamique**.

   Si vous avez configuré des domaines dans la fenêtre **Admin** > **Gestion des domaines**, vous pouvez sélectionner un domaine dans la liste **Domaines**. Seuls les actifs dans les plages de CIDR et les domaines qui sont configurés pour vos scanners sont analysés.
7. Sous l'onglet **Quand analyser**, définissez le planning d'exécution, l'heure de début d'analyse et les éventuelles périodes d'exécution définies.
8. Sous l'onglet **E-mail**, définissez les informations à envoyer à propos de cette analyse et à qui les envoyer.
9. Si vous n'utilisez pas des données d'identification centralisées, ajoutez les données d'identification nécessaires à l'analyse sous l'onglet **Données d'identification supplémentaires**.

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

Concepts associés

Ensembles de données d'identification centralisés

Exécution manuelle de profils d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez exécuter manuellement un ou plusieurs profils d'analyse.

Vous pouvez également planifier des analyses de sorte qu'elles soient exécutées à une date et une heure ultérieures. Pour plus d'informations, voir «Planification des analyses», à la page 44.

Avant de commencer

Vérifiez qu'un processeur de vulnérabilité est déployé. Pour plus d'informations, voir «Vérification du déploiement d'un processeur de vulnérabilité», à la page 7.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
3. Sur la page **Profils d'analyse**, activez la case à cocher dans la ligne attribuée aux profils de l'analyse que vous souhaitez exécuter.

   Remarque : Pour trouver les profils d'analyse que vous souhaitez exécuter, utilisez la zone de barre d'outils **Nom** pour filtrer les profils d'analyse par nom.
4. Dans la barre d'outils, cliquez sur **Exécuter**.

   Par défaut, des analyses rapides sont effectuées via les protocoles TCP et UDP. Une analyse rapide inclut plus de ports dans la plage 1 - 1024.

Concepts associés

Détails relatifs au profil d'analyse

Tâches associées

Gestion des résultats d'analyse

Nouvelle analyse d'un actif à l'aide de l'option de menu contextuel

Dans IBM QRadar Vulnerability Manager, vous pouvez effectuer rapidement une nouvelle analyse d'un actif à l'aide de l'option de menu contextuel.

L'option d'analyse clic droit est également disponible dans l'onglet **Infractions** de QRadar, ou la vue d'actif de sous-réseau de QRadar Risk Manager.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez **Gérer les vulnérabilités** > **Par actif**.
3. Sur la page **Par actif**, identifiez l'actif que vous souhaitez analyser à nouveau.
4. Cliquez avec le bouton droit de la souris sur **Adresse IP**, puis sélectionnez **Exécuter une analyse de vulnérabilité**.
5. Dans la fenêtre **Exécuter une analyse de vulnérabilité**, sélectionnez le profil d'analyse que vous souhaitez utiliser lors de la nouvelle analyse de l'actif.

   Le processus d'analyse nécessite un profil d'analyse. Ce profil détermine les options de configuration qui sont utilisées lors de l'exécution de l'analyse.

   Pour afficher un profil d'analyse dans la fenêtre **Exécuter une analyse de vulnérabilité**, vous devez sélectionner la case à cocher **Analyse à la demande activée** dans l'onglet **Détails** dans la page **Configuration du profil d'analyse**.

   Important : Le profil d'analyse que vous sélectionnez peut être associé à plusieurs cibles d'analyse ou plages d'adresses IP. Toutefois, lorsque vous utilisez l'option du menu contextuel, seul l'actif que vous sélectionnez est analysé.
6. Cliquez sur **Analyser maintenant**.
7. Cliquez sur **Fermer la fenêtre**.
8. Pour consultez la progression de l'analyse contextuelle, dans le volet de navigation, cliquez sur **Résultats de l'analyse**.

   Les analyses contextuelles sont identifiées par le préfixe **RC:**.

Concepts associés

Vulnérabilités des actifs

Détails relatifs au profil d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez décrire votre analyse, sélectionner le scanner à utiliser, ainsi qu'un certain nombre d'options de politique d'analyse.

Les détails de profil d'analyse sont spécifiés dans l'onglet **Détails**, sur la page **Configuration du profil d'analyse**.

Vérifiez plus particulièrement les options suivantes :

Tableau 8. Options de configuration des détails du profil d'analyse

Options	Description
Utilisez les données d'identification centralisées	Indique que le profil utilise des droits d'accès prédéfinis. Les informations d'identification centralisées sont définies dans la fenêtre **Admin** > **Configuration système** > **Données d'identification centralisées**.
Serveur d'analyse	Le scanner sélectionné dépend de la configuration de votre réseau. Par exemple, pour analyser des actifs de la zone démilitarisée, sélectionnez un scanner ayant accès à cette zone de votre réseau. Le serveur d'analyse **Controller** est déployé avec le processeur de vulnérabilité sur votre console QRadar ou hôte géré QRadar Vulnerability Manager. **Restriction :** Un seul processeur de vulnérabilité est autorisé dans votre déploiement. Vous pouvez toutefois déployer plusieurs programmes d'analyse sur des dispositifs de programmes d'analyse d'hôtes gérés QRadar Vulnerability Manager dédiés ou sur des hôtes gérés QRadar.
Analyse à la demande	Permet l'analyse à la demande des actifs pour le profil. Utilisez le menu contextuel sur la page **Actifs** pour effectuer une analyse de vulnérabilité à la demande. En sélectionnant cette option, vous mettez également à disposition le profil à utiliser si vous voulez déclencher une analyse en réponse à un événement de règle personnalisée. En permettant l'analyse à la demande, vous activez également l'analyse dynamique.
Sélection de serveurs dynamiques	Permet d'indiquer si vous voulez utiliser un scanner de vulnérabilité distinct pour chaque plage CIDR que vous analysez. Lors d'une analyse, QRadar Vulnerability Manager distribue automatiquement l'activité d'analyse au programme d'analyse approprié pour chaque plage CIDR spécifiée. Si vous avez configuré des domaines dans la fenêtre **Gestion des domaines** de l'onglet **Admin**, vous pouvez également sélectionner le domaine que vous souhaitez analyser.
Limite de la bande passante	Bande passante de l'analyse. Le paramètre par défaut est medium. **Important :** La sélection d'une valeur supérieure à 1 000 kbit/s risque d'affecter les performances du réseau.
Politiques d'administration d'analyse	Critères d'analyse préconfigurés relatifs aux ports et aux protocoles. Pour plus d'informations, voir «Politiques d'administration d'analyse», à la page 53.

Concepts associés

Analyses de vulnérabilité dynamiques

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse afin d'utiliser certains programmes d'analyse des vulnérabilités pour des plages CIDR spécifiques dans votre réseau. Par exemple, vos programmes d'analyse pourraient n'avoir accès qu'à certaines zones de votre réseau.

Politiques d'administration d'analyse

Tâches associées

Création d'un profil d'analyse à la demande

Pour déclencher une analyse en réponse à un événement de règle personnalisée, configurez un profil d'analyse à la demande et activez l'analyse dynamique.

Planification des analyses

Dans IBM QRadar Vulnerability Manager, vous pouvez planifier les dates et les heures auxquelles vous souhaitez analyser vos actifs réseau pour rechercher des vulnérabilités connues.

La planification d'analyse est contrôlée via le panneau **Quand analyser** de la page **Configuration du profil d'analyse***. Un profil d'analyse configuré avec un paramètre manuel doit être exécuté manuellement. Cependant, les profils d'analyse qui ne sont pas configurés comme des analyses manuelles, peuvent également être exécutés manuellement. Lorsque vous sélectionnez une planification d'analyse, vous pouvez affiner votre planification à l'aide des fenêtres opérationnelles pour configurer des heures d'analyses autorisées.

Sélectionnez l'une des options de planification suivantes :

- Manuel
- Exécuter une fois
- Quotidienne
- Hebdomadaire
- Mensuelle
- Avancé

  Utilisez les expressions cron pour créer des planifications, par exemple : à 9h00 du lundi au vendredi, ou à 3h30 le premier vendredi de chaque mois. Les expressions cron vous offrent la possibilité de créer des planifications d'analyse irrégulières. Planifiez une analyse par jour au maximum.

Tenez compte de l'impact du passage à l'heure d'été sur vos planifications d'analyse **Exécuter une fois**, **Quotidien**, **Hebdomadaire** et **Mensuel**. Par exemple, le 27 mars 2016, l'heure du Royaume-Uni avance d'1 heure à 1h00 du matin, de sorte que toutes les analyses configurées pour s'exécuter entre 1h00 et 1h59 le 27 mars 2016 s'exécutent entre 2h00 et 2h59.

Les planifications d'analyses **avancées** configurées pour s'exécuter entre 1h00 et 1h59 le 27 mars 2016 seront ignorées et ne seront pas exécutées. Toutes les analyses suivantes s'exécuteront aux heures planifiées.

Tâches associées

Configuration d'un intervalle d'analyse autorisé

Consultation des analyses planifiées au format agenda

Analyse des domaines sur une base mensuelle

Dans IBM QRadar Vulnerability Manager, Vous pouvez configurer un profil d'analyse des domaines de votre réseau tous les mois.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.

3. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. Pour configurer des analyses mensuelles, vous devez également suivre les étapes restantes de cette procédure.
4. Cliquez sur le panneau **Quand analyser**.
5. Dans la liste **Exécuter la planification**, sélectionnez **Mensuelle**.
6. Dans la zone **Heure de début**, sélectionnez la date et l'heure de début de votre analyse.
7. Dans la zone **Jour du mois**, sélectionnez un jour pour chaque mois au cours duquel votre analyse s'exécute.
8. Cliquez sur l'onglet concernant le **domaine et l'application Web**.
9. Dans la zone **Domaines**, entrez l'adresse URL de l'actif que vous voulez analyser et cliquez sur (**>**).
10. Cliquez sur **Sauvegarder**.
11. Au cours et à la fin de l'analyse, vous pouvez surveiller la progression de l'analyse et contrôler les analyses terminées.

Planification des analyses des nouveaux actifs non analysés

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer les analyses planifiées des actifs réseau non analysés découverts récemment.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, cliquez sur **Profils d'actifs** puis, dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
3. Pour spécifier les actifs non analysés découverts récemment, exécutez les étapes suivantes dans le panneau **Paramètres de recherche** :
   a) Sélectionnez **Jours depuis la détection de l'actif**, **Inférieur à 2**, puis cliquez sur **Ajouter un filtre**.
   b) Sélectionnez **Jours depuis l'analyse de l'actif**, **Supérieur à 2**, puis cliquez sur **Ajouter un filtre**.
   c) Cliquez sur **Rechercher**.
4. Dans la barre d'outils, cliquez sur **Sauvegarder les critères**, puis suivez les étapes suivantes :
   a) Dans la zone **Entrez le nom de cette recherche**, entrez le nom de votre recherche d'actifs.
   b) Cliquez sur **Inclure dans mes recherches rapides**.
   c) Cliquez sur **Partager avec tout le monde**.
   d) Cliquez sur **OK**.
5. Cliquez sur l'onglet **Vulnérabilités**.
6. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
7. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. Pour programmer des analyses pour les actifs non analysés, vous devez également suivre les étapes restantes de cette procédure.
8. Dans le panneau **Inclure les recherches sauvegardées**, sélectionnez votre recherche enregistrée d'actifs dans la liste **Recherches sauvegardées disponibles** et cliquez sur (**>**).
9. Cliquez sur le panneau **Quand analyser**, puis dans la liste **Exécuter la planification**, sélectionnez **Hebdomadaire**.
10. Dans les zones **Heure de début**, entrez ou sélectionnez la date et l'heure d'exécution de votre analyse chaque jour.
11. Cochez les cases correspondant aux jours de la semaine où vous souhaitez que votre analyse soit exécutée.
12. Cliquez sur **Sauvegarder**.

Pour plus d'informations sur l'utilisation de l'onglet **Actifs** et sur l'enregistrement des recherches d'actifs, voir le *Guide d'utilisation* de votre produit.

Tâches associées

Recherche des données de vulnérabilité

Consultation des analyses planifiées au format agenda

Dans IBM QRadar Vulnerability Manager, l'agenda des analyses planifiées fournit un emplacement central auquel vous pouvez consulter des informations sur les analyses planifiées.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le volet de navigation, cliquez sur l'option d'**administration** > **Analyses planifiées**.
3. Passez la souris sur l'analyse planifiée pour afficher les informations sur l'analyse planifiée.

   Par exemple, vous pouvez afficher le temps qu'une analyse a pris.
4. Double-cliquez sur une analyse planifiée pour modifier le profil d'analyse.

Cibles d'analyse réseau et exclusions

Dans IBM QRadar Vulnerability Manager, vous pouvez fournir des informations relatives aux actifs, aux domaines ou aux toiles virtuelles sur le réseau que vous souhaitez analyser.

Pour spécifier les actifs du réseau à analyser, utilisez l'onglet **Détails** sur la page **Configuration du profil d'analyse**.

Vous pouvez exclure un hôte spécifique ou une plage d'hôtes à ne jamais analyser. Par exemple, vous pouvez empêcher l'exécution d'une analyse sur des serveurs critiques hébergeant les applications de votre production. Vous pouvez également souhaiter configurer votre analyse pour cibler uniquement les zones spécifiques de votre réseau.

QRadar Vulnerability Manager s'intègre à QRadar en offrant la possibilité d'analyser les actifs faisant partie d'une recherche d'actif enregistrée.

Cibles d'analyse

Vous pouvez spécifier vos cibles d'analyse en définissant une plage CIDR, une adresse IP, une plage d'adresses IP ou une combinaison des trois.

Analyse des domaines

Vous pouvez ajouter des domaines à votre profil d'analyse pour tester les transferts de zone DNS sur chacun des domaines spécifiés.

Un hôte peut utiliser le transfert de zone DNS pour demander et recevoir un transfert de zone complet concernant un domaine. Le transfert de zone est un problème de sécurité car les données DNS sont utilisées pour déchiffrer la topologie de votre réseau. Les données contenues dans un transfert de zone DNS étant sensibles, toute exposition de celles-ci peut être perçue comme une vulnérabilité. Les informations obtenues peuvent être utilisées à des fins malveillantes comme la mauvaise utilisation ou l'usurpation DNS.

Analyses utilisant des recherches d'actifs enregistrées

Vous pouvez analyser les actifs et les adresses IP associés à une QRadar recherche d'actif enregistrée.

Les recherches enregistrées sont affichées dans la section **Recherche sauvegardée des actifs** de l'onglet **Détails**.

Pour plus d'informations sur l'enregistrement d'une recherche d'actifs, voir le *Guide d'utilisation* de votre produit.

Exclusion de cibles d'analyse réseau

Dans la section **Actifs exclus** de l'onglet **Domaine et l'application Web**, vous pouvez spécifier les adresses IP, les plages d'adresses IP, ou les plages CIDR pour les actifs qui ne doivent pas être analysés. Par exemple, si vous souhaitez éviter l'analyse d'un serveur très chargé, instable ou sensible, excluez ces actifs.

Lorsque vous configurez une exclusion d'analyse d'une configuration du profil d'analyse, l'exclusion s'applique uniquement au profil d'analyse.

Toiles virtuelles

Vous pouvez configurer un profil d'analyse pour analyser les adresses URL qui sont hébergées sur la même adresse IP.

Lorsque vous effectuez une analyse d'une toile virtuelle, QRadar Vulnerability Manager vérifie chaque page Web afin d'y détecter les vulnérabilités liées à l'injection SQL et au scriptage de site croisé.

Tâches associées

Analyse de plages CIDR avec différents programmes d'analyse des vulnérabilités
Dans IBM QRadar Vulnerability Manager, vous pouvez analyser des zones de votre réseau avec différents programmes d'analyse des vulnérabilités.

Exclusion d'actifs de toutes les analyses
Dans IBM QRadar Vulnerability Manager, les exclusions d'analyse spécifient les actifs de votre réseau qui ne sont pas analysés.

Planification des analyses des nouveaux actifs non analysés

Analyse des domaines sur une base mensuelle

Exclusion d'actifs de toutes les analyses

Dans IBM QRadar Vulnerability Manager, les exclusions d'analyse spécifient les actifs de votre réseau qui ne sont pas analysés.

Pourquoi et quand exécuter cette tâche

Les exclusions d'analyse s'appliquent à toutes les configurations de profil d'analyse et peuvent être utilisées pour exclure une activité d'analyse des serveurs instables ou sensibles. Utilisez la zone **Adresses IP** dans la page **Exclusions de l'analyse** pour entrer les adresses IP, les plages d'adresses IP, ou les plages CIDR que vous voulez exclure de toutes les analyses. Pour accéder à la page **Exclusions de l'analyse** :

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Exclusions de l'analyse**.
3. Dans la barre d'outils, sélectionnez **Actions** > **Ajouter**.

   Remarque : Vous pouvez également utiliser la section **Actifs exclus** de l'onglet **Vulnérabilités** > **Administration** > **Profils d'analyse** > **Ajouter** > **Domaine et l'application Web** pour exclure des actifs d'un profil d'analyse particulier.

Gestion des exclusions d'analyse

Dans IBM QRadar Vulnerability Manager vous pouvez mettre à jour, supprimer ou imprimer des exclusions d'analyse.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Exclusions de l'analyse**.
3. Dans la liste figurant sur la page **Exclusions de l'analyse**, cliquez sur l'exclusion que vous souhaitez modifier dans la zone **Exclusions de l'analyse**.
4. Dans la barre d'outils, sélectionnez une option dans le menu **Actions**.
5. En fonction de votre sélection, suivez les instructions à l'écran pour effectuer cette tâche.

Analyse des protocoles et des ports

Dans IBM QRadar Vulnerability Manager, vous pouvez choisir plusieurs protocoles d'analyse et analyser différentes plages de ports.

Vous pouvez configurer vos protocoles de port de profil d'analyse en utilisant les options d'analyse TCP et UDP.

Configurez les protocoles d'analyse et les ports que vous souhaitez analyser sur l'onglet **Analyse du port** de la fenêtre de configuration d'une politique d'administration d'analyse nouvelle ou existante.

Remarque : Vous pouvez également configurer l'analyse de port à partir de l'onglet **Comment analyser** de la fenêtre **Configuration du profil d'analyse** mais cette option est uniquement activée pour la compatibilité avec les versions antérieures. N'utilisez pas l'onglet **Comment analyser** pour configurer les nouvelles analyses de ports.

Analyse d'une plage entière de port

Dans IBM QRadar Vulnerability Manager, vous pouvez analyser la plage entière de port sur les actifs que vous indiquez.

Pourquoi et quand exécuter cette tâche

Créez une politique d'administration d'analyse pour spécifier les ports que vous souhaitez analyser, puis ajoutez cette politique d'administration d'analyse à un profil d'analyse que vous pouvez utiliser pour exécuter l'analyse.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Politiques d'administration d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter** pour créer une nouvelle politique d'administration d'analyse ou sur **Editer** pour modifier une politique existante.
4. Cliquez sur l'onglet **Paramètres**.
   a) Entrez un nom et une description pour la politique d'administration d'analyse.
   b) Sélectionnez le type d'analyse.
5. Cliquez sur l'onglet **Analyse du port**.
6. Dans la zone **Protocole**, sélectionnez un protocole. Les valeurs par défaut sont **TCP & UDP**.

   Remarque : Les analyses du port UDP sont bien plus lentes que celles du port TCP en raison du mode de fonctionnement du port UDP. Une analyse de port UDP peut mettre 24 heures à analyser tous les ports (1-65535) sur un actif.
7. Dans la zone **Plage**, tapez **1-65535**.

   Restriction : Les plages de ports doivent être séparées par un tiret, délimitées par une virgule, consécutives, dans l'ordre croissant et ne pas se chevaucher. Plusieurs plages de ports doivent être séparées par une virgule. Les exemples suivants montrent les délimiteurs qui sont utilisés pour entrer les plages de ports : (1-1024 1055, 2000-65535).

8. Dans la zone **Délai d'attente (m)**, entrez le délai, en minutes, après lequel vous souhaitez que l'analyse soit annulée si aucun résultat d'analyse n'est détecté.

   Important : Vous pouvez entrer n'importe quelle valeur dans la plage 1 - 500. Veillez à ne pas entrer un délai trop court, autrement l'analyse des ports ne peut pas détecter tous les ports en cours d'exécution. Les résultats d'analyse détectés avant la période d'expiration sont affichés.
9. Facultatif : Configurez plus d'options sur les autres onglets si vous souhaitez utiliser la politique d'administration d'analyse pour effectuer d'autres tâches.
10. Cliquez sur **Sauvegarder**.
11. Sur la page **Profil d'analyse**, créez un nouveau profil d'analyse.
    a) Ajoutez la politique d'analyse que vous venez de sauvegarder.
    b) Configurez les paramètres restants du profil d'analyse et sauvegardez.
    c) Sur la page **Profil d'analyse**, sélectionnez le nouveau profil d'analyse puis cliquez sur **Exécuter** dans la barre d'outils pour exécuter l'analyse.

    Pour en savoir plus sur la création d'un profil d'analyse, voir «Création d'un profil d'analyse», à la page 39.

    Remarque : Vous pouvez également configurer l'analyse de port à partir de l'onglet **Comment analyser** de la fenêtre **Configuration du profil d'analyse** mais cette option est uniquement activée pour la compatibilité avec les versions antérieures. N'utilisez pas l'onglet **Comment analyser** pour configurer les nouvelles analyses de ports.

Analyse d'actifs avec des ports ouverts

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer un profil d'analyse de façon à pouvoir analyser des actifs avec des ports ouverts.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, cliquez sur **Profils d'actifs** puis, dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
3. Pour spécifier les actifs ayant des ports ouverts, configurez les options suivantes dans le panneau **Paramètres de recherche** :
   a) Sélectionnez **Actifs avec port ouvert** et **Est égal à 80**, puis cliquez sur **Ajouter un filtre**.
   b) Sélectionnez **Actifs avec port ouvert** et **Est égal à 8080**, puis cliquez sur **Ajouter un filtre**.
   c) Cliquez sur **Rechercher**.
4. Dans la barre d'outils, cliquez sur **Sauvegarder les critères** et configurez les options suivantes :
   a) Dans la zone **Entrez le nom de cette recherche**, entrez le nom de votre recherche d'actifs.
   b) Cliquez sur **Inclure dans mes recherches rapides**.
   c) Cliquez sur **Partager avec tout le monde**, puis sur **OK**.
5. Cliquez sur l'onglet **Vulnérabilités**.
6. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
7. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. Pour analyser les actifs avec des ports ouverts, vous devez également suivre les étapes restantes de cette procédure.
8. Dans l'onglet **Détails**, sélectionnez votre recherche enregistrée d'actifs dans la liste **Recherches sauvegardées disponibles** et cliquez sur **>**.

   Lorsque vous incluez une recherche d'actifs sauvegardée dans votre profil d'analyse, les actifs et les adresses IP associés aux critères de recherche sont analysés.

9. Cliquez sur le panneau **Quand analyser**, puis dans la liste **Exécuter la planification**, sélectionnez **Manuelle**.
10. Cliquez sur le panneau **Eléments à analyser**.
11. Cliquez sur **Sauvegarder**.

    Pour plus d'informations sur l'enregistrement d'une recherche d'actifs, voir le *Guide d'utilisation* de votre produit.

Que faire ensuite

Exécuter les étapes dans la procédure, «Exécution manuelle de profils d'analyse», à la page 41.

Configuration d'un intervalle d'analyse autorisé

Dans IBM QRadar Vulnerability Manager, vous pouvez créer une fenêtre opérationnelle pour indiquer les heures auxquelles une analyse peut s'exécuter.

Pourquoi et quand exécuter cette tâche

Si une analyse ne se termine pas dans la fenêtre opérationnelle, elle est interrompue et continue lorsque la fenêtre opérationnelle s'ouvre à nouveau. Pour configurer une fenêtre opérationnelle :

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Fenêtre opérationnelle**.
3. Dans la barre d'outils, cliquez sur **Actions** > **Ajouter**.
4. Tapez un nom pour définir le créneau opérationnel dans la zone **Nom**.
5. Choisissez une planification pour les fenêtres opérationnelles dans la liste des **planifications**.
6. Sélectionnez les heures où l'analyse est autorisée.
7. Sélectionnez votre fuseau horaire.
8. Si vous avez sélectionné **Hebdomadaire** dans la liste des **planifications**, cochez les jours de la semaine dans le panneau **Hebdomadaire**.
9. Si vous avez sélectionné **Mensuelle** dans la liste des **planifications**, sélectionnez un jour dans la liste **Jour du mois**.
10. Cliquez sur **Sauvegarder**.

    Les fenêtres opérationnelles peuvent être associées à des profils d'analyse à l'aide de l'onglet **Quand analyser** dans la page **Configuration du profil d'analyse**.

    Si vous affectez deux fenêtres opérationnelles se chevauchant à un profil d'analyse, celle-ci s'exécute du début de la première fenêtre opérationnelle à la fin de la seconde fenêtre opérationnelle. Par exemple, si vous configurez deux fenêtres quotidiennes opérationnelles pour les périodes entre 1h et 6h et entre 5h et 9h, l'analyse s'exécute entre 1h et 9h.

    Pour les fenêtres opérationnelles qui ne se chevauchent pas, l'analyse commence à partir de l'heure de début de la première fenêtre opérationnelle et se met sur pause s'il existe un écart entre les deux fenêtres, puis reprend à partir de l'heure de début de la fenêtre suivante.

Analyses durant les heures autorisées

Dans IBM QRadar Vulnerability Manager, vous pouvez planifier une analyse des actifs de réseau aux heures indiquées, à l'aide d'une fenêtre opérationnelle.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.

2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Créneaux opérationnels**.
3. Dans la barre d'outils, sélectionnez **Actions** > **Ajouter**.
4. Entrez un nom pour votre fenêtre opérationnelle, configurez un intervalle de temps autorisé et cliquez sur **Sauvegarder**.
5. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
6. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. Pour configurer une analyse pendant les heures autorisées, vous devez également suivre les étapes restantes de cette procédure.
7. Cliquez sur l'onglet **Quand analyser**.
8. Dans la liste **Exécuter la planification**, sélectionnez **Quotidienne**.
9. Dans les zones **Heure de début**, entrez ou sélectionnez la date et l'heure d'exécution de votre analyse chaque jour.
10. Dans le panneau **Fenêtres opérationnelles**, sélectionnez votre fenêtre opérationnelle dans la liste et cliquez sur (**>**).
11. Cliquez sur **Sauvegarder**.

Gestion des fenêtres opérationnelles

Dans IBM QRadar Vulnerability Manager, vous pouvez éditer, supprimer et imprimer des fenêtres opérationnelles.

A faire : Vous pouvez modifier une fenêtre opérationnelle alors qu'elle est associée à un profil d'analyse.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Créneaux opérationnels**.
3. Sélectionnez la fenêtre opérationnelle que vous souhaitez éditer.
4. Dans la barre d'outils, sélectionnez une option dans le menu **Actions**.
5. Suivez les instructions de l'interface utilisateur.

   Restriction : Il n'est pas possible de supprimer une fenêtre opérationnelle qui est associée à un profil d'analyse. Vous devez d'abord déconnecter la fenêtre opérationnelle du profil d'analyse.

Déconnexion d'une fenêtre opérationnelle

Si vous souhaitez supprimer une fenêtre opérationnelle qui est associée à un profil d'analyse, vous devez déconnecter la fenêtre opérationnelle du profil d'analyse.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
3. Sélectionnez le profil d'analyse que vous souhaitez modifier.
4. Dans la barre d'outils, cliquez sur **Editer**.
5. Cliquez sur le panneau **Quand analyser**.
6. Sélectionnez l'option correspondante dans la liste **Exécuter la planification** comme requis.
7. Dans la zone **Nom**, sélectionnez le créneau opérationnel que vous souhaitez déconnecter et cliquez sur (**<**).
8. Cliquez sur **Sauvegarder**.

Analyses de vulnérabilité dynamiques

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse afin d'utiliser certains programmes d'analyse des vulnérabilités pour des plages CIDR spécifiques dans votre réseau. Par exemple, vos programmes d'analyse pourraient n'avoir accès qu'à certaines zones de votre réseau.

Lors d'une analyse, QRadar Vulnerability Manager détermine le programme d'analyse à utiliser pour chaque CIDR, adresse IP ou plage d'adresses IP spécifié dans votre profil d'analyse.

Analyse dynamique et domaines

Si vous avez configuré des domaines dans la fenêtre **Gestion des domaines** sur l'onglet **Admin**, vous pouvez associer des scanners avec les domaines que vous avez ajoutés.

Par exemple, vous pouvez associer différents scanners chacun à un domaine différent, ou à différentes plages CIDR dans le même domaine. QRadar analyse dynamiquement les plages CIDR configurées qui contiennent les adresses IP que vous spécifiez sur tous les des domaines qui sont associés aux scanners sur votre système. Les actifs avec la même adresse IP sur différents domaines sont analysés individuellement si la plage de CIDR pour chaque domaine comprend cette adresse IP. Si une adresse IP ne est pas dans une plage de CIDR configurée pour un domaine de scanner, QRadar analyse le domaine qui est configuré pour le scanner de contrôleur pour l'actif.

Configuration de l'analyse dynamique

Pour utiliser l'*analyse dynamique*, vous devez effectuer les actions suivantes :

1. Ajoutez des programmes d'analyse des vulnérabilités à votre déploiement QRadar Vulnerability Manager. Pour plus d'informations, voir «Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager», à la page 8.
2. Associez les scanners de vulnérabilités avec des plages de CIDR et des domaines.
3. Configurez une analyse de plusieurs plages de CIDR et activez **Sélection de serveur dynamique** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**.

Concepts associés

Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager

Détails relatifs au profil d'analyse

Tâches associées

Création d'un profil d'analyse à la demande

Pour déclencher une analyse en réponse à un événement de règle personnalisée, configurez un profil d'analyse à la demande et activez l'analyse dynamique.

Association de programmes d'analyse des vulnérabilités à des plages CIDR

Dans IBM QRadar Vulnerability Manager, pour effectuer une analyse dynamique, vous devez associer des programmes d'analyse des vulnérabilités à différents segments de votre réseau.

Avant de commencer

Vous devez ajouter des programmes d'analyse des vulnérabilités supplémentaires à votre déploiement. Pour plus d'informations, voir «Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager», à la page 8.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Scanners**.

Avertissement : Par défaut, le scanner Controller est affiché. Le programme d'analyse du contrôleur fait partie du processeur QRadar Vulnerability Manager déployé dans la console

QRadar ou sur un dispositif de traitement QRadar Vulnerability Manager dédié. Vous pouvez affecter une plage CIDR au scanner Controller, mais vous devez déployer des programmes d'analyse supplémentaires pour l'utilisation de l'analyse dynamique.

3. Cliquez sur un scanner dans la page **Scanners**.
4. Dans la barre d'outils, cliquez sur **Editer**.

   Restriction : Vous ne pouvez pas éditer le nom du scanner. Pour modifier un nom de scanner, cliquez sur **Admin** > **Gestion du système et de la licence** > **Actions de déploiement** > **Gestion du déploiement de vulnérabilité**.
5. Dans la zone **CIDR**, entrez une plage CIDR ou plusieurs plages CIDR séparées par des virgules.
6. Cliquez sur **Sauvegarder**.

Concepts associés

Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager

Tâches associées

Création d'un profil d'analyse à la demande

Pour déclencher une analyse en réponse à un événement de règle personnalisée, configurez un profil d'analyse à la demande et activez l'analyse dynamique.

Analyse de plages CIDR avec différents programmes d'analyse des vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez analyser des zones de votre réseau avec différents programmes d'analyse des vulnérabilités.

Avant de commencer

Vous devez configurer vos plages CIDR réseau afin d'utiliser différents programmes d'analyse des vulnérabilités dans votre déploiement QRadar Vulnerability Manager. Pour plus d'informations, voir «Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager», à la page 8.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Cliquez sur la case **Sélection de serveur dynamique**.

   Si vous avez configuré des domaines dans la fenêtre **Admin** > **Gestion des domaines**, vous pouvez sélectionner un domaine dans la liste **Domaine**. Seuls les actifs dans le domaine que vous avez sélectionnés sont analysés.
5. Ajoutez plusieurs plages CIDR.
6. Cliquez sur **Sauvegarder**.
7. Cliquez sur la case dans la ligne qui est assignée à votre analyse sur la page **Profils d'analyse** et cliquez sur **Exécuter**.

Tâches associées

Création d'un profil d'analyse à la demande

Pour déclencher une analyse en réponse à un événement de règle personnalisée, configurez un profil d'analyse à la demande et activez l'analyse dynamique.

Politiques d'administration d'analyse

Une politique d'administration d'analyse fournit un emplacement centralisé pour la configuration d'exigences d'analyse spécifiques.

Vous pouvez utiliser des politiques d'administration d'analyse pour spécifier les types d'analyse, les ports à analyser, les vulnérabilités à détecter et les outils d'analyse à utiliser. Dans IBM QRadar Vulnerability Manager, une *politique d'administration d'analyse* est associée à un profil d'analyse et utilisée pour contrôler une analyse des vulnérabilités. Vous utilisez la liste **Politiques d'analyse** sur l'onglet **Détails** de la page **Configuration du profil d'analyse** pour associer une politique d'analyse à un profil d'analyse.

Vous pouvez créer une politique d'analyse ou copier et modifier une politique préconfigurée distribuée avec QRadar Vulnerability Manager.

Politiques d'analyse préconfigurées

Les politiques d'analyse préconfigurées suivantes sont distribuées avec QRadar Vulnerability Manager :

- Analyse complète
- Analyse de reconnaissance
- Analyse de base de données
- Analyse de correctifs
- Analyse PCI
- Analyse Web

Une description de chaque politique d'analyse préconfigurée figure dans la page**Politiques d'analyse**.

Tâches associées

Modification d'une politique d'analyse préconfigurée
Dans IBM QRadar Vulnerability Manager, vous pouvez copier une politique d'analyse préconfigurée et modifier la politique en fonction de vos besoins d'analyse précis.

Configuration d'une politique d'analyse
Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une politique d'analyse pour répondre à toutes les exigences spécifiques de vos analyses de vulnérabilité. Vous pouvez copier et renommer une politique d'analyse préconfigurée ou vous pouvez ajouter une nouvelle politique d'analyse. Vous ne pouvez pas modifier une politique d'analyse préconfigurée.

Mises à jour automatiques des politiques d'analyse des vulnérabilités critiques

Dans le cadre des mises à jour automatiques quotidiennes de IBM QRadar Vulnerability Manager, vous recevez de nouvelles politiques d'analyse pour des tâches telles que la détection de vulnérabilités du jour zéro sur vos actifs.

Utilisez les politiques d'analyse qui sont fournies par la mise à jour automatique pour créer des profils d'analyse afin de rechercher des vulnérabilités spécifiques. Pour afficher toutes les politiques d'analyse sur votre système, accédez à **Administration** > **Politiques d'analyse** dans l'onglet **Vulnérabilités**.

Vous ne devez pas modifier les politiques d'analyse qui sont fournies par la mise à jour automatique car vos modifications peuvent être remplacées par des mises à jour ultérieures. Vous pouvez créer une copie et la modifier.

Si vous supprimez une politique d'analyse qui est fournie par mise à jour automatique, elle peut être récupérée seulement par le support client QRadar.

Modification d'une politique d'analyse préconfigurée

Dans IBM QRadar Vulnerability Manager, vous pouvez copier une politique d'analyse préconfigurée et modifier la politique en fonction de vos besoins d'analyse précis.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option **Administration** > **Politiques d'analyse**.
3. Dans la page **Politiques d'analyse**, cliquez sur une politique d'analyse préconfigurée.
4. Dans la barre d'outils, cliquez sur **Editer**.

5. Cliquez sur **Copier**.
6. Dans la fenêtre **Copier la politique d'analyse**, entrez un nouveau nom dans la zone **Nom** et cliquez sur **OK**.
7. Cliquez sur la copie de la politique d'analyse et, dans la barre d'outils, cliquez sur **Editer**.
8. Dans le volet **Description**, entrez les nouvelles informations concernant la politique d'analyse.

   Important : Si vous modifiez la nouvelle politique d'analyse, vous devez mettre à jour la description.
9. Pour modifier la politique d'analyse, utilisez les onglets **Analyse du port**, **Vulnérabilités**, **Groupe d'outils** ou **Outils**.

   Restriction : En fonction du **Type d'analyse** que vous sélectionnez, vous ne pouvez pas utiliser tous les onglets de la fenêtre **Politique d'analyse**.

Configuration d'une politique d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une politique d'analyse pour répondre à toutes les exigences spécifiques de vos analyses de vulnérabilité. Vous pouvez copier et renommer une politique d'analyse préconfigurée ou vous pouvez ajouter une nouvelle politique d'analyse. Vous ne pouvez pas modifier une politique d'analyse préconfigurée.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Politiques d'administration d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Saisissez le nom et la description de votre politique d'analyse.

   Pour configurer une politique d'analyse, vous devez au moins configurer les zones obligatoires dans la fenêtre **New Scan Policy** qui sont les zones **Name** et **Description**.
5. Dans la liste **Scan Type**, sélectionnez le type d'analyse.
6. Pour gérer et optimiser le processus de reconnaissance d'actifs, cliquez sur l'onglet **Asset Discovery**.
7. Pour gérer les ports et les protocoles qui sont utilisés pour une analyse, cliquez sur l'onglet **Analyse du port**.
8. Pour inclure des vulnérabilités spécifiques dans votre politique d'analyse de correctifs, cliquez sur l'onglet **Vulnérabilités**.

   Remarque : L'onglet **Vulnérabilités** est disponible uniquement lorsque vous sélectionnez une analyse de correctif.
9. Pour inclure ou exclure des groupes d'outils de votre politique d'analyse, cliquez sur l'onglet **Tool Groups**.

   Remarque : L'onglet **Tool Groups** est disponible uniquement lorsque vous sélectionnez une politique sans donnée d'identification ou d'analyse complète (full-scan ou full-scan plus).
10. Pour inclure ou exclure des outils d'une politique d'analyse, cliquez sur l'onglet **Tools**.

    Remarque : Cet onglet est disponible uniquement lorsque vous sélectionnez une règle Full Scan Plus ou Full Scan sans données d'identification.

    Important : Si vous ne modifiez pas les outils ou les groupes d'outils, et que vous sélectionnez l'option **Full** comme type analyse, tous les outils et les groupes d'outils qui sont associés à une analyse complète sont inclus dans votre politique d'analyse.
11. Cliquez sur **Save**.

Chapitre 6. Gestion des faux positifs

Généralement, les faux positifs d'une analyse de vulnérabilité se produisent lorsque le scanner peut uniquement accéder à un sous-ensemble de l'information requise, ce qui l'empêche de déterminer clairement si une vulnérabilité existe ou non.

Pour aider à réduire le nombre de faux positifs, vous devez configurer vos scanners avec les données d'identification appropriées. Les analyses ont besoin de pouvoir accéder à toutes les informations requises concernant les données des actifs pour pouvoir déterminer si une vulnérabilité existe.

Pourquoi des faux positifs sont-ils générés ?

Un faux positif peut être généré si le scanner peut uniquement lire les informations de configuration des bannières de service. Par exemple, un scanner lisant une bannière Apache peut détecter que seule la version 2.2.15 est installée à partir de la bannière HTTP, même si la version 2.2.15-39 est également installée et que la version contient un correctif logiciel ayant été rétroporté.

Pour citer un autre exemple, imaginons que le scanner lit la bannière et détecte la version de SSH qui est installée mais ne peut pas détecter le niveau de correctif ou le système d'exploitation. Si le scanner détecte que SSH-2 est installé mais n'est pas capable d'identifier le système d'exploitation, le scanner ne peut pas déterminer avec exactitude si une vulnérabilité existe dans des instances. La vulnérabilité peut être identifiée correctement sur un actif mais elle représente un faux positif sur un autre actif car les vulnérabilités SSH détectées sur les SSH Red Hat peuvent être différentes sur les autres systèmes d'exploitation Linux.

Pourquoi les scanners ne peuvent-ils pas extraire toutes les informations requises ?

Les scanners de vulnérabilité ne peuvent pas toujours accéder aux informations dont ils ont besoin pour déterminer avec exactitude si une vulnérabilité existe. Cette limitation entraîne généralement la génération de faux positifs.

Les scanners ne réussissent pas à s'authentifier

Si le scanner ne peut pas s'authentifier sur le noeud final, il doit se servir des informations limitées obtenues des vérifications de services de réseau anonymes tels que les informations extraites des bannières de lecture.

Les bannières peuvent contenir des versions incorrectes et des informations obsolètes sur les niveaux de correctifs, qui génèrent des faux positifs. Par contre, si le scanner peut s'authentifier, il peut déterminer la version complète du système d'exploitation et les informations sur les niveaux de correctifs puis supprimer les vulnérabilités qui représentent des faux positifs.

Recommandations sur les bannières

Utilisez ces recommandations sur les bannières lorsque vous configurez l'analyse des vulnérabilités dans votre réseau :

- N'incluez pas d'informations détaillées ou sensibles dans une bannière car un pirate informatique pourrait obtenir des informations cruciales sur les applications et les services s'exécutant sur un actif puis utiliser les vulnérabilités connues pour les exploiter.
- Reconnaissez le type d'information disponible de manière anonyme dans les bannières. Evaluez les vecteurs d'attaques probablement tentés. Ces informations sont utiles pour évaluer la sécurité de votre réseau et pour collecter des informations sur le réseau.
- Marquez les informations de vulnérabilité lues dans les bannières comme faux positifs en étiquetant les vulnérabilités comme exception dans les onglets tels que le panneau **Instances de vulnérabilité** de la fenêtre **Détails de l'actif** ou de la fenêtre **Historique des vulnérabilités**.
- Réglez les analyses en activant ou en désactivant les outils des politiques d'administration d'analyse pouvant empêcher ces analyses de démarrer.

© Copyright IBM Corp. 2012, 2020

Techniques d'analyses authentifiées basées sur Windows

L'analyse authentifiée basée sur Windows utilise les deux techniques suivantes pour détecter les vulnérabilités :

- L'analyse de registre lorsque le scanner nécessite un accès au registre.
- L'analyse OVAL lorsque WMI (Windows Management Instrumentation) doit être configuré correctement.

Si l'une de ces deux techniques échoue, le résultat d'analyse sera propice aux faux positifs.

Vous devez activer le service de registre distant pour que le scanner accède au registre.

Une mauvaise configuration de WMI (Windows Management Instrumentation) peut générer des faux positifs.

Identifier les échecs d'authentification

Si une analyse ne s'authentifie pas correctement, survolez le symbole d'avertissement avec votre curseur pour voir pourquoi l'analyse a rencontré des problèmes. Par exemple,

```
The last scan of this asset failed
STATUS_LOGON_FAILURE
Therefore the vulnerability may not be accurate
```

D'autres exemples de messages incluent `SSH logon failure`, `remote registry service not started` et `no WMI access`.

Concepts associés

Analyse sur les actifs Windows

QRadar Vulnerability Manager utilise l'analyse de registre et l'analyse OVAL (Open Vulnerability Assessment Language) pour détecter les vulnérabilités sur les actifs Windows. Utilisez les analyses authentifiées pour détecter toutes les vulnérabilités de Windows. Les analyses non authentifiées risquent de ne pas détecter toutes les vulnérabilités de Windows.

Tâches associées

Configuration d'une analyse authentifiée du système d'exploitation Windows

Activation des droits pour les analyses de correctifs Linux ou UNIX

Application d'une règle d'exception de vulnérabilité

Comment le résultat d'analyse de la vulnérabilité est-il détecté ?

Déterminez si le résultat d'analyse de la vulnérabilité est généré à partir d'une analyse authentifiée ou d'une lecture anonyme d'une bannière. Les résultats d'analyse qui sont générés à partir d'une lecture anonyme d'une bannière seront probablement des faux positifs.

Survolez la colonne **Détails** du résultat d'analyse de vulnérabilité de l'actif pour voir comment la vulnérabilité est détectée.

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le menu de navigation, cliquez sur **Résultats de l'analyse**.
3. Cliquez deux fois sur un profil d'analyse dans la colonne **Nom**.
4. Cliquez sur une ligne de la colonne **Instances de vulnérabilité**.
5. Survolez un résultat de la colonne **Détails** pour afficher plus de détails.

   Par exemple, les détails suivants peuvent être générés lorsque le scanner lit une bannière :

   ```
   SERVER: Apache/2.2.15(Red Hat)
   ```

Analyses de correctifs et faux positifs

Les vulnérabilités qui sont détectées à partir des analyses de correctifs sont rarement des faux positifs, sauf si elles concernent les mises à jour des bases de connaissances Windows. Les mises à jour Windows,

qui sont préfixées par un numéro de base de connaissances peuvent être des faux positifs si la phase WMI (Windows Management Instrumentation) de l'analyse Windows authentifiée échoue.

Les mises à jour Windows deviennent obsolètes dans le temps. Par exemple, une base de connaissances Windows remplace la base de connaissances initiale ayant adressé un correctif de vulnérabilité d'origine. Le remplacement ne constitue pas de problème en cas de mises à jour Windows récentes ou si l'analyse WMI ou OVAL réussit car l'analyse prend en compte toutes les nouvelles mises à jour.

Examen d'un faux positif potentiel d'une analyse authentifiée

Une analyse authentifiée peut générer un faux positif si elle échoue.

Pourquoi et quand exécuter cette tâche

Recherche de la vulnérabilité.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le menu de navigation, cliquez sur **Résultats d'analyse**.
3. Dans la fenêtre **Résultats d'analyse**, cliquez sur une ligne de la colonne Vulnérabilités.
4. Cliquez sur la vulnérabilité que vous voulez examiner.
5. Cliquez sur le lien **Détails du plug-in** pour ouvrir la fenêtre de correctif pour la vulnérabilité.
6. Utilisez les onglets pour rechercher les recommandations Oval Definition, Windows Knowledge Base ou UNIX sur la vulnérabilité.
   - Pour les vulnérabilités créées à partir d'un test OVAL (Open Vulnerability and Assessment Language), cliquez sur l'onglet **OVAL** approprié pour afficher les critères que QRadar Vulnerability Manager utilise dans le test.
   - Pour les vulnérabilités créées à partir d'une analyse de registre de base de connaissances Windows, cliquez sur l'onglet **Base de connaissances Windows** pour afficher les mises à jour (bases de connaissances) que QRadar Vulnerability Manager associe à la vulnérabilité.
   - Pour les vulnérabilités créées en raison d'un gestionnaire de package RPM manquant, cliquez sur l'onglet **Unix**. Les packages et les révisions qui s'affichent sont comparés aux versions de systèmes d'exploitation appropriées.

Chapitre 7. Analyse des correctifs authentifiés

Dans IBM QRadar Vulnerability Manager, vous pouvez analyser les noms de communauté et exécuter des analyses de correctifs authentifiés pour les systèmes d'exploitation Windows, Linux et UNIX.

Noms de communauté SNMP

Vous pouvez analyser les actifs de votre réseau à l'aide de noms de communauté SNMP. Cette fonction s'applique à SNMP V1 et V2c.

Lorsque vous analysez des actifs, QRadar Vulnerability Manager s'authentifie à l'aide des services SNMP détectés et effectue une analyse des détaillée.

Analyses des correctifs Windows

Pour la recherche des correctifs manquants sous Windows, l'accès distant au registre et l'interface de gestion Windows (WMI) doivent être activés. Si votre analyse des correctifs Windows renvoie des problèmes de connectivité WMI, vous devez configurer vos systèmes Windows.

Si vous souhaitez lire des données WMI sur un serveur distant, vous devez activer les connexions entre votre console QRadar et le serveur en cours de surveillance. Si le serveur utilise un pare-feu Windows, vous devez configurer le système pour activer les requêtes WMI distantes.

Si vous utilisez un compte non administrateur pour surveiller le serveur Windows, vous devez activer le compte pour qu'il interagisse avec le modèle DCOM (Distributed Component Object Model).

Si l'outil d'analyse de correctif ne peut pas se connecter à un actif Windows, une icône d'avertissement triangulaire jaune s'affiche en regard de l'actif dans les résultats d'analyse. La vulnérabilité suivante apparaît : `Local Checks Error`.

L'activation de certaines instructions pour les clients RPC non authentifiés dans votre stratégie de groupe Windows empêche QRadar Vulnerability Manager d'exécuter des requêtes WMI lorsqu'il analyse un serveur Windows. Lorsque l'authentification échoue, une icône d'avertissement en forme de triangle jaune s'affiche en regard de l'actif dans les résultats de l'analyse. Par exemple, si vous activez l'option **Restrict Unauthenticated RPC Client** sous Windows 2012, vous pouvez sélectionner **None**, **Authenticated** ou **Authenticated without exceptions** dans le menu. Si vous sélectionnez **Authenticated without exceptions**, QRadar Vulnerability Manager ne peut pas exécuter les requêtes WMI et ne peut pas effectuer l'analyse.

Analyse sécurisée d'un système d'exploitation Linux authentifié

Pour analyser des systèmes d'exploitation Linux en utilisant l'authentification sécurisée, vous pouvez configurer le chiffrement par clé publique entre la console ou l'hôte géré et les cibles d'analyse.

Lorsque l'authentification sécurisée est configurée, vous n'avez pas besoin de spécifier un mot de passe de système d'exploitation Linux dans votre profil d'analyse.

Vous devez configurer l'authentification par clé publique sur chaque système d'exploitation Linux que vous analysez.

Si vous déplacez votre processeur de vulnérabilité vers un dispositif de processeur de vulnérabilité dédié, vous devez reconfigurer l'authentification sécurisée entre le dispositif de processeur de vulnérabilité dédié et la cible d'analyse.

Si l'outil d'analyse de correctif ne peut pas se connecter à un actif Linux, une icône d'avertissement triangulaire jaune s'affiche en regard de l'actif dans les résultats d'analyse. La vulnérabilité suivante apparaît : : `SSH Patch Scanning - Failed Logon`.

Tâches associées

Configuration de l'authentification par clé publique du système d'exploitation Linux

Configuration d'une analyse authentifiée des systèmes d'exploitation Linux ou UNIX

© Copyright IBM Corp. 2012, 2020

Configuration d'une analyse authentifiée du système d'exploitation Windows

Ensembles de données d'identification centralisés

Lorsque vous exécutez des analyses authentifiées, vous pouvez utiliser une liste centralisée, qui stocke les données d'identification de connexion pour vos systèmes d'exploitation Linux, UNIX, ou Windows. Votre administrateur système doit configurer la liste des données d'identification.

Un administrateur peut indiquer des données d'identification pour des périphériques réseau SNMP et des systèmes d'exploitation Linux, UNIX ou Windows. Par conséquent, un utilisateur chargé de configurer un profil d'analyse n'a pas besoin de connaître les données d'identification de chaque actif analysé. De même, en cas de modification des données d'identification d'un actif, les données d'identification peuvent être modifiées de façon centralisée au lieu de mettre à jour le profil d'analyse.

Tâches associées

Configuration d'une analyse authentifiée des systèmes d'exploitation Linux ou UNIX

Configuration d'une analyse authentifiée du système d'exploitation Windows

Création d'un profil de test de performances

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

Configuration d'un ensemble de données d'identification

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

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Dans le panneau **Configuration système**, cliquez sur **Données d'identification centralisées**.
3. Dans la fenêtre **Données d'identification centralisées**, sur la barre d'outils, cliquez sur **Ajouter**.

   Pour configurer un ensemble de données d'identification, la seule zone obligatoire de la fenêtre **Jeu de données d'identification** est la zone **Nom**.
4. Dans la fenêtre **Jeu de données d'identification**, cliquez sur l'onglet **Actifs**.
5. Saisissez une plage CIDR pour les actifs dont vous voulez spécifier les données d'identification, puis cliquez sur **Actifs**.

   Les utilisateurs doivent détenir des droits d'accès au réseau fournis dans le profil de sécurité d'une adresse IP ou d'une plage d'adresses CIDR, qu'ils utilisent ou créent des données d'identification via les **Données d'identification centralisées**.
6. Cliquez sur les onglets **Linux/Unix, Windows, ou périphériques réseau (SNMP)**, puis entrez vos données d'identification.
7. Cliquez sur **Sauvegarder**.

Configuration de l'authentification par clé publique du système d'exploitation Linux

Pour analyser les systèmes d'exploitation Linux avec l'authentification par clé publique sécurisée, vous devez configurer la console IBM QRadar ou l'hôte géré et l'actif à analyser. Lorsque l'authentification est configurée, vous pouvez effectuer des analyses authentifiées en spécifiant un nom d'utilisateur pour le système d'exploitation Linux, et sans spécifier de mot de passe. QRadar prend en charge à la fois `rsa` et `dsa` pour la génération de clé SSH.

Avant de commencer

Vous devez installer une clé publique et une clé privée sur un scanner QVM, et installer la clé publique sur la cible d'analyse.

Un scanner QVM est installé automatiquement sur un hôte de processeur QVM, et peut aussi être installé sur d'autres hôtes gérés.

Le compte utilisateur sur la cible d'analyse doit disposer d'un shell de connexion et doit être capable d'exécuter les commandes requises pour une analyse de correctif sur la cible. Pour plus d'informations, voir «Activation des droits pour les analyses de correctifs Linux ou UNIX», à la page 65.

La procédure suivante décrit la configuration d'une seule paire de clés publique/privée et son transfert sur un scanner QVM et une cible d'analyse.

Procédure

1. Avec SSH, connectez-vous à la console QVM en tant que superutilisateur.
2. Générez un paire de clés publiques en entrant la commande suivante :

   ```
   su -m -c 'ssh-keygen -t <type_clé>' qvmuser
   ```

   Remarque : *<type_clé>* peut être dsa ou rsa.
3. Acceptez le fichier par défaut en appuyant sur **Entrée**.
4. Acceptez le mot de passe par défaut de la clé public en appuyant sur **Entrée**.
5. Appuyez de nouveau sur **Entrée** pour confirmer.
6. Copiez les clés publique et privée sur tous les hôtes gérés sur lesquels un scanner QVM est installé.

   ```
   cd /home/qvmuser/.ssh
   ```

   ```
   rsync -ogp id_<type_clé> id_<type_clé>.pub <adresse_IP>:/home/qvmuser/.ssh
   ```

   - Remplacez *<type_clé>* par dsa ou rsa.
   - Remplacez *<adresse_IP>* par l'adresse IP du scanner et entrez le mot de passe root lorsque vous y êtes invité.

   Remarque : Le processeur QVM comprend un scanner. Si le processeur ne s'exécute pas sur la console QRadar, vous devez également transférer les clés sur le processeur QVM.
7. Copiez la clé publique dans la cible d'analyse en entrant la commande suivante :

   ```
   cd /home/qvmuser/.ssh
   ```

   ```
   ssh-copy-id -i id_<type_clé>.pub <user>@<adresse_IP>
   ```

   - *<type_clé>* – dsa ou rsa.
   - *<adresse_IP>* – adresse IP de la cible d'analyse.
   - *<utilisateur>* – utilisateur sur la cible d'analyse.
8. Entrez le mot de passe utilisateur pour la cible d'analyse.
9. Vérifiez que le compte *qvmuser* sur le scanner QVM peut se connecter par SSH à la cible d'analyse sans mot de passe en tapant la commande suivante :

   ```
   su -m -c 'ssh -o StrictHostKeyChecking=no <utilisateur>@<Adresse IP> ls'
   qvmuser
   ```

   - *<adresse_IP>* – adresse IP de la cible d'analyse.
   - *<utilisateur>* – utilisateur sur la cible d'analyse.

   Une liste des fichiers dans le répertoire de base de l'utilisateur sur le système cible est affichée.

Que faire ensuite

Créez un profil d'analyse dans QRadar Vulnerability Manager avec le nom d'utilisateur sur la cible d'analyse sans spécifier de mot de passe et exécutez une analyse de correctif.

Tâches associées

Configuration d'une analyse authentifiée des systèmes d'exploitation Linux ou UNIX

Configuration d'une analyse authentifiée des systèmes d'exploitation Linux ou UNIX

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse d'authentification des systèmes d'exploitation Linux ou UNIX qui se trouvent sur votre réseau. Vous pouvez indiquer manuellement les données d'identification dans le profil d'analyse ou utiliser un ensemble de données d'identification.

Avant de commencer

Pour effectuer une analyse en utilisant une liste de données d'identification, vous devez d'abord définir une liste centrale des données d'identification nécessaires à vos systèmes d'exploitation. Pour plus d'informations, voir «Configuration d'un ensemble de données d'identification», à la page 62.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. Pour configurer une analyse authentifiée, vous devez également suivre les étapes restantes de cette procédure.
4. Cliquez sur **Utiliser les données d'identification centralisées** pour analyser vos systèmes d'exploitation Linux ou UNIX.

   Si un ensemble de données d'identification n'est pas configuré et que vous ne spécifiez pas manuellement les données d'identification, les outils d'analyse sont exécutés, mais aucune donnée d'identification n'est transmise.

   Si QVM ne trouve pas de jeu de données d'identification centralisé pour les hôtes que vous analysez, il utilise les données d'identification existantes que vous spécifiez manuellement dans l'onglet **Données d'identification supplémentaires**.
5. Cliquez sur l'onglet **Quand analyser**.
6. Dans la liste **Exécuter la planification**, sélectionnez **Manuelle**.
7. Cliquez sur l'onglet des **créneaux supplémentaires**.
8. Dans la zone d'**analyse de correctifs Linux/Unix**, entrez le nom d'utilisateur et le mot de passe pour les hôtes Linux ou UNIX à analyser et cliquez sur **>**.

   Aucun mot de passe n'est nécessaire, si vous avez configuré une authentification par clé publique sécurisée entre la console et la cible d'analyse.
9. Cliquez sur **Sauvegarder**.
10. Dans la page **Profils d'analyse**, cliquez sur **Exécuter**.

Concepts associés

Ensembles de données d'identification centralisés

Tâches associées

Configuration d'un ensemble de données d'identification

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

Configuration de l'authentification par clé publique du système d'exploitation Linux

Activation des droits pour les analyses de correctifs Linux ou UNIX

Les comptes utilisateur non superutilisateur doivent posséder les droits appropriés pour exécuter les commandes nécessaires à QRadar Vulnerability Manager pour l'analyse des correctifs sur les ordinateurs Linux et UNIX.

Pourquoi et quand exécuter cette tâche

Si vous souhaitez vérifier que le compte utilisateur exécuté pour l'analyse possède les droits appropriés pour l'analyse de correctifs sous Linux ou UNIX :

Procédure

1. Exécutez SSH pour l'actif.
2. Exécutez les commandes uname suivantes :

```
uname -m
uname -n
uname -s
uname -r
uname -v
uname -p
uname -a
```

3. En fonction de votre système d'exploitation, exécutez les commandes suivantes :

Tableau 9. Commandes à exécuter sur votre système d'exploitation

Système d'exploitation	Commandes

Linux	Les fichiers suivants comportent le contenu correspondant à votre distribution :
	/etc/redhat-release
	/etc/SuSE-release
	/etc/debian-version
	/etc/slackware-version
	/etc/mandrake-version
	/etc/gentoo-version
	Par exemple, sur Red Hat Enterprise Linux, utilisez les commandes suivantes :
	`ls /etc/redhat-release`
	`cat/etc/redhat-release`
	`rpm -qa --qf '%{NAME}--%{VERSION}---%{RELEASE}|%{EPOCH}--%{ARCH}---%{FILENAMES}--%{SIGPGP}---%{SIGGPG}\n'`
	`rpm -qa --qf '%{NAME}-%{VERSION}-%{RELEASE}|%{EPOCH}\n'`

Tableau 9. Commandes à exécuter sur votre système d'exploitation (suite)

Système d'exploitation	Commandes

Solaris	`/usr/bin/svcs -a/`
	`usr/bin/pkginfo -x | awk '{`
	`if ( NR % 2 ) { prev = \$1 }`
	`else  { print prev\" \"\$0  } }'`
	`/usr/bin/showrev -p`
	`/usr/sbin/patchadd -p`
	`/usr/bin/isainfo -b`
	`/usr/bin/isainfo -k`
	`/usr/bin/isainfo -n`
	`/usr/bin/isainfo -v`

HP-UX	`/usr/sbin/swlist -l fileset -a revision` `/usr/sbin/swlist -l patch`
AIX	`oslevel -r` `lslpp -Lc`
ESX	`vmware -vesxupdate query --all` `. /etc/profile ;  /sbin/esxupdate query –all`

Conseil :

Il est recommandé de désactiver les notifications par courrier électronique pour le compte de l'utilisateur d'analyse car ce type de notification peut interférer avec le traitement des résultats de l'analyse. Pour plus de détails, consultez la documentation de votre système d'exploitation.

Chapitre 8. Analyse sur les actifs Windows

QRadar Vulnerability Manager utilise l'analyse de registre et l'analyse OVAL (Open Vulnerability Assessment Language) pour détecter les vulnérabilités sur les actifs Windows. Utilisez les analyses authentifiées pour détecter toutes les vulnérabilités de Windows. Les analyses non authentifiées risquent de ne pas détecter toutes les vulnérabilités de Windows.

Quand les données de vulnérabilité sont-elles visibles dans QRadar ?

Les vulnérabilités nouvellement publiées sont visibles sur le tableau de bord QRadar Vulnerability Manager et dans la section de recherche de l'onglet **Vulnérabilité** dans QRadar.

QRadar Vulnerability Manager obtient des mises à jour quotidiennes sur les vulnérabilités ainsi que des informations, des recommandations, les vulnérabilités nouvellement publiées et leurs métadonnées associées, les données de test ainsi que toutes les nouvelles détections.

Les systèmes QRadar Vulnerability Manager sont généralement actualisés avec les vulnérabilités les plus récentes 2 à 3 jours après avoir été annoncées.

Quels sont les types de méthodes d'analyse disponibles ?

La liste suivante offre des renseignements importants sur les méthodes d'analyse disponibles pour détecter les vulnérabilités sur les actifs basés Windows :

Analyses authentifiées et non authentifiées
Vous devez utiliser des analyses authentifiées pour détecter toutes les vulnérabilités basées Windows. Si vous utilisez une analyse non authentifiée pour détecter les vulnérabilités basées Windows, les résultats peuvent être incomplets et comporter des faux-positifs.

Analyses de registre
L'analyse de registre est utilisée pour détecter les vulnérabilités sur le système d'exploitation Windows.

- QRadar Vulnerability Manager utilise le service de registre distant et WMI (Windows Management Instrumentation) pour extraire les informations concernant les service packs de la base de connaissance, les logiciels installés et les services activés des noeuds finaux qu'il analyse et ces informations sont liées à des définitions de vulnérabilité.
- Chaque définition Windows inclut le bulletin, la base de connaissance, le service pack, et le service Windows requis.

Analyses OVAL (Open Vulnerability Assessment Language)
Les analyses OVAL (Open Vulnerability Assessment Language) sont utilisées pour détecter des vulnérabilités sur les systèmes d'exploitation Windows.

Open Vulnerability Assessment Language (OVAL) est une norme qui est référencée lorsque vous effectuez des tests OVAL de vulnérabilité et des tests de configuration sur les actifs. La liste ci-dessous contient des informations sur les vulnérabilités et les tests OVAL.

- Les tests peuvent inclure n'importe quelle combinaison de clés de registre, valeurs de clés de registre, versions `.dll` et `.exe`, services d'exécution et présence de fichiers.
- Chaque définition de vulnérabilité est une expression logique XML qui détermine si le système est vulnérable.
- Toutes les versions `.exe` et `.dll` sont testées.
- Vous pouvez cliquer sur le lien CVE d'une vulnérabilité pour vérifier si elle comporte un test OVAL, par exemple CVE-2013-3910 (https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3910)
- Les définitions de test OVAL sont disponibles en ligne sur le site Web Oval (https://oval.cisecurity.org/)
- Le test OVAL peut ignorer une vulnérabilité générée.

© Copyright IBM Corp. 2012, 2020

Analyses des correctifs des systèmes d'exploitation Windows

L'analyse des *correctifs* des systèmes d'exploitation Windows est une méthode d'accès au réseau authentifié qui est utilisée pour rechercher des correctifs ou des mises à jour de logiciels de sécurité manquants sur un ordinateur de destination.

Les analyses de correctifs effectuent une analyse de port Nmap limitée sur les ports 22, 139 et 445 pour déterminer si l'actif est un actif Windows ou un actif UNIX. Si l'analyse de port détecte des ports NetBIOS 139 ou 445, il sait que ces ports appartiennent à un actif basé Windows. L'outil de vulnérabilité enum est utilisé pour analyser un actif Windows.

Les analyses de correctifs ne sont pas intrusives et elles n'effectuent aucun test de vulnérabilité active.

Les analyses de correctifs prennent en compte les correctifs remplacés de manière automatique.

Il est possible d'analyser des ordinateurs pour rechercher les correctifs des systèmes d'exploitation Windows sans configurer Windows Management Instrumentation (WMI) et les partages administratifs mais les résultats ne seront pas complets et risqueront de générer des faux positifs.

Configuration requise pour l'analyse des actifs Windows

La liste suivante décrit les conditions requises que vous devez configurer pour l'analyse des actifs Windows :

- Configurez l'accès au registre distant sur les actifs.
- Configurez Windows Management Instrumentation (WMI) sur les actifs.
- Pour pouvoir lire les données WMI sur un serveur distant à travers un pare-feu, vous devez autoriser les requêtes WMI à travers un pare-feu Windows.
- Si vous utilisez un compte non administrateur pour surveiller le serveur Windows, vous devez définir des droits DCOM minimum et accorder des droits d'accès distant DCOM pour ce compte non administrateur.
- Configurez des partages administratifs sur les actifs.

Configuration d'une analyse authentifiée du système d'exploitation Windows

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse des systèmes d'exploitation Windows qui sont installés sur votre réseau. Vous pouvez indiquer manuellement les données d'identification dans le profil d'analyse ou utiliser un ensemble de données d'identification.

Si l'analyse est effectuée sans privilèges d'administration, QRadar Vulnerability Manager analyse le registre distant pour chaque installation Windows.

Si l'analyse est effectuée sans privilèges d'administration, elle est incomplète, susceptible de donner lieu à des faux positifs, et ne couvre pas plusieurs applications tierces.

Avant de commencer

QRadar Vulnerability Manager utilise des protocoles d'accès distant standard Windows qui sont activés par défaut dans la majorité des déploiements Windows.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. Pour configurer une analyse

authentifiée du système d'exploitation Windows, vous devez également suivre les étapes restantes de cette procédure.

4. Cliquez sur **Utiliser les données d'identification centralisées** pour analyser vos systèmes d'exploitation Windows.

   Vous devez configurer un ensemble de données d'identification ou spécifier manuellement des données d'identification pour les hôtes pour que les outils d'analyse qui nécessitent les données d'identification puissent fonctionner.

   Si QVM ne trouve pas de jeu de données d'identification centralisé pour les hôtes que vous analysez, il utilise les données d'identification existantes que vous spécifiez manuellement dans l'onglet **Données d'identification supplémentaires**.
5. Cliquez sur le panneau **Quand analyser**.
6. Dans la liste **Exécuter la planification**, sélectionnez **Manuelle**.

   Si vous souhaitez que l'analyse s'exécute à un moment ultérieur, sélectionnez l'une des options **Exécuter la planification** disponibles.
7. Cliquez dans la zone des **données d'identification supplémentaires**.
8. Dans la zone **Analyse des correctifs Windows**, entrez les informations requises dans les zones **Domaine**, **Nom d'utilisateur** et **Mot de passe** pour les hôtes Windows que vous voulez analyser et cliquez sur (**>**).

   Le nom de domaine que vous entrez est votre domaine Windows et non un domaine Internet.
9. Cliquez sur **Sauvegarder**.
10. Dans la page **Profils d'analyse**, cliquez sur **Exécuter**.

Concepts associés

Ensembles de données d'identification centralisés

Analyse des correctifs authentifiés

Registre distant

Le service de registre distant doit être activé, démarré et accessible par le dispositif de scanner QRadar Vulnerability Manager et l'utilisateur d'analyse configuré et utilisé dans le profil d'analyse.

Si le registre distant n'est pas accessible, l'analyse des correctifs Windows échoue complètement.

Si QRadar Vulnerability Manager ne peut pas accéder au registre distant, les résultats d'analyse enregistrent l'erreur suivante :

```
Local Checks Error – Remote Registry Service Not Running
```

Dans QRadar Vulnerability Manager version 7.2.3 et versions suivantes, une icône triangle jaune s'affiche en regard de l'actif dans les résultats d'analyse.

L'état du service de registre distant peut être vérifié depuis le **panneau de contrôle administratif** sous **Services**. Vérifiez que les services dépendants suivants sont démarrés :

- RPC (appel d'une procédure distante)
- DCOM Server Process Launcher
- RPC EndPoint Mapper

QRadar Vulnerability Manager peut accéder au registre distant sur le NetBIOS classique (ports 135, 137, 139) ou sur le tout nouveau NetBIOS sur TCP (port 445). Les pare-feu réseau ou personnels qui bloquent l'accès à l'un de ces protocoles empêchent l'accès aux analyses de correctif Windows.

Les comptes utilisateurs administratifs ont accès par défaut au registre distant. Les comptes utilisateurs non administratifs n'ont pas accès au registre distant. Vous devez configurer l'accès.

Activation de l'accès distant du registre aux actifs sur le système d'exploitation Windows

Pour analyser des systèmes Windows, vous devez configurer votre registre.

Procédure

1. Connectez-vous à votre système Windows.
2. Cliquez sur **Démarrer**.
3. Dans la zone **Rechercher les programmes et fichiers**, entrez **services**, puis appuyez sur la touche Entrée.
4. Dans la fenêtre **Services**, recherchez le service **de registre distant**.
5. Faites un clic droit sur le service **de registre distant**, puis cliquez sur **Démarrer**.
6. Fermez la fenêtre **Services**.

Affectation de droits minimum sur le registre distant

Les comptes utilisateurs administratifs ont accès par défaut au registre distant. Les comptes utilisateurs non administratifs n'ont pas accès au registre distant. Vous devez configurer l'accès.

Procédure

1. Sur l'ordinateur Windows cible, créez ou concevez un utilisateur Local ou Global (par exemple, "QVM_scan_user") et affectez un accès au registre en lecture seule au compte de l'utilisateur non administratif.
2. Ouvrez une session sur votre ordinateur Windows en utilisant un compte qui dispose des privilèges d'administrateur. Cliquez sur **Démarrer** > **Exécuter**.
3. Entrez `regedit`.
4. Cliquez sur **OK**.
5. Accédez à la clé :

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers \winreg.

   Les droits qui sont associés à cette clé de registre contrôlent les utilisateurs ou le groupe qui peut accéder au registre distant depuis le réseau.
6. Mettez en évidence la clé **winreg** et effectuez l'une des opérations suivantes :
   - Sous Windows XP ou version suivante, cliquez sur **Editer** > **Autorisations**.
   - Sous Windows 2000, cliquez sur **Sécurité** > **Autorisations**.
7. Accordez l'accès en lecture seule au compte "QVM_scan_user" désigné.

   Sous Windows XP, le paramètre *ForceGuest* est activé par défaut en mode groupe de travail. Ce paramètre peut provoquer des problèmes d'accès pour les connexions et les partages WMI, les autres services DCOM et les services RPC. Vous ne pouvez pas désactiver le paramètre *ForceGuest* sur les ordinateurs Windows XP Home.

Configuration de WMI

QRadar Vulnerability Manager utilise Windows Management Instrumentation (WMI) pour rechercher et identifier les versions des fichiers .exe et .dll installés sur les actifs cibles qui sont analysés.

Pourquoi et quand exécuter cette tâche

Sans les informations fournies par Windows Management Instrumentation (WMI), de nombreuses applications tierces sont manquées. Les faux positifs qui sont détectés pendant l'analyse du registre (avec le service de registre distant) ne peuvent pas être identifiés ou supprimés par QRadar Vulnerability Manager.

WMI est installé sur tous les systèmes d'exploitation Windows modernes, tels que Windows Vista, Windows 2008, Windows 2012, Windows 7, Windows 8 et Windows 8.1).

Les demandes WMI à distance doivent être activées et accessibles par l'utilisateur d'analyse sur les actifs qui sont analysés. Si WMI n'est pas disponible, l'erreur suivante est signalée dans les résultats d'analyse :

```
Local Checks Error – Unable to Query WMI serviceMount Remote Filesystem
```

Dans QRadar Vulnerability Manager version 7.2.3 et versions suivantes, une icône d'avertissement sous forme de triangle jaune s'affiche en regard de l'actif dans les résultats d'analyse.

Pour lire des données WMI sur un serveur distant, il est nécessaire d'établir une connexion entre votre ordinateur de gestion (sur lequel est installé le logiciel de surveillance) au serveur que vous surveillez. Si le serveur cible exécute Windows Firewall (également appelé Internet Connection Firewall) qui est installé sur les ordinateurs Windows XP et Windows 2003, vous devez configurer le pare-feu pour permettre le passage des demandes WMI distantes. Pour configurer le pare-feu Windows afin d'autoriser les demandes WMI à distance, ouvrez une invite shell et entrez la commande suivante :

```
netsh firewall set service RemoteAdmin enable
```

Si votre analyse de correctifs n'aboutit pas, procédez comme suit.

Procédure

1. Sur le serveur cible, sélectionnez **Panneau de configuration** > **Outils d'administration** > **Gestion de l'ordinateur**.
2. Développez **Services et applications**.
3. Cliquez avec le bouton droit sur **Contrôle WMI**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Sécurité**.
5. Cliquez sur **Sécurité**.
6. Si nécessaire, ajoutez l'utilisateur d'analyse et cliquez sur l'option **Appel à distance autorisé** pour l'utilisateur ou le groupe qui demande des données WMI. Pour ajouter un utilisateur ou groupe d'analyse :
   a) Cliquez sur **Ajouter**.
   b) Dans la zone **Entrez les noms d'objets à sélectionner** entrez le nom de groupe d'utilisateurs ou d'utilisateur.
   c) Cliquez sur **OK**.
7. Cliquez sur **Avancé** et appliquez à la racine et aux espaces de sous-nom.

   Remarque : Dans certains cas, vous devrez peut-être également configurer le pare-feu Windows et les paramètres DCOM.

   Si vous rencontrez des problèmes WMI, vous pouvez installer les outils d'administration WMI à partir du site Web de Microsoft.

   Ces outils comprennent un navigateur WMI destiné à simplifier la connexion à une machine distante et l'exploration des informations WMI. Ils peuvent vous aider à isoler tous les problèmes de connectivité dans un environnement plus direct et plus simple.

Définition de droits DCOM minimum

Pour la connexion à un ordinateur distant à l'aide de WMI, vous devez vous assurer que les paramètres DCOM et les paramètres de sécurité d'espace-noms WMI sont activés pour la connexion.

Pourquoi et quand exécuter cette tâche

Pour accorder des droits de lacement et d'activation à distance DCOM pour un utilisateur ou un groupe, procédez comme suit.

Procédure

1. Cliquez sur **Démarrer** > **Exécuter**, entrez DCOMCNFG et cliquez sur **OK**.
2. Dans la boîte de dialogue **Services de composants**, développez **Services de composants**, **Ordinateurs**, puis cliquez avec le bouton droit sur **Poste de travail** et sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de l'ordinateur**, cliquez sur l'onglet **Sécurité COM**.
4. Sous **Autorisations d'exécution et d'activation**, cliquez sur **Modifier les limites**.
5. Dans la boîte de dialogue **Autorisation d'exécution**, si votre nom ou votre groupe n'apparaît pas dans la liste **Noms d'utilisateur ou de groupes**, procédez comme suit.
   a) Dans la boîte de dialogue **Autorisation d'exécution**, cliquez sur **Ajouter**.
   b) Dans la boîte de dialogue **Sélectionner les utilisateurs, ordinateurs ou groupes**, ajoutez votre nom et le groupe dans la zone **Entrez les noms d'objets à sélectionner**, puis cliquez sur **OK**.
6. Dans la boîte de dialogue **Autorisation d'exécution**, sélectionnez votre utilisateur et votre groupe dans la zone **Noms d'utilisateurs ou de groupes**.
7. Dans la colonne **Autoriser**, sous **Autorisations pour l'utilisateur**, sélectionnez **Exécution à distance** et **Activation à distance**, puis cliquez sur **OK**.

Définition de droits d'accès distant DCOM

Vous devez définir des autorisations d'accès à distance DCOM pour certains utilisateurs et groupes.

Pourquoi et quand exécuter cette tâche

Si l'ordinateur A se connecte à distance à l'ordinateur B, vous pouvez définir les autorisations d'accès à distance sur l'ordinateur B pour permettre à un utilisateur ou un groupe qui n'est pas membre du groupe Administrateurs sur l'ordinateur B de se connecter à distance à l'ordinateur B.

Procédure

1. Cliquez sur **Démarrer** > **Exécuter**, entrez DCOMCNFG et cliquez sur **OK**.
2. Dans la boîte de dialogue **Services de composants**, développez **Services de composants**, **Ordinateurs**, puis cliquez avec le bouton droit sur **Poste de travail** et sélectionnez **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de l'ordinateur**, cliquez sur l'onglet **Sécurité COM**.
4. Dans la section **Autorisations d'accès**, cliquez sur **Modifier les limites**.
5. Configurez l'un des utilisateurs ou groupes suivants pour lui attribuer des droits d'accès à distance :
   - Dans la boîte de dialogue **Autorisations d'accès**, sélectionnez le nom **ANONYMOUS LOGON** dans la zone **Noms d'utilisateurs ou de groupes**. Dans la zone **Permissions for ANONYMOUS LOGON**, cochez la case **Autoriser** pour **Accès distant**, puis cliquez sur **OK**.
   - Dans la boîte de dialogue **Autorisations d'accès**, sélectionnez le nom **Tous** dans la zone **Noms d'utilisateurs ou de groupes**. Dans la zone **Permissions for Everyone**, cochez la case **Autoriser** pour **Accès distant**, puis cliquez sur **OK**.

- Dans la boîte de dialogue **Autorisations d'accès**, sélectionnez le nom **<utilisateur d'analyse QVM>** dans la zone **Noms d'utilisateurs ou de groupes**. Dans la zone des droits d'accès pour <utilisateur d'analyse QVM>, cochez la case **Autoriser** pour **Accès distant**, puis cliquez sur **OK**.

Remarque : Si vous souhaitez utiliser le compte utilisateur **<Utilisateur d'analyse QVM>**, vous devez créer le compte utilisateur avant d'accorder les droits d'accès distants DCOM. Vous devez également configurer l'accès WMI (étape 6) pour cet utilisateur.

Partages administratifs

Tous les ordinateurs Windows disposent de partages administratifs `\\machinename\driveletter$`, en particulier lorsqu'ils font partie d'un domaine.

QRadar Vulnerability Manager utilise les partages administratifs pour détecter les vulnérabilités dans certaines applications :

- Mozilla Firefox
- Mozilla Thunderbird
- Java™ FX
- Apache Archiva
- Apache Continuum
- Préférences de Google Chrome

Les partages administratifs ne sont pas visibles des autres utilisateurs non administratifs, et certaines organisations désactivent les partages administratifs ou utilisent des comptes utilisateurs non administratifs pour l'analyse. Si les partages administratifs ne sont pas accessibles, QRadar Vulnerability Manager peut ignorer des vulnérabilités dans les produits de la liste précédente ou produire des faux positifs. En général, les tests de vulnérabilité QRadar Vulnerability Manager utilisent uniquement les partages administratifs en dernier ressort, et ont recours aux analyses de registre et à WMI.

Activation des partages administratifs

Sous Windows Vista ou versions suivantes, les partages administratifs sont désactivés par défaut en mode "workgroup".

Pourquoi et quand exécuter cette tâche

Pour activer les partages administratifs, procédez comme suit.

Procédure

1. Cliquez sur **Démarrer** > **Exécuter** et saisissez `regedit`.
2. Accédez à la clé suivante : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\System**
3. Cliquez avec le bouton droit sur **Contrôle WMI**, puis cliquez sur **Propriétés**.
4. Ajoutez un nouveau DWORD nommé : `LocalAccountTokenFilterPolicy`
5. Définissez la valeur 1.

Désactivation des partages administratifs

Certaines organisations ne souhaitent pas activer les partages administratifs. Toutefois, lors de l'activation du service de registre distant, le service de serveur est démarré et les partages administratifs sont activés.

Pourquoi et quand exécuter cette tâche

Pour désactiver les partages administratifs, modifiez la clé de registre suivante :

Procédure

1. Cliquez sur **Démarrer** > **Exécuter** et saisissez `regedit`.
2. Accédez à la clé suivante : **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \LanManServer**
3. Définissez le paramètre **`AutoShareWks`** sur `0`.

   Remarque : Cette action ne désactive pas le partage IPC$. Même si ce partage n'est pas utilisé pour l'accès aux fichiers directement, assurez-vous que l'accès anonyme à ce partage est déactivé. Vous pouvez aussi retirer complètement le partage IPC$ en le supprimant au démarrage à l'aide de la commande suivante :

   ```
   net share IPC$ /delete
   ```

   Utilisez cette méthode pour retirer également les partages C$ et D$.

Configuration manuelle de l'authentification NTLMv2 pour éviter des échecs d'analyse

Vous devez configurer manuellement les analyses de données d'identification exécutées pour les actifs qui utilisent Microsoft New Technology LAN Manager version 2 (NTLMv2) afin d'éviter les échecs d'analyse.

Pourquoi et quand exécuter cette tâche

Lorsque vous exécutez une analyse de données d'identification pour un actif Windows qui utilise le niveau d'authentification LAN Manager de `"Send NTLMv2 response only. Refuse LM and NTLM"`, l'authentification de certains outils d'analyse peut échouer. Un triangle d'avertissement jaune s'affiche pour l'actif et une vulnérabilité d'erreur des vérifications locales est émise. Le fait d'exécuter plusieurs fois l'analyse peut provoquer le verrouillage du compte utilisateur hors de l'actif.

Afin d'éviter l'échec des analyses exécutées pour les actifs qui utilisent NTMLv2, activez manuellement l'authentification NTMLv2 dans les fichiers suivants sur le scanner QVM :

- `/opt/qvm/etc/smb.conf`
- `/opt/qvm/etc/smb.conf.smbv1`
- `/opt/qvm/etc/smb.conf.smbv2`

Procédure

Ouvrez chacun de ces fichiers et ajoutez la ligne suivante : `client ntlmv2 auth = yes`

Chapitre 9. Règles d'exception relatives aux vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer des règles d'exception afin de réduire le nombre de faux positifs en matière de vulnérabilités.

Lorsque vous appliquez des règles d'exception à des vulnérabilités, vous réduisez le nombre de vulnérabilités affichées dans les résultats de la recherche.

Si vous créez une exception de vulnérabilité, cette dernière n'est pas retirée de QRadar Vulnerability Manager.

Affichage des règles d'exception

Pour afficher les exceptions de vulnérabilité, vous pouvez effectuer une recherche dans les données de vulnérabilité en utilisant des filtres de recherche.

Pour afficher les règles d'exception, cliquez sur l'onglet **Vulnérabilités**, puis sur **Exceptions de vulnérabilité** dans le panneau de navigation.

Conseil : Le tableau **Règles des exceptions** affiche uniquement le dernier commentaire entré. Pour consulter d'autres commentaires, survolez la colonne **Commentaire** correspondant à la règle.

Tâches associées

Réduction du nombre de faux positifs de vulnérabilité

Application d'une règle d'exception de vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez appliquer manuellement une règle d'exception à une vulnérabilité qui, selon vous, n'est pas une menace.

Si vous appliquez une règle d'exception, la vulnérabilité ne s'affichera plus dans les résultats de la recherche QRadar Vulnerability Manager. Cependant, elle n'est pas supprimée dans QRadar Vulnerability Manager.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités** > **Par réseau**.
3. Recherchez vos données de vulnérabilité. Dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
4. Cliquez sur le lien dans la colonne **Instances de vulnérabilité**.
5. Sélectionnez la vulnérabilité pour laquelle vous souhaitez créer une règle d'exception.
6. Dans la barre d'outils, sélectionnez **Actions** > **Exception**.
7. Dans la zone **Règle d'exception**, sélectionnez une option d'expiration.
8. Sélectionnez un motif dans la liste **Motif**.
9. Dans la zone **Actifs**, sélectionnez vos actifs cible pour la règle d'exception en effectuant un choix parmi les options suivantes :
   - Pour appliquer l'exception à tous les actifs, sélectionnez **Exception concernant vulnérabilité pour tous les actifs**.
   - Pour appliquer l'exception à un actif spécifique, sélectionnez **Exception pour actif spécifique avec IP actuel**.

     Par défaut, l'actif associé à la vulnérabilité choisie à l'étape 5 est sélectionné.

© Copyright IBM Corp. 2012, 2020

- Pour appliquer l'exception à une adresse IP, à un routage CIDR ou à un réseau, entrez les détails, sélectionnez votre domaine puis cliquez sur **Ajouter**.

  Si vous sélectionnez un réseau spécifique dans la hiérarchie, l'exception s'applique uniquement aux adresses IP de ce réseau. Par exemple, si une adresse IP est affectée à deux réseaux de la hiérarchie, l'exception ne s'applique pas à la même adresse IP dans le deuxième réseau, sauf si vous avez défini une exception pour cela.

10. Dans la zone **Remarques**, entrez des informations dans la zone de texte **Commentaires**.
11. Cliquez sur **Sauvegarder** ou sur **Annuler**.

Concepts associés

Gestion des faux positifs

Généralement, les faux positifs d'une analyse de vulnérabilité se produisent lorsque le scanner peut uniquement accéder à un sous-ensemble de l'information requise, ce qui l'empêche de déterminer clairement si une vulnérabilité existe ou non.

Tâches associées

Recherche des données de vulnérabilité

Gestion d'une règle d'exception de vulnérabilité

Si vous recevez de nouvelles informations concernant une vulnérabilité, vous pouvez mettre à jour ou supprimer une règle d'exception de vulnérabilité existante.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Exceptions de vulnérabilité**.
3. Cliquez sur la vulnérabilité que vous voulez gérer.
4. Dans la barre d'outils, sélectionnez une option dans le menu **Actions**.

   Important : Si vous supprimez une règle d'exception de vulnérabilité, aucun avertissement ne s'affiche. La vulnérabilité est immédiatement supprimée.
5. Cliquez sur **Sauvegarder**.

Recherche d'exceptions de vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez rechercher vos données de vulnérabilité et filtrer les résultats de la recherche afin d'afficher des exceptions de vulnérabilités.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez **Gérer les vulnérabilités** > **Par actif**.
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Pour filtrer vos données de vulnérabilité afin d'inclure des exceptions de vulnérabilités, dans le panneau **Paramètres de recherche**, sélectionnez l'une des options suivantes :
   - Inclure les exceptions de vulnérabilité

     Affiche toutes les vulnérabilités, y compris celles sur lesquelles une exception est appliquée.
   - Inclure uniquement les exceptions de vulnérabilité

     Affiche uniquement les vulnérabilités sur lesquelles une exception est appliquée.
5. Cliquez sur **Ajouter un filtre**.
6. Cliquez sur **Rechercher**.

Chapitre 10. Examens des analyses

Dans IBM QRadar Vulnerability Manager, vous pouvez examiner le récapitulatif des données des actifs et des vulnérabilités pour chaque analyse.

Pour examiner les analyses des vulnérabilités, vous pouvez exécuter les tâches suivantes :

- Créez des critères de recherche de vulnérabilités complexes.
- Examinez les niveaux de risque d'exploitation au niveau d'un réseau, d'un actif et d'une vulnérabilité.
- Hiérarchisez vos processus de correction des vulnérabilités.

Résultats d'analyse

La page **Résultats de l'analyse** vous permet d'examiner en détail les informations suivantes :

- Progression d'une analyse et outils d'analyse dans la file d'attente et en cours d'exécution.
- Etat d'une analyse. Par exemple, une analyse dont le statut est **Arrêté** indique que l'analyse s'est terminée correctement ou a été annulée.
- Niveau de risque associé à chaque profil d'analyse terminée. La colonne **Score** présente le score CVSS (Common Vulnerability Scoring System) associé au profil d'analyse terminée. Le score temporel et le score de base CVSS sont inclus dans le calcul de ce score contrairement au score environnemental CVSS. Ce dernier est intégré dans la colonne **Score de risque** de trouvant dans la fenêtre **Gérer les vulnérabilités**.
- Nombre total d'actifs détectés par l'analyse.
- Nombre total de vulnérabilités détectées par le profil d'analyse terminée.
- Nombre total de services ouverts détectés par le profil d'analyse terminée.

Remarque : La progression de l'analyse peut indiquer que l'analyse est terminée (100 %) alors que les résultats sont toujours en cours de traitement. Pour voir si le traitement est terminé, survolez la barre de progression.

Nombre de vulnérabilités

La page **Résultats de l'analyse** affiche les vulnérabilités et les instances des vulnérabilités dans les colonnes **Vulnérabilités** et **Instances des vulnérabilités**, respectivement.

- La colonne **Vulnérabilités** affiche le nombre total de vulnérabilités uniques qui ont été détectées sur tous les actifs analysés.
- Lorsque vous analysez plusieurs actifs, la même vulnérabilité peut être présente sur des actifs différents. Par conséquent, la colonne **Instances de vulnérabilité** affiche le nombre total de vulnérabilités qui ont été détectées sur tous les actifs analysés.

Rechercher les résultats d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez rechercher vos résultats d'analyse et les filtrer.

Par exemple, vous pouvez vouloir identifier des analyses récentes, des analyses effectuées sur une adresse IP spécifique ou des analyses ayant détecté une vulnérabilité particulière.

Pourquoi et quand exécuter cette tâche

Utilisez la zone **Nom** sur l'onglet **Vulnerabilities** pour rechercher les résultats par nom de profil d'analyse. Pour utiliser des critères plus avancés dans votre recherche, procédez comme suit.

Les restrictions de niveau domaine ne sont pas appliquées tant que les profils de sécurité ne sont pas mis à jour avec un domaine associé et les modifications ne sont pas déployées.

© Copyright IBM Corp. 2012, 2020

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Résultats de l'analyse**.
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.

   Pour rechercher vos résultats d'analyse, aucune zone n'est obligatoire. Tous les paramètres sont facultatifs.
4. Pour afficher les résultats des analyses effectuées récemment dans une période donnée (en jours), entrez une valeur dans la zone **Analyse effectuée au cours des derniers jours**.
5. Pour afficher les résultats des analyses de détection d'une vulnérabilité spécifique, cliquez sur **Parcourir** dans la zone **Contient la vulnérabilité**.
6. Pour afficher les résultats des analyses qui étaient planifiées uniquement, cliquez sur **Exclure de l'analyse à la demande**.
7. Cliquez sur **Rechercher**.

Concepts associés

Planification des analyses
Dans IBM QRadar Vulnerability Manager, vous pouvez planifier les dates et les heures auxquelles vous souhaitez analyser vos actifs réseau pour rechercher des vulnérabilités connues.

Inclusion d'en-têtes de colonne dans les recherches d'actif

Limitez les recherches d'actif à l'aide de filtres incluant des profils d'actifs, un nom, un nombre de vulnérabilités et un score de risque.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, cliquez sur **Profils d'actifs** puis, dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
3. Dans la zone contenant les noms de colonne, dans la zone située à gauche, cliquez sur les en-têtes de colonne que vous voulez inclure dans votre recherche, puis cliquez sur le bouton fléché afin de déplacer les en-têtes sélectionnés vers la zone située à droite.
4. Cliquez sur boutons haut et bas pour modifier la priorité des en-têtes de colonne sélectionnés.
5. Lorsque la zone à droite contient tous les en-têtes de colonne sur lesquels vous voulez effectuer la recherche, cliquez sur **Rechercher**.

Gestion des résultats d'analyse

Dans IBM QRadar Vulnerability Manager, sur la page **Résultats de l'analyse**, vous pouvez gérer vos résultats d'analyse ainsi que les analyses en cours d'exécution.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Résultats de l'analyse**.
3. Si vous souhaitez relancer les analyses effectuées, sélectionnez la case à cocher dans les lignes attribuées aux analyses et cliquez sur **Exécuter**.

   Une analyse terminée a le statut **Arrêté**.
4. Pour supprimer des résultats d'analyse terminée :
   a) Sur la page **Résultats d'analyse**, activez la case à cocher dans les lignes attribuées aux résultats de l'analyse que vous souhaitez supprimer.

b) Dans la barre d'outils, cliquez sur **Supprimer**.

Si vous supprimez un ensemble de résultats d'analyse, aucun avertissement ne s'affiche. Les résultats sont immédiatement supprimés.

A faire : Lorsque vous sélectionnez l'ensemble de résultats d'analyse, ni les données d'analyse du modèle d'actif QRadar ni le profil d'analyse ne sont supprimés.

5. Pour annuler une analyse en cours d'exécution :
   a) Sur la page **Résultats d'analyse**, activez la case à cocher dans les lignes attribuées aux analyses que vous souhaitez supprimer.
   b) Dans la barre d'outils, cliquez sur **Annuler**.

   Vous pouvez annuler une analyse dont le statut est **En cours d'exécution** ou **En pause**.

   Après l'annulation d'une analyse, son état est **Arrêté**.

Nouvelle publication des résultats d'analyse

Si le modèle d'actif n'est pas automatiquement mis à jour avec les résultats d'une analyse terminée, vous pouvez publier ces résultats manuellement à partir de la page **Résultats d'analyse**.

Pourquoi et quand exécuter cette tâche

Si vous n'avez pas coché la case **Update Asset Model** lorsque vous avez configuré un profil d'analyse, les résultats d'analyse ne sont pas automatiquement publiés sur le modèle d'actif. Vous pouvez mettre à jour le modèle d'actif manuellement avec des résultats d'analyse pour ce profil.

Procédure

1. Accédez à **Vulnérabilités** > **Résultats d'analyse**
2. Activez la case à cocher dans la ligne attribuée aux résultats d'analyse que vous souhaitez republier.
3. Cliquez sur **Republier** dans la barre d'outils de la page **Résultats d'analyse**, puis cliquez sur **OK**.

   Une icône d'avertissement rouge dans la colonne **Type** indique que le modèle d'actif n'est pas mis à jour avec les résultats d'analyse sélectionnés. L'icône d'avertissement rouge disparaît une fois que le processus de republication est terminé.
4. Déplacez le pointeur de la souris sur la colonne **Type** pour afficher la confirmation dans l'infobulle que le modèle d'actif est mis à jour pour les résultats d'analyse sélectionnés.

   Remarque : Vous pouvez republier plusieurs résultats d'analyse simultanément. Toutefois, si vous republiez deux ensembles de résultats d'analyse à partir du même profil, le modèle d'actif est mis à jour uniquement avec la dernière série de résultats d'analyse.

   Si vous avez configuré la génération automatique de rapport sur l'onglet **E-mail** de la page **Configuration du profil d'analyse**, les rapports sont générés et envoyés aux adresses de courrier électronique que vous avez configurées lorsque vous avez republié les résultats d'analyse.

Niveaux de risque et catégories de vulnérabilité associés aux actifs

Dans IBM QRadar Vulnerability Manager, vous pouvez sonder le niveau de risque d'exploitation de vos actifs analysés sur la page **Actifs des résultats d'analyse**.

La page **Actifs des résultats d'analyse** fournit un récapitulatif des risques et des vulnérabilités relatifs à chacun des actifs que vous avez analysés à l'aide d'un profil d'analyse.

Score du risque

Chaque vulnérabilité détectée sur votre réseau a un score du risque qui est calculé sur l'indice de base CVSS (Common Vulnerability Scoring System). Un score du risque élevé indique la possibilité d'une exploitation de la vulnérabilité.

Sur la page **Actifs des résultats d'analyse**, la colonne **Score** cumule le score du risque présenté par chaque vulnérabilité sur un actif. La valeur cumulée fournit une indication du niveau de risque associé à chaque actif.

Pour identifier rapidement les actifs les plus exposés à l'exploitation d'une vulnérabilité, cliquez sur l'en-tête la colonne **Score** pour trier les actifs par niveau de risque.

Nombre et catégories de vulnérabilités

La page **Actifs des résultats d'analyse** affiche le nombre total de vulnérabilités et de services ouverts qui sont découverts sur chaque actif analysé.

Pour identifier les actifs présentant le plus grand nombre de vulnérabilités, cliquez sur l'en-tête de colonne **Instances de vulnérabilité** afin de classer vos actifs.

Les colonnes **Elevée**, **Moyenne**, **Faible** et **Avertissement** regroupent toutes les vulnérabilités en fonction de leur risque.

Les colonnes **% vérifications de règle réussies** et **% vérifications de règle échouées** affichent le pourcentage de vérifications de règles que l'actif a réussies ou échouées dans l'analyse de référence. Cliquez sur les valeurs dans ces colonnes pour voir plus d'informations sur les contrôles de règles qui ont réussi ou échoué sur la page **Vérifications de règle de résultats d'analyse**.

Données relatives aux actifs, aux vulnérabilités et aux services ouverts

Dans IBM QRadar Vulnerability Manager, la page **Détails de l'actif - Résultats d'analyse** affiche des données sur les actifs, les vulnérabilités et les services ouverts.

Les options de la barre d'outils vous permettent de basculer entre l'affichage des vulnérabilités et l'affichage des services ouverts.

La page **Détails de l'actif - Résultats d'analyse** fournit les informations suivantes :

- Des informations récapitulatives sur l'actif que vous avez analysé, telles le système d'exploitation et le groupe du réseau.
- Une liste des vulnérabilités ou des services ouverts qui ont été détectés sur l'actif analysé.
- Différentes méthodes de catégorisation et de classement de votre liste de vulnérabilités ou de services ouverts, par exemple, par **risque**, **gravité** et **score**.
- Un moyen rapide d'afficher des informations sur le service ouvert ou la vulnérabilité. Dans la barre d'outils, cliquez sur **Vulnérabilités** ou sur **Services ouverts**.
- Un moyen simple d'afficher des informations détaillées sur l'actif que vous avez analysé. Dans la barre d'outils, cliquez sur **Détails de l'actif**.
- Une autre méthode de création d'une exception de vulnérabilité. Dans la barre d'outils, cliquez sur **Actions** > **Exception**.

L'icône attention indique que l'analyse a échoué. Survolez l'icône pour plus de détails.

Pour plus d'informations sur la fenêtre **Détails de l'actif**, voir le *Guide d'utilisation* de votre produit.

Concepts associés

Règles d'exception relatives aux vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer des règles d'exception afin de réduire le nombre de faux positifs en matière de vulnérabilités.

Affichage de l'état des téléchargements de correctif d'actif

Affichez si un téléchargement de correctif d'actif est instance. Si aucun téléchargement n'est en instance, l'actif à tous les correctifs disponibles.

Procédure

1. Recherchez l'actif dont vous voulez confirmer l'état de correctif.
2. Cliquez sur Adresse IP d'actif afin d'ouvrir la fenêtre **Détails de l'actif**.
3. Cliquez sur **Détails** > **Propriétés** afin d'ouvrir la fenêtre **Propriétés d'actif**.
4. Cliquez sur la flèche **Correctifs Windows**.
5. Consultez l'état de correctif dans la colonne **En attente**.
   - Vrai - l'actif a des correctifs en attente de téléchargement.
   - Faux - l'actif n'a aucun correctif en attente de téléchargement.

Risque et gravité PCI des vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez examiner le risque et la gravité PCI (Payment Card Industry) de chaque vulnérabilité détectée par une analyse.

Vous pouvez examiner les informations suivantes :

- Le niveau de risque associé à la vulnérabilité.
- Le nombre d'actifs de votre réseau sur lesquels une vulnérabilité spécifique a été trouvée.

Pour avoir des détails sur une vulnérabilité, vous pouvez cliquer sur un lien de vulnérabilité dans la colonne **Vulnérabilité**.

Identification et résolution des problèmes d'analyse

Identifiez et résolvez les problèmes d'analyse dans votre réseau en examinant les journaux ainsi que les messages d'erreur et d'avertissement.

Temps de réponse lent de l'hôte analysé
Déployez le dispositif d'analyse QRadar Vulnerability Manager à proximité des actifs que vous analysez. Utilisez des commandes, telles que traceroute, afin de vous assurer que les paquets atteignent l'actif en moins de 50 ms. Sinon la durée des analyses peut être longue.

Statut de vérification des outils d'analyse

Si l'exécution de vos analyses est en cours depuis longtemps et que vous souhaitez savoir quels outils sont en cours d'utilisation, survolez le pourcentage de progression se trouvant sur la page des résultats de l'analyse avec le curseur afin d'afficher une fenêtre en incrustation, présentant l'outil actif.

L'analyse de correctif ne se connecte pas à un actif Linux
Si l'outil d'analyse de correctif ne se connecte pas à un actif Linux, une icône d'avertissement triangulaire jaune s'affiche en regard de l'actif dans les résultats d'analyse.

Le message d'erreur SSH `Patch Scanning - Failed Logon` peut s'afficher.

Validez le nom d'utilisateur et le mot de passe. Si vous utilisez le chiffrement de clé publique, vérifiez la clé publique.

Pour analyser des systèmes d'exploitation Linux en utilisant l'authentification sécurisée, configurez le chiffrement par clé publique entre la console ou l'hôte géré et les cibles d'analyse. Les comptes utilisateur non root doivent disposer des droits appropriés pour exécuter les commandes nécessaires à QRadar Vulnerability Manager pour l'analyse des correctifs sur les ordinateurs Linux et UNIX. Pour plus d'informations, voir Chapitre 7, «Analyse des correctifs authentifiés», à la page 61.

Erreur des vérifications locales

Si l'outil d'analyse de correctif ne peut pas se connecter à un actif Windows, une icône d'avertissement triangulaire jaune s'affiche en regard de l'actif dans les résultats d'analyse.

Le message d'erreur `Local Checks Error` peut s'afficher. Il indique que l'analyse authentifiée a échoué.

Vous pouvez configurer des données d'identification dans le profil d'analyse ou dans les données d'identification centralisées. Si le scanner analyse des hôtes Windows, les trois services Windows suivants doivent être configurés correctement :

- Registre à distance
- Windows Management Instrumentation (WMI)
- Partages d'administration

Pour plus d'informations, voir Chapitre 8, «Analyse sur les actifs Windows», à la page 67.

Titres de vulnérabilité identiques dans différentes bases de connaissances

Si la base de connaissances d'un bulletin est remplacée par une base de connaissances d'un bulletin ultérieur, le titre de vulnérabilité ne change pas.

Analyse bloquée

Si l'analyse est bloquée ou si elle s'interrompt, un utilisateur autorisé peut se connecter au scanner et vérifier la connectivité avec le processeur de l'analyse. Pour connaître les erreurs de connexion, consultez les fichiers journaux QRadar Vulnerability Manager.

L'analyse du port UDP dure longtemps

Si une politique d'analyse est configurée pour analyser tous les ports UDP, l'analyse peut être longue, plus particulièrement si l'hôte cible a plusieurs ports UDP fermés. Pour les analyses PCI, il n'est pas nécessaire d'analyser tous les ports UDP. Pour plus d'informations, voir «Durées d'analyse et analyse des ports», à la page 28.

Avertissement sur le nombre d'actifs analysés

Si le message d'avertissement suivant s'affiche sur l'écran **Résultats d'analyse**, les performances et le résultats de l'analyse ne sont pas affectés :

WARNING: You have scanned *<number>* assets but are only licensed to scan *<number>* assets. License Update Required!

Remarque : Il est recommandé de vérifier le nombre d'analyses d'actif autorisées par votre licence QRadar Vulnerability Manager.

Envoi d'un e-mail aux propriétaires d'actif lors du démarrage et de l'arrêt des analyses de vulnérabilité

Envoyez un e-mail aux propriétaires techniques d'actif afin de les informer de la planification de l'analyse. Vous pouvez aussi envoyer des rapports aux propriétaires d'actif .

Avant de commencer

Configurez le serveur de messagerie du système et les propriétaires techniques pour les actifs. Pour plus d'informations, voir *IBM QRadar Administration Guide*.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Cliquez sur **Admin** > **Profils d'analyse**.
3. Sur la ligne affectée à l'analyse que vous souhaitez modifier, cochez la case et cliquez sur **Editer** sur la barre d'outils.
4. Dans la zone **Contenu de l'e-mail** de l'onglet **E-mail**, sélectionnez les cases appropriées.
5. Si vous avez sélectionné la case à cocher **Rapports** dans la zone **Rapports disponibles**, sélectionnez les rapports à envoyer par e-mail et cliquez sur la flèche pour déplacer les rapports dans la zone **Rapports sélectionnés**.

   Les rapports peuvent être volumineux. Confirmez que les rapports envoyés ne sont pas rejetés par fournisseur de messagerie du destinataire.
6. Dans la zone du **destinataire de l'e-mail**, sélectionnez les destinataires qui doivent recevoir les e-mails :
   - Pour envoyer l'e-mail aux propriétaires techniques configurés des actifs analysés, sélectionnez la case correspondant aux **propriétaires techniques**. Les propriétaires techniques reçoivent des e-mails sur leurs actifs uniquement.
   - Pour entrer ou sélectionner des adresses e-mail dans la zone, sélectionnez la case correspondant aux **adresses**. Sélectionnez les e-mails, puis cliquez sur l'option permettant de **vous ajouter** afin qu'un e-mail soit envoyé aux destinataires d'e-mail sélectionnée. Les adresses e-mail entrées reçoivent des e-mails et des rapports concernant tous les actifs analysés.
7. Cliquez sur **Sauvegarder**.

Chapitre 11. Gestion des vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez gérer, rechercher et filtrer vos données de vulnérabilité afin de vous concentrer sur celles qui constituent le plus grand risque pour votre organisation.

Les données de vulnérabilité affichées s'appuient sur les informations de statut de vulnérabilité qui sont conservées dans le modèle d'actif QRadar. Ces informations incluent les vulnérabilités qui ont été détectées par le programme d'analyse QRadar Vulnerability Manager, mais également celles qui ont été importées de produits d'analyse externes.

Gérez vos vulnérabilités pour fournir les informations suivantes :

- Une vue de réseau de votre posture de vulnérabilité actuelle.
- Identifiez les vulnérabilités qui constituent le plus grand risque pour votre organisation et affectent les vulnérabilités aux utilisateurs QRadar en vue d'une correction.
- Etablissez la manière d'influencer lourdement votre réseau par les vulnérabilités puis affichez les informations détaillées sur les actifs de réseau contenant les vulnérabilités.
- Décidez des différentes vulnérabilités qui constituent un risque moindre pour votre organisation puis créez des exceptions de vulnérabilités.
- Affichez les informations historiques sur les vulnérabilités se trouvant sur votre réseau.
- Affichez les données de vulnérabilité par réseau, actif, vulnérabilité, service ouvert ou par instance de vulnérabilité.

Système CVSS (Common Vulnerability Scoring System)

Le système CVSS (Common Vulnerability Scoring System) permet d'évaluer la gravité et les risques en matière de sécurité du système informatique.

CVSS est une infrastructure ouverte composée des groupes de métriques suivants :

- Base
- Temporel
- Environnemental

Base
La plage de gravité du score de base s'étend de 0 à 10 et représente les caractéristiques inhérentes de la vulnérabilité. Le score de base constitue une partie importante du score CVSS final. Il peut être divisé en sous-scores, présentés ci-dessous :

- Impact

  Le sous-score d'impact représente les métriques concernant l'impact de confidentialité, d'intégrité et de disponibilité d'une vulnérabilité exploitée.
- Exploitabilité

  Le sous-score d'exploitabilité représente les métriques de vecteur d'accès, de complexité d'accès et d'authentification. De plus, il mesure le mode d'accès à la vulnérabilité, la complexité de l'attaque et le nombre de fois où un attaquant doit s'authentifier pour exploiter une vulnérabilité.

Temporel

Le score temporel représente les caractéristiques d'une menace de vulnérabilité qui évolue avec le temps et se compose des métriques suivantes :

- Exploitabilité

© Copyright IBM Corp. 2012, 2020

Disponibilité des techniques ou du code pouvant être utilisés pour exploiter la vulnérabilité, qui change avec le temps.

- Niveau de résolution

  Niveau de résolution disponible pour une vulnérabilité.

- Niveau de fiabilité du rapport

  Niveau de fiabilité concernant l'existence de la vulnérabilité et crédibilité de ses détails techniques.

Environnemental

Le score environnemental représente les caractéristiques de la vulnérabilité impactées par l'environnement de l'utilisateur. Configurez les métriques environnementales suivantes pour mettre en évidence les vulnérabilités des actifs importants ou critiques en appliquant des métriques environnementales plus élevées. Appliquez les scores les plus élevés aux actifs les plus importants car les pertes associées à ces actifs ont des conséquences plus importantes pour l'organisation.

- Dommages collatéraux potentiels (CDP)

  Risque de danger de mort ou de perte d'actifs physiques par endommagement ou vol.

- Distribution cible (TD)

  Proportion de systèmes vulnérables dans l'environnement de l'utilisateur.

- Exigences de confidentialité (CR)

  Niveau d'impact de la perte de confidentialité lorsqu'une vulnérabilité est exploitée dans cet actif.

- Exigences d'intégrité (IR)

  Cette métrique définit le niveau d'impact de la perte d'intégrité lorsqu'une vulnérabilité est exploitée dans cet actif.

- Exigences de disponibilité (AR)

  Niveau d'impact pour la disponibilité de l'actif lorsqu'une vulnérabilité est exploitée dans cet actif.

Tâches associées

Configuration du risque environnemental pour un actif
Utilisez le score environnemental CVSS pour manipuler et définir la priorité du score de risque pour les actifs sélectionnés. Si vous configurez les paramètres **CVSS, poids et conformité** pour un actif, vous pouvez appliquer des scores de risque plus élevés pour les actifs qui sont plus importants ou critiques.

Examen détaillé des scores du risque des vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez examiner en détail les scores du risque des vulnérabilités et comprendre le mode de calcul de chaque score.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Cliquez sur la colonne **Score de risque** pour classer vos vulnérabilités en fonction du risque.
4. Pour examiner en détail le score du risque d'une vulnérabilité, survolez-le avec la souris.

Détails du score du risque

Dans IBM QRadar Vulnerability Manager, les scores du risque des vulnérabilités fournissent une indication du risque que pose une vulnérabilité à votre organisation.

Avec IBM QRadar Risk Manager, vous pouvez configurer des règles qui ajustent les scores du risque des vulnérabilités et attirent ainsi votre attention sur les tâches de résolution importantes.

Score du risque

La page **Score de risque** fournit un contexte réseau spécifique en s'appuyant sur les métriques de base, temporelles et environnementales du système CVSS (Common Vulnerability Scoring System).

Lorsque QRadar Risk Manager n'est pas utilisé pour gérer les risques, la colonne **Score de risque** affiche le score de la métrique environnementale CVSS avec une valeur maximale de 10.

Ajustements du risque

Si IBM QRadar Risk Manager est installé et que vous avez configuré des règles du risque pour les vulnérabilités, les ajustements du risque sont indiqués dans une liste. Ces ajustements augmentent ou diminuent le risque global associé à une vulnérabilité.

Concepts associés

Intégration à QRadar Vulnerability Manager

Tâches associées

Hiérarchisation des vulnérabilités à haut risque par l'application de règles du risque

Classification des risques personnalisés

Utilisez les scores des risques personnalisés de QRadar Vulnerability Manager pour classer les vulnérabilités qui représentent le risque le plus sérieux pour votre organisation. La classification des risques personnalisés vous permet d'ignorer le risque d'une vulnérabilité en établissant votre propre classification.

En fonction de vos besoins, vous pouvez être amené à ignorer le risque d'une vulnérabilité en appliquant votre propre classification des risques. Une vulnérabilité que QRadar Vulnerability Manager a classée avec un score CVSS élevé peut ne pas représenter un risque sérieux en raison de nombreux facteurs d'atténuation. Par exemple, si une vulnérabilité CVSS 9.5 IPv6 est publiée et qu'une entreprise n'a pas d'infrastructure IPV6, le score CVSS élevé n'est pas justifié..

Configuration des scores du risque personnalisé pour des vulnérabilités

IBM QRadar Vulnerability Manager permet d'ajouter en interne un score du risque personnalisé à des vulnérabilités afin de refléter le risque qu'il représente réellement pour votre organisation.

Avant de commencer

Remarque :

Un travail de mise à jour automatique s'exécute la nuit pour mettre à jour toutes les zones relatives aux risques personnalisés. Pour la génération des rapports et les recherches sauvegardées, les modifications apportées aux risques personnalisés ne prennent pas effet immédiatement. Vous pouvez exécuter la mise à jour automatique manuellement pour compléter les informations de risque personnalisé indiquées. Exécutez la mise à jour automatique en cliquant sur l'icône **Mise à jour automatique** dans l'onglet **Admin**.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Rechercher** > **Vulnérabilités**.
3. Pour affecter un score du risque personnalisé à un actif, procédez comme suit :
   a) Sélectionnez une vulnérabilité et cliquez sur **Editer/Trier**.
   b) Sélectionnez un type de risque personnalisé dans la fenêtre **Affectation de risque personnalisé** :
      - `Vide` : aucune modification n'est apportée au risque personnalisé mais une remarque est affectée.
      - `Critique`

- Elevé
- Moyen
- Faible
- Avertissement
- CVSS : La vulnérabilité est associée à un risque personnalisé défini conformément aux règles du score CVSS en cours.
- Annuler l'affectation : La vulnérabilité n'est plus associée à un niveau de risque personnalisé. Utilisez cette option pour supprimer un risque personnalisé existant.

c) Facultatif : Ajoutez une remarque à l'aide de la zone de saisie RTF pour refléter l'affectation de la vulnérabilité. Par exemple, vous pouvez ajouter une remarque pour expliquer pourquoi vous modifiez la classification.

d) Cliquez sur **Sauvegarder**.

e) Lorsqu'un risque personnalisé est créé pour une vulnérabilité, une nouvelle colonne appelée **Risque personnalisé** s'affiche dans l'écran **Recherche de vulnérabilités**.

4. Pour afficher les détails d'un risque personnalisé et la remarque sur l'affectation d'un risque personnalisé, cliquez deux fois sur la vulnérabilité dans l'écran **Recherche de vulnérabilités**.
5. Pour rechercher des vulnérabilités qui n'ont pas encore été triées, procédez comme suit :
   a) Dans le panneau de navigation, cliquez sur **Rechercher** > **Vulnérabilités**.
   b) Cliquez sur **Rechercher** > **Nouvelle recherche**.
   c) Dans la section **Niveau de risque personnalisé**, sélectionnez l'un des paramètres suivants pour la recherche :

Tableau 10. Paramètres de recherche des risques personnalisés

Type de recherche des risques personnalisés	Description
Toutes les vulnérabilités	Renvoie toutes les vulnérabilités, qu'un risque personnalisé soit affecté ou non.
Toutes les vulnérabilités triées	Renvoie toutes les vulnérabilités auxquelles un risque personnalisé a été affecté.
Toutes les vulnérabilités pas encore triées	Renvoie toutes les vulnérabilités auxquelles un risque personnalisé n'a pas été affecté.
Toutes les vulnérabilités avec le niveau de risque personnalisé spécifique	Renvoie les vulnérabilités filtrées en fonction du type de risque personnalisé sélectionné, par exemple Critique, Elevé ou Moyen.

   d) Cliquez sur **Rechercher**.
6. Exportez une liste de vulnérabilités dans l'écran **Liste de vulnérabilités** à des fins d'audit ou de conformité en procédant comme suit :
   a) Dans le panneau de navigation, cliquez sur **Rechercher** > **Vulnérabilités**.
   b) Sélectionnez l'option d'exportation requise :

- **Exporter au format XML**
- **Exporter au format CSV**

Recherche des données de vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités importantes en recherchant vos données de vulnérabilité.

QRadar Vulnerability Manager fournit plusieurs méthodes permettant de rechercher vos données. La recherche peut s'effectuer par réseau, actif, service ouvert ou vulnérabilité.

Les recherches enregistrées par défaut sont une méthode rapide d'identification du risque dans votre organisation. Elles sont affichées dans la zone **Recherches sauvegardées disponibles** sur la page **Recherche du gestionnaire de vulnérabilités**.

Avant de commencer

Vous devez créer un profil d'analyse et analyser les actifs réseau.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Pour charger une recherche enregistrée, procédez comme suit.
   a) Sélectionnez un groupe dans la liste **Groupe**.
   b) Dans la zone **Saisir une recherche sauvegardée**, entrez la recherche enregistrée que vous voulez charger.
   c) Dans la liste **Recherches sauvegardées disponibles**, sélectionnez une recherche enregistrée, puis cliquez sur **Charger**.
   d) Cliquez sur **Rechercher**.
5. Si vous souhaitez créer une autre recherche, exécutez les étapes suivantes dans le panneau **Paramètres de recherche** :
   a) Dans la zone **Première liste**, sélectionnez le paramètre que vous souhaitez utiliser.
   b) Dans la zone **Seconde liste**, sélectionnez un modificateur de recherche. Les modificateurs disponibles sont liés au paramètre de recherche que vous sélectionnez.
   c) Dans la zone **Troisième liste**, entrez ou sélectionnez les informations spécifiques qui sont associées à votre paramètre de recherche.
   d) Cliquez sur **Ajouter un filtre**.

   Par exemple, pour envoyer les vulnérabilités affectées à un utilisateur technique par courrier électronique, sélectionnez **Contact propriétaire technique** et indiquez une adresse électronique configurée dans la page **Affectation de vulnérabilité**.
6. Cliquez sur **Rechercher**.
7. Dans la barre d'outils, cliquez sur **Sauvegarder les critères de recherche**.

   Important : Les rapports des vulnérabilités utilisent les informations de recherche enregistrées. Si vous souhaitez créer un rapport envoyé par courrier électronique à un utilisateur technique, vous devez enregistrer vos critères de recherche.

Concepts associés

Paramètres de recherche de vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez rechercher des données de vulnérabilité et enregistrer les recherches afin de les utiliser ultérieurement.

Recherches rapides de vulnérabilité

Recherchez les vulnérabilités en tapant une chaîne de recherche de texte qui utilise des mots ou des phrases simples.

Dans IBM QRadar Vulnerability Manager, vous pouvez utiliser des recherches rapides pour filtrer les vulnérabilités sur les pages **Vulnérabilités qui me sont affectées** et **Gérer les vulnérabilités**.

Utilisez la liste **Recherches rapides** pour faire une recherche de vulnérabilité préconfigurée.

Utilisez la zone **Filtre rapide** pour créer vos propres filtres de vulnérabilité. Cliquez sur **Enregistrer les critères de recherche** pour ajouter des filtres rapides de vulnérabilité à la liste **Recherches rapides**.

Tableau 11. Instructions de syntaxe de filtre rapide de vulnérabilité

Description	**Exemple**

Inclure tout texte brut que vous pensez trouver dans le titre de la vulnérabilité, la description, la solution, l'inquiétude, le type d'ID de référence ou la valeur d'ID de référence.	`2012-3764`
	`MS203`
	`java`

Pour rechercher uniquement le texte dans le titre de vulnérabilité, ajoutez **:A** à la chaîne de texte de recherche	`PHP:A`
Pour rechercher uniquement le texte dans la description de la vulnérabilité, ajoutez **:B** à la chaîne de texte de recherche	`cross-site scripting:B`
Pour rechercher uniquement le texte dans le type de référence externe de la vulnérabilité, ajoutez **:C** à la chaîne de texte de recherche	`RedHat RHSA:C`
Inclure des caractères génériques. Le terme de recherche ne peut pas commencer par un caractère générique.	`SSLv*`

Grouper les termes avec les opérateurs logiques : **AND**, **OR** et **NOT** (ou **!**). Pour être reconnus comme opérateurs logiques et non comme critères de recherche, les opérateurs doivent être en majuscules.	`PHP AND Traversal`
	`XSS:A OR cross-site scripting:A`
	`!MySQL`
	`NOT MySQL`

Tâches associées

Enregistrement des critères de recherche de vulnérabilité

Paramètres de recherche de vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez rechercher des données de vulnérabilité et enregistrer les recherches afin de les utiliser ultérieurement.

Le tableau ci-après n'est pas une liste exhaustive des paramètres de recherche de vulnérabilités, mais un sous-ensemble des options disponibles.

Sélectionnez l'un des paramètres suivants pour rechercher des données de vulnérabilité et les afficher.

Tableau 12. Paramètres de recherche de vulnérabilités	
Option	**Description**
Complexité d'accès	Niveau de complexité de l'attaque qui est requis pour exploiter une vulnérabilité.
Vecteur d'accès	Emplacement réseau à partir duquel une vulnérabilité peut être exploitée.
Recherche sauvegardée d'actif	Hôte, adresse IP ou plage des adresses IP associés à une recherche d'actifs enregistrée. Pour plus d'informations sur l'enregistrement des recherches d'actifs, voir le *Guide d'utilisation* de votre produit.
Actifs avec service ouvert	Actifs associés à des services ouverts spécifiques. Par exemple, HTTP, FTP et SMTP.
Authentification	Nombre de fois qu'un attaquant doit s'authentifier sur une cible pour exploiter une vulnérabilité.
Impact sur la disponibilité	Niveau de compromission de la disponibilité de ressource en cas d'exploitation d'une vulnérabilité.
Impact sur la confidentialité	Niveau d'information confidentielle pouvant être obtenu en cas d'exploitation d'une vulnérabilité.
Jours depuis la détection de l'actif	Nombre de jours qui se sont écoulés depuis la découverte de l'actif présentant la vulnérabilité sur votre réseau. Les actifs peuvent être reconnus soit par une analyse active ou passivement ou en utilisant l'analyse du journal ou de flux.
Jours depuis le trafic de service de vulnérabilité associé	Vulnérabilités sur les actifs associés au trafic de la couche 7 vers ou depuis un actif, en fonction du nombre de jours écoulés depuis la détection du trafic.
Domaine	Si vous avez configuré IBM QRadar pour les systèmes multi-domaines, utilisez cette option pour spécifier le domaine dans lequel vous souhaitez rechercher des vulnérabilités.
Par service ouvert	Recherche des vulnérabilités associées à des services ouverts particuliers comme HTTP, FTP et SMTP.
Référence externe de type	Vulnérabilités associées à un fixlet IBM BigFix. Ce paramètre vous permet d'afficher uniquement les vulnérabilités sans correctif disponible.
Impact	Impact potentiel pour votre organisation. Par exemple : la perte du contrôle d'accès, le temps d'indisponibilité et la perte de réputation.
Inclure les premiers avertissements	Inclut les vulnérabilités nouvellement publiées qui sont détectées sur votre réseau et ne figurent dans aucun résultat d'analyse.
Inclure les exceptions de vulnérabilité	Vulnérabilités avec application d'une règle d'exception.

Tableau 12. Paramètres de recherche de vulnérabilités (suite)

Option	Description
Impact sur l'intégrité	Niveau de compromission de l'intégrité du système en cas d'exploitation d'une vulnérabilité.
Inclure uniquement les actifs avec risque	Vulnérabilités qui réussissent ou échouent aux règles du risque spécifiques définies et contrôlées dans IBM QRadar Risk Manager. **Remarque :** Vous devez surveiller au moins une question dans la page **Moniteur de politique d'administration** sur l'onglet **Risques** pour utiliser ce paramètre de recherche.
Inclure uniquement les actifs avec risque transmis	Vulnérabilités qui réussissent aux règles du risque spécifiques définies et contrôlées dans QRadar Risk Manager.
Inclure uniquement les premiers avertissements	Inclut uniquement les vulnérabilités nouvellement publiées qui sont détectées sur votre réseau et ne figurent dans aucun résultat d'analyse.
Inclure uniquement les exceptions de vulnérabilité	Inclut uniquement les vulnérabilités ayant une règle d'exception appliquée dans votre recherche.
En retard (jours)	Recherche de vulnérabilités ayant un retard de résolution d'un nombre de jours spécifié.
Statut du correctif	Filtrage des vulnérabilités par état des correctifs. Pour plus d'informations, voir «Identification de l'état de correctif des vulnérabilités», à la page 99.
Gravité PCI	Recherche des vulnérabilités par niveau de gravité PCI (élevé, moyen ou faible) assigné par le service de conformité PCI. Les vulnérabilités auxquelles a été attribué un niveau de gravité PCI élevé ou moyen échouent le test de conformité PCI.
Recherche rapide	Vous pouvez rechercher un titre de vulnérabilités, une description, une solution et un ID de référence externe. Dans la zone **Recherche rapide**, vous pouvez utiliser les opérateurs AND, OR, NOT et les crochets.
Risque	Recherche des vulnérabilités par niveau de risque (haut, moyen, faible, avertissement).
Non affecté	Recherche des vulnérabilités sans utilisateur assigné pour les corriger.
Référence externe de vulnérabilité	Vulnérabilités qui reposent sur une liste importée d'ID de vulnérabilités, par exemple l'ID CVE. Pour plus d'informations sur les jeux de référence, voir le *Guide d'administration* de votre produit.
Correctif virtuel fourni par le fournisseur pour la vulnérabilité	Vulnérabilités qui peuvent être corrigées par un système de prévention des intrusions.

Tableau 12. Paramètres de recherche de vulnérabilités (suite)	
Option	**Description**
Etat de vulnérabilité	Etat de la vulnérabilité depuis la dernière analyse de votre réseau ou de vos actifs réseau spécifiques. Par exemple, lorsque vous effectuez une analyse des actifs, les vulnérabilités détectées sont nouvelles, préexistantes, corrigées ou existantes.
Vulnérabilités à risque	Filtrage des vulnérabilités par résultats de la politique de risque. Vous devez surveiller au moins une question dans la page **Moniteur de politique d'administration** sur l'onglet **Risques** pour utiliser ce paramètre de recherche.

Enregistrement des critères de recherche de vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez enregistrer vos critères de recherche de vulnérabilité pour une utilisation ultérieure.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche** et effectuez la recherche des données.
4. Dans la barre d'outils, cliquez sur **Sauvegarder les critères de recherche**.
5. Dans la fenêtre **Sauvegarder les critères de recherche**, entrez un nom reconnaissable pour votre recherche enregistrée.
6. Pour inclure votre recherche enregistrée dans la liste **Recherches rapides** sur la barre d'outils, cliquez sur **Inclure dans mes recherches rapides**.
7. Pour partager vos critères de la recherche enregistrée avec tous les utilisateurs QRadar, cliquez sur **Partager avec tout le monde**.
8. Pour placer votre recherche enregistrée dans un groupe, cliquez sur un groupe, ou cliquez sur **Gérer les groupes** pour créer un groupe.

   Pour plus d'informations sur la gestion des groupes de recherche, voir le *Guide d'administration* de votre produit.
9. Si vous souhaitez afficher les résultats de votre recherche enregistrée lorsque vous cliquez sur l'une des pages **Gérer les vulnérabilités** dans le panneau de navigation, cliquez sur **Définir comme valeur par défaut**.
10. Cliquez sur **OK**.

Suppression de critères de recherche de vulnérabilités enregistrée

Dans IBM QRadar Vulnerability Manager, vous pouvez supprimer vos critères de recherche enregistrée des vulnérabilités.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez **Gérer les vulnérabilités** > **Par réseau**
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.

4. Sur la page **Recherche du gestionnaire de vulnérabilités**, dans la liste **Recherches sauvegardées disponibles**, sélectionnez la recherche enregistrée que vous souhaitez supprimer.
5. Cliquez sur **Supprimer**.
6. Cliquez sur **OK**.

Instances de vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez afficher les vulnérabilités dans chaque actifs analysé de votre réseau. Chaque vulnérabilité doit être répertoriée plusieurs fois, car la vulnérabilité existe sur plusieurs de vos actifs.

Si vous configurez des programmes d'analyse VA (Vulnerability Assessment) tiers dans l'onglet QRadar **Admin**, les vulnérabilités qui sont détectées sont automatiquement affichées sur la page **Par instances des vulnérabilités**.

Pour plus d'informations sur les programmes d'analyse VA, voir le *Guide d'administration* de votre produit.

La page **Par instances des vulnérabilités** fournit les informations suivantes :

- Vue des différentes vulnérabilités détectées par analyse des actifs réseau.
- Risque que représente chaque vulnérabilité pour le secteur PCI (Payment Card Industry).
- Risque que représente une vulnérabilité pour votre organisation. Cliquez sur la colonne **Score de risque** pour identifier les vulnérabilités à haut risque.
- Nom ou adresse électronique de l'utilisateur affecté à la résolution de la vulnérabilité.
- Le nombre de jours octroyé pour la résolution de la vulnérabilité.

Concepts associés

Détails du score du risque

Vulnérabilités des réseaux

Dans IBM QRadar Vulnerability Manager, vous pouvez consulter les données relatives aux vulnérabilités regroupées par réseau.

La page **Par réseau** contient les informations suivantes :

- Un score de risque cumulé basé sur les vulnérabilités détectées pour chacun de vos réseaux.
- Le nombre d'actifs, de vulnérabilités et de services ouverts pour chaque réseau.
- Le nombre de vulnérabilités des actifs affectées à un utilisateur technique dont la résolution est en retard.

Vulnérabilités des actifs

Dans IBM QRadar Vulnerability Manager, vous pouvez afficher un récapitulatif des données relatives aux vulnérabilités regroupées par actif analysé.

Vous pouvez utiliser la page **Par actif** pour hiérarchiser les tâches de résolution pour les actifs de votre société qui présent le risque le plus élevé.

La page **Par actif** contient les informations suivantes :

- Un score de risque cumulé basé sur les vulnérabilités détectées pour chacun de vos actifs.

  Cliquez dans la colonne **Score de risque** pour trier les actifs en fonction de leur risque.
- Le nombre de vulnérabilités des actifs affectées à un utilisateur technique dont la résolution est en retard.

Vulnérabilités des services ouverts

Dans IBM QRadar Vulnerability Manager, vous pouvez afficher des données de vulnérabilité qui sont regroupées au niveau du service ouvert.

La page **Par service ouvert** affiche un score de risque cumulé et un nombre de vulnérabilités pour chaque service dans tout le réseau.

Examen détaillé de l'historique d'une vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez afficher des informations utiles sur l'historique d'une vulnérabilité.

Par exemple, vous pouvez enquêter sur la façon dont le score du risque d'une vulnérabilité a été calculé. Vous pouvez également consulter des informations sur le moment où une vulnérabilité a été détectée pour la première fois et sur l'analyse qui a permis de la détecter.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Recherchez vos données de vulnérabilité.
4. Cliquez sur la vulnérabilité que vous voulez examiner.
5. Dans la barre d'outils, sélectionnez **Actions** > **Historique**.

Tâches associées

Recherche des données de vulnérabilité

Réduction du nombre de faux positifs de vulnérabilité

Dans IBM QRadar Vulnerability Manager, vous pouvez créer automatiquement des règles d'exception pour les vulnérabilités qui sont associées à un type de serveur spécifique.

Lorsque vous configurez des types de serveur, QRadar Vulnerability Manager crée des règles d'exception et diminue automatiquement les vulnérabilités qui sont renvoyées par la recherche de vos données.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, sélectionnez **Reconnaissance des serveurs**.
3. Pour créer automatiquement des règles d'exception de faux positifs de vulnérabilité sur des types de serveur spécifiques, dans la liste **Type de serveur**, sélectionnez l'une des options suivantes :
   - FTP Servers
   - DNS Servers
   - Mail Servers
   - Web Servers

   L'actualisation de la zone **Ports** peut prendre quelques minutes.
4. Dans la liste **Réseau**, sélectionnez le réseau pour vos serveurs.
5. Cliquez sur **Reconnaître les serveurs**.
6. Dans le panneau **Serveurs correspondants**, sélectionnez les serveurs sur lesquels les règles d'exception de vulnérabilité ont été créées.
7. Cliquez sur **Approuver les serveurs sélectionnés**.

Résultats

Suivant le type de serveur sélectionné, les vulnérabilités suivantes sont automatiquement définies comme règles d'exceptions de faux positifs :

Tableau 13. Vulnérabilités de type de serveur

Type de serveur	**Vulnérabilité**
Serveurs FTP	**Serveur FTP présent**
Serveurs DNS	**Serveur DNS en cours d'exécution**
Serveurs de messagerie	**Serveur SMTP détecté**
Serveurs Web	**Service Web en cours d'exécution**

Examen des actifs et des vulnérabilités à haut risque

Dans IBM QRadar Vulnerability Manager, vous pouvez examiner les vulnérabilités à haut risque susceptibles d'être exploitées à des fins malveillantes.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Sur la page **Par instances des vulnérabilités**, cliquez sur l'en-tête de colonne **Score de risque** pour trier les vulnérabilités par score du risque.
4. Pour examiner les métriques CVSS utilisées pour dériver le score de risque, survolez avec le pointeur de la souris la zone **Score de risque**.
5. Identifiez la vulnérabilité ayant le score le plus élevé, puis cliquez sur le lien **Vulnérabilité**.
6. Dans la fenêtre **Détails de la vulnérabilité**, examinez la vulnérabilité :
   a) Pour afficher le site Web IBM Security Systems, cliquez sur le lien **X-Force**.
   b) Pour afficher le site Web National Vulnerability Database, cliquez sur le lien **CVE**.

      Le site Web IBM Security Systems et la base de données NVD (National Vulnerability Database) fournissent des informations de résolution et des détails sur la manière dont une vulnérabilité peut nuire à votre organisation.
   c) Pour ouvrir la fenêtre **Correctif** de la vulnérabilité, cliquez sur le lien **Détails du plug-in**. Utilisez les onglets pour rechercher les recommandations Oval Definition, Windows Knowledge Base ou UNIX sur la vulnérabilité. Cette fonction fournit des informations sur la manière dont QRadar Vulnerability Manager recherche des données de vulnérabilité lors d'une analyse de correctif. Vous pouvez l'utiliser pour identifier la raison pour laquelle une vulnérabilité est apparue ou non sur un actif.
   d) La zone de texte **Solution** contient des informations détaillées sur la façon de remédier à une vulnérabilité.

Concepts associés

Détails du score du risque

Hiérarchisation des vulnérabilités à haut risque par l'application de règles du risque

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

Lorsque vous appliquez une politique d'administration de risque, le score de risque d'une vulnérabilité est ajusté, ce qui permet aux administrateurs d'identifier plus précisément les vulnérabilités qui exigent une attention immédiate.

Dans l'exemple ci-dessous, le score du risque est automatiquement augmenté par un facteur de pourcentage pour toutes les vulnérabilités qui restent actives sur votre réseau après 40 jours.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
4. Dans le panneau **Paramètres de recherche**, configurez les filtres suivants :
   a) **Risque élevé**
   b) **Jours depuis la découverte de vulnérabilités supérieur ou égal à 40**
5. Cliquez sur **Rechercher**, puis dans la barre d'outils, cliquez sur **Sauvegarder les critères de recherche**.

   Entrez un nom de recherche enregistrée qui est identifiable dans QRadar Risk Manager.
6. Cliquez sur l'onglet **Risques**.
7. Dans le panneau de navigation, cliquez sur **Moniteur de politique d'administration**.
8. Dans la barre d'outils, cliquez sur **Actions** > **Nouveau**.
9. Dans la zone **What do you want to name this question**, entrez un nom.
10. Dans la zone **Which tests do you want to include in your question**, cliquez sur **are susceptible to vulnerabilities contained in vulnerability saved searches**.
11. Dans **Find Assets that**, cliquez sur la valeur soulignée dans la zone **are susceptible to vulnerabilities contained in vulnerability saved searches**.
12. Identifiez votre recherche enregistrée de vulnérabilités à haut risque QRadar Vulnerability Manager, puis cliquez sur **Ajouter** et sur **OK**.
13. Cliquez sur **Sauvegarder la question**.
14. Dans le panneau **Questions**, sélectionnez votre question dans la liste puis dans la barre d'outils, cliquez sur **Moniteur**.

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

Que faire ensuite

Sous l'onglet **Vulnérabilités**, vous pouvez rechercher vos vulnérabilités à haut risque et les classer par ordre de priorité.

Concepts associés

Intégration à QRadar Vulnerability Manager

Tâches associées

Enregistrement des critères de recherche de vulnérabilité

Configuration de couleurs d'affichage personnalisées pour les scores de risque

Configurez un code couleur personnalisé pour les scores de risque IBM QRadar Vulnerability Manager afin d'afficher ces scores de risque codées en couleur dans les interfaces de QRadar Vulnerability Manager.

Procédure

1. Dans IBM QRadar, **Vulnérabilités** > **Affectation de vulnérabilité** > **Préférences de risques**.
2. Dans la colonne **Est supérieur ou égal à**, entrez la valeur de score du risque minimum pour Elevé, Moyen, Faible et Avertissement.
3. Dans la colonne **Couleur**, sélectionnez ou définissez une couleur pour représenter les scores de risque Elevé, Moyen, Faible et Avertissement.

   Remarque : Les couleurs que vous appliquez ne changent pas les couleurs de risque par défaut dans la page **Résultats d'analyse**. La colonne **Score** de la page **Résultats d'analyse** et la page des **détails d'actifs des résultats d'analyse** utilisent les valeurs et couleurs par défaut, vous ne pouvez pas les modifier.

Identification des vulnérabilités ayant un correctif BigFix

Dans IBM QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités pour lesquelles un correctif est disponible.

Après avoir identifié les vulnérabilités pour lesquelles un correctif est disponible, vous pouvez obtenir des informations détaillées sur le correctif dans la fenêtre **Détails de la vulnérabilité**.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Dans le panneau **Paramètres de recherche**, configurez les options suivantes :
   a) Dans la zone **Première liste**, sélectionnez **Référence externe de type**.
   b) Dans la zone **Seconde liste**, sélectionnez **Est égal à**.
   c) Dans la zone **Troisième liste**, sélectionnez **Correctif IBM BigFix**.
   d) Cliquez sur **Ajouter un filtre**.
   e) Cliquez sur **Rechercher**.

      La page **Par instances des vulnérabilités** affiche les vulnérabilités pour lesquelles un correctif est disponible.
5. Classez les vulnérabilités en fonction de leur importance en cliquant sur l'en-tête de colonne **Score de risque**.
6. Pour avoir des détails sur le correctif d'une vulnérabilité, cliquez sur un lien de vulnérabilité dans la colonne **Vulnérabilité**.
7. Dans la fenêtre **Détails de la vulnérabilité**, faites défiler jusqu'au bas de la fenêtre pour afficher des informations sur le correctif de la vulnérabilité.

   ID site et **ID Fixlet** sont des identificateurs uniques que vous pouvez utiliser pour appliquer les correctifs de vulnérabilité à l'aide d'IBM BigFix.

La colonne **Base** indique une référence unique qui permet d'accéder à des informations complémentaires dans une base de connaissances.

Identification de l'état de correctif des vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez identifier l'état de correctif de vos vulnérabilités.

En filtrant les vulnérabilités corrigées, vous pouvez hiérarchiser leur processus de résolution en axant vos efforts sur les vulnérabilités qui sont les plus critiques dans votre organisation.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Gérer les vulnérabilités**.
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Dans la zone **Première liste** du panneau **Paramètres de recherche**, sélectionnez **Etat de correctif**.
5. Dans la zone **Seconde liste**, sélectionnez un modificateur de recherche.
6. Pour filtrer vos vulnérabilités en fonction de leur état de correctif, sélectionnez l'une des options suivantes dans la troisième liste :

Option	Description
Téléchargements en attente	Sélectionnez cette option pour afficher les vulnérabilités dont la correction est planifiée.
Redémarrage en attente	Sélectionnez cette option pour afficher les vulnérabilités qui seront corrigées après le redémarrage de l'actif analysé.
Corrigé	Sélectionnez cette option pour afficher les vulnérabilités qui sont corrigées par IBM BigFix.

7. Cliquez sur **Ajouter un filtre**.
8. Cliquez sur **Rechercher**.

Concepts associés

Intégration à IBM BigFix

Suppression des données de vulnérabilité non souhaitées

Utilisez la fonctionnalité de nettoyage de vulnérabilité QRadar Vulnerability Manager afin de supprimer les données de vulnérabilité périmées à partir du modèle d'actif.

Pourquoi et quand exécuter cette tâche

L'un des scénarios suivants peut vous laisser des données de vulnérabilité non souhaitées :

- Changement de type de scanner
- Actifs déclassés
- Changement d'adresse IP
- Examens inexacts ou de test

Important : Lorsque vous avez supprimé les données de vulnérabilité pour un actif ou un type de scanner, vous ne pouvez plus les récupérer.

Procédure

Pour supprimer des données de vulnérabilité indésirables, vous disposez de deux options :

- Utilisez l'option **Actions** > **Nettoyer les vulnérabilités (toutes)** dans la page **Actifs** pour supprimer toutes les données de vulnérabilité pour un type de scanner sélectionné.
- Utilisez l'option **Actions** > **Nettoyer les vulnérabilités (toutes)** dans la page **Détails d'actif** pour supprimer toutes les données de vulnérabilité pour un actif donné sur un type de scanner sélectionné.

Configuration des périodes de conservation de données de vulnérabilité

Vous pouvez régler le délai de conservation des données sur les tendances de la vulnérabilité et les résultats d'analyse dans la fenêtre **Configuration du profileur d'actif**.

Pourquoi et quand exécuter cette tâche

Utilisez les règles de configuration dans la section **Conservation de la vulnérabilité QVM** de la fenêtre **Configuration du profileur d'actif** pour définir le temps de conservation par IBM QRadar Vulnerability Manager des données sur les tendances de la vulnérabilité et des résultats de l'analyse.

Procédure

1. Cliquez sur **Admin** > **Configuration du profileur d'actif**.
2. Dans la section **Conservation de la vulnérabilité QVM** de la fenêtre **Configuration du profileur d'actif**, saisissez une valeur dans les zones suivantes :

Règle	Description	Valeur par défaut
Données des rapports de tendance de la vulnérabilité (en jours)	Indique combien de jours QRadar Vulnerability Manager conserve des données sur les tendances de la vulnérabilité pour une utilisation dans les rapports quotidiens des vulnérabilités.	14 jours
Données des rapports de tendance de la vulnérabilité (en semaines)	Indique combien de semaines QRadar Vulnerability Manager conserve des données sur les tendances de la vulnérabilité pour une utilisation dans les rapports hebdomadaires des vulnérabilités.	14 semaines
Données des rapports de tendance de la vulnérabilité (en mois)	Indique combien de mois QRadar Vulnerability Manager conserve les données sur les tendances de la vulnérabilité pour l'utilisation dans les rapports mensuels des vulnérabilités.	14 mois
Purger les résultats de l'analyse après la période (en jours)	Utilisez cette règle avec **Purger les résultats de l'analyse après la période (en cycles d'exécution)** pour définir les limites de conservation des données d'analyse des résultats. Définit le nombre de jours pendant lesquels QRadar Vulnerability Manager conserve les données après l'application de la règle de limitation **Purger les résultats de l'analyse après la période (en cycles d'exécution)**.	30 jours

Règle	Description	Valeur par défaut
Purger les résultats de l'analyse après la période (en cycles d'exécution)	Utilisez cette règle avec **Purger les résultats de l'analyse après la période (en jours)** pour définir les limites de rétention des données de résultats d'analyse. Définit le nombre de versions de données de résultats d'analyse retenues par QRadar Vulnerability Manager. Cette règle a préséance sur la valeur que vous définissez dans **Purger les résultats de l'analyse après la période (en jours)**. Pour les valeurs par défaut pour les règles **Purger les résultats de l'analyse après la période (en jours)** et **Purger les résultats de l'analyse après la période (en cycles d'exécution)** : • QRadar Vulnerability Manager conserve les données des résultats de l'analyse pour les trois cycles d'exécution les plus récents. Il conserve également toutes les autres versions de résultats pour les analyses que vous exécutez dans la limite de 30 jours. • Si l'un des trois cycles d'exécution les plus récents ont eu lieu au-delà de la limite de 30 jours,QRadar Vulnerability Manager conserve les données de résultats de l'analyse de ces cycles d'exécution.	3 cycles d'exécution

3. Cliquez sur **Sauvegarder**.

Chapitre 12. Résolution des vulnérabilités

Dans QRadar Vulnerability Manager, vous pouvez affecter les vulnérabilités à un utilisateur technique pour qu'elles soient résolues.

Vous pouvez affecter des vulnérabilités à votre utilisateur technique en utilisant deux méthodes.

- Affectez des vulnérabilités individuelles à un utilisateur technique pour qu'elles soient résolues.
- Affectez un utilisateur technique comme propriétaire des groupes d'actifs.

Remarque : Un ticket fermé puis ré-ouvert manuellement a le statut **Ré-ouvert** et ne peut pas être fermé par le processus de résolution automatique. Un ticket ré-ouvert manuellement doit également être fermé manuellement. Si un profil d'analyse détecte une vulnérabilité qui a été fermée, le statut du ticket devient alors **Ouvert**. Ces tickets peuvent être fermés par le processus de résolution automatique une fois que la vulnérabilité n'est plus détectée dans le profil d'analyse.

Tâches associées

Configuration des délais de résolution pour les vulnérabilités dans les actifs affectés

Affectation des vulnérabilités individuelles à un utilisateur technique pour qu'elles soient résolues

Dans IBM QRadar Vulnerability Manager, vous pouvez affecter des vulnérabilités individuelles à un utilisateur QRadar pour qu'elles soient résolues.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez **Gérer les vulnérabilités**.
3. Recherchez vos données de vulnérabilité.
4. Sélectionnez la vulnérabilité que vous souhaitez affecter à la résolution.
5. Dans la barre d'outils, cliquez sur **Actions** > **Affecter/Modifier**.
6. Sélectionnez un utilisateur technique dans la liste **Utilisateurs affectés**.

   Vous affectez les utilisateurs techniques dans la page **Affectation de vulnérabilité**. Pour plus d'informations, voir «Affectation d'un utilisateur technique comme propriétaire des groupes d'actifs», à la page 103.
7. Dans la liste **Date d'échéance**, sélectionnez une date butoir à laquelle la vulnérabilité doit être résolue.

   Si vous ne sélectionnez pas de date, la **Date d'échéance** est définie sur la date en cours.
8. Dans la zone **Notes**, entrez des informations pertinentes expliquant la raison de l'affectation de la vulnérabilité.
9. Cliquez sur **Sauvegarder**.

Affectation d'un utilisateur technique comme propriétaire des groupes d'actifs

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer des groupes d'actifs et affecter automatiquement leurs vulnérabilités à des utilisateurs techniques.

Une fois que vous avez affecté un utilisateur technique et analysé les actifs, toutes les vulnérabilités des actifs sont affectées à l'utilisateur technique pour être résolues.

© Copyright IBM Corp. 2012, 2020

Le délai de résolution des vulnérabilités peut être configuré à l'aide de l'option **Heures de résolution** en fonction de leur risque ou de leur gravité.

Si vous ajoutez un nouvel actif à votre réseau et qu'il appartient au groupe d'actifs d'un utilisateur technique, les vulnérabilités de l'actif sont affectées automatiquement à l'utilisateur technique.

Vous pouvez envoyer automatiquement les rapports par courrier électronique aux utilisateurs techniques en indiquant les détails des vulnérabilités qu'ils sont chargés de résoudre.

Les options **Heures de résolution**, **Planifier** et **Préférences de risques** sont activées uniquement pour les utilisateurs administratifs et les utilisateurs non-administrateurs qui n'ont pas de domaine associé.

Avant de commencer

Si vous souhaitez configurer un groupe d'actifs identifiés par une recherche d'actifs enregistrée, vous devez recherchez vos actifs et enregistrer les résultats.

Pour plus d'informations sur la recherche des actifs et l'enregistrement des résultats, consultez le *guide d'utilisation* du produit.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Affectation de vulnérabilité**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Entrez un nom, une adresse électronique et une plage CIDR.

   Pour affecter automatiquement un utilisateur technique dans la fenêtre **Nouveau propriétaire d'actif**, les seules zones obligatoires sont **Nom**, **E-mail** et **CIDR**. Si des environnements multi-domaine sont activés, sélectionnez une association de domaine pour ce propriétaire d'actif en particulier.
5. Si vous avez configuré IBM QRadar pour plusieurs domaines, sélectionnez le domaine concerné dans la liste **Domaines**.
6. Pour filtrer la liste des actifs dans la plage CIDR par nom d'actif, entrez une chaîne de texte dans la zone **Filtre de nom d'actif**.
7. Pour filtrer la liste d'actifs dans la plage CIDR par système d'exploitation, entrez une chaîne de texte dans la zone **Filtre de système d'exploitation**.
8. Pour affecter l'utilisateur technique aux actifs qui sont associés à une recherche d'actif enregistrée, cliquez sur **Recherche d'actif**. L'option **Recherche d'actif** est désactivée si des domaines ont été configurés dans la page **Gestion de domaine**.
9. Cliquez sur **Sauvegarder**.
10. Dans la barre d'outils, cliquez sur **Heures de résolution**.

    Vous pouvez configurer le délai de résolution pour chaque type de vulnérabilité en fonction de leur risque et de leur gravité.

    Par exemple, vous pouvez avoir besoin que les vulnérabilités représentant un risque élevé soient résolues en 5 jours.
11. Dans la barre d'outils, cliquez sur l'option permettant de **planifier**.

    Par défaut, le contact d'utilisateur technique pour vos actifs est mis à jour toutes les 24 heures.

    Les nouveaux actifs ajoutés à votre déploiement et qui appartiennent à la plage CIDR que vous avez indiquée sont automatiquement mis à jour avec le contact technique que vous avez spécifié.

    Important : La planification concerne les associations définies entre les utilisateurs techniques et les groupes d'actifs.
12. Cliquez sur **Mettre à jour maintenant**, afin de définir immédiatement le propriétaire de vos actifs.

    En fonction de la taille de votre déploiement, la mise à jour de vos actifs peut prendre un certain temps.

13. Cliquez sur **Sauvegarder**.

    Les vulnérabilités déjà affectées à un utilisateur technique pour la résolution sont mises à jour avec le nouvel utilisateur technique.
14. Si des vulnérabilités n'avaient pas été affectés précédemment à un utilisateur technique, vous devez analyser les actifs que vous avez affectés à l'utilisateur technique.

    Important : L'analyse des actifs permet de s'assurer que les vulnérabilités affectées à un utilisateur technique existent dans l'actif.

Configuration des délais de résolution pour les vulnérabilités dans les actifs affectés

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer les délais de résolution des différents types de vulnérabilités.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Affectation de vulnérabilité**.
3. Sélectionnez une affectation dans la liste **Propriétaires de l'actif**.
4. Dans la barre d'outils, cliquez sur **Heures de résolution**.
5. Mettez à jour les délais de résolution des vulnérabilités en fonction de leur risque et de leur gravité.
6. Cliquez sur **Sauvegarder**.

Chapitre 13. Rapports de vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez générer ou modifier un rapport existant, ou utiliser l'assistant de rapport pour créer, planifier et distribuer un nouveau rapport.

QRadar Vulnerability Manager contient plusieurs rapports par défaut.

L'assistant de rapport fournit un guide par étape sur la manière de concevoir, de planifier et de générer des rapports.

Pour plus d'informations, voir *IBM QRadar - Guide d'utilisation*.

Envoi d'un courrier électronique aux utilisateurs techniques avec les vulnérabilités à résoudre qui leurs sont affectées

Lorsque vous affectez des vulnérabilités à un utilisateur technique pour qu'elles soient résolues, vous pouvez générer un rapport qui est envoyé à l'utilisateur technique.

Le courrier électronique contient les informations concernant les vulnérabilités que l'utilisateur technique doit résoudre.

Génération de rapports de conformité PCI

Vous pouvez générer un rapport de conformité pour vos actifs PCI.

Le rapport de conformité démontre que vous avez pris toutes les précautions de sécurité nécessaire à la protection de vos actifs critiques.

Exécution d'un rapport QRadar Vulnerability Manager par défaut

Dans IBM QRadar Vulnerability Manager, vous pouvez exécuter un rapport de gestion des vulnérabilités par défaut.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Dans la liste des rapports, cliquez sur le rapport que vous souhaitez exécuter.

   Par exemple, vous pouvez afficher un rapport présentant vos vulnérabilités au cours des sept derniers jours.
3. Dans la barre d'outils, sélectionnez **Actions** > **Exécuter le rapport**, puis cliquez sur **OK**.
4. Pour afficher le rapport final au format PDF, cliquez sur l'icône dans la colonne **Formats**.

Envoi par courrier électronique aux utilisateurs techniques des rapports de vulnérabilités qui leurs sont affectés

Dans IBM QRadar Vulnerability Manager, vous pouvez envoyer un rapport des vulnérabilités affectés au contact technique pour chaque actif.

Un rapport envoyé par courrier électronique rappel aux administrateurs les vulnérabilités qui leur sont affectées et doivent être résolues. Les rapports peuvent être programmés tous les mois, toutes les semaines, tous les jours ou toutes les heures.

Avant de commencer

Vous devez exécuter les tâches suivantes :

© Copyright IBM Corp. 2012, 2020

1. Affectez un utilisateur technique comme propriétaire des groupes d'actifs. Pour plus d'informations, voir «Affectation d'un utilisateur technique comme propriétaire des groupes d'actifs», à la page 103
2. Analysez les actifs auxquels vous avez affecté le propriétaire technique.
3. Créez et enregistrez une recherche de vulnérabilités qui utilise le paramètre **Contact propriétaire technique** comme entrée. Pour plus d'informations, voir «Recherche des données de vulnérabilité», à la page 89

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Dans la barre d'outils, sélectionnez **Actions** > **Créer**.
3. Cliquez sur **Hebdomadaire**, puis sur **Suivant**.
4. Cliquez sur la présentation de rapport qui s'affiche dans le coin supérieur gauche de l'assistant de création de rapports, puis cliquez sur **Suivant**.
5. Dans la zone **Titre du rapport**, entrez un titre de rapport.
6. Dans la liste **Type de graphique**, sélectionnez **Vulnérabilités des actifs**, puis dans la zone **Titre du graphique**, entrez un titre pour le graphique.
7. Si un contact technique est responsable de plus de cinq actifs et que vous souhaitez envoyer par e-mail toutes les informations d'actif, augmentez la valeur dans la zone **Limiter les actifs aux principaux**.

   A faire : A l'aide de l'onglet **Actifs**, vous devez vous assurer que le même propriétaire de contact technique est affecté à chaque actif dont il est responsable.
8. Dans la zone **Type de graphique**, sélectionnez **Table d'agrégation**.

   Si vous sélectionnez une valeur autre que **Table d'agrégation**, le rapport ne génère pas de sous-rapport de vulnérabilité.
9. Dans le panneau **Contenu du graphique**, cliquez sur **Recherche à utiliser**, sélectionnez ensuite votre recherche enregistrée des vulnérabilités pour les contacts techniques, puis cliquez sur **Sauvegarder les détails du conteneur**.
10. Cliquez sur **Suivant**, puis sélectionnez le type de sortie de votre rapport.
11. Dans la section de distribution de rapports de l'assistant de rapport, cliquez sur **Rapports multiples**.
12. Cliquez sur **Tous les propriétaires de l'actif**.
13. Cliquez sur **Charger les propriétaires d'actif** pour afficher une liste des détails de contact de tous les utilisateurs techniques.

    Vous pouvez supprimer les utilisateurs techniques auxquels vous ne souhaitez pas envoyer de liste des vulnérabilités affectées par courrier électronique.
14. Dans la liste des rapports, sélectionnez le rapport que vous avez créé puis dans la barre d'outils, sélectionnez **Actions** > **Exécuter le rapport**.

Tâches associées

Affectation d'un utilisateur technique comme propriétaire des groupes d'actifs

Recherche des données de vulnérabilité

Génération de rapports de conformité PCI

Dans IBM QRadar Vulnerability Manager, vous pouvez générer un rapport de conformité pour vos actifs PCI. Par exemple, générez un rapport pour les actifs qui stockent les informations de carte de crédit ou d'autres informations financières sensibles.

Le rapport de conformité démontre que vous avez pris les précautions de sécurité nécessaires à la protection de vos actifs.

Procédure

1. Exécutez une analyse PCI pour les actifs de votre réseau qui exécutent ou traitent des informations PCI.

   Pour plus d'informations, voir «Création d'un profil d'analyse», à la page 39.
2. Mettez les plans de conformité et les déclarations logicielles à jour.

   Votre plan de conformité et vos déclarations logicielles s'affichent dans la section des remarques spéciales du récapitulatif.

   Pour plus d'informations, consultez les normes de sécurité PCI pour les fournisseurs de logiciels approuvés.
3. Créez et exécutez un rapport de conformité PCI pour les actifs analysés.

Tâches associées

Création d'un profil d'analyse

Mise à jour des plans de conformité des actifs et des déclarations logicielles

Dans IBM QRadar Vulnerability Manager, si vous souhaitez générer un rapport de conformité PCI pour vos actifs, vous devez remplir vos attestations pour chaque actif.

Votre attestation de conformité est affichée dans votre rapport de conformité PCI.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, cliquez sur **Profils d'actifs**.
3. Dans la page **Actifs**, sélectionnez l'actif pour lequel vous souhaitez fournir une attestation.
4. Dans la barre d'outils, cliquez sur **Modifier un actif**.
5. Dans la fenêtre **Editer le profil d'actif**, cliquez dans le volet **CVSS, poids et conformité**.
6. Renseignez les zones suivantes. Utilisez l'infobulle si vous avez besoin d'aide :
   - Plan de conformité
   - Remarques sur la conformité
   - Déclaration des remarques sur la conformité
   - Description des remarques sur la conformité
   - Motif pour lequel la conformité est en dehors du périmètre
7. Cliquez sur **Sauvegarder**.

Création d'un rapport de conformité PCI

Dans IBM QRadar Vulnerability Manager, vous pouvez créer et exécuter un rapport de conformité PCI.

Le rapport de conformité PCI démontre que les actifs impliqués dans les activités PCI sont conformes aux consignes de sécurité visant à empêcher une attaque extérieure.

Avant de commencer

Veillez à exécutez une analyse de conformité PCI.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Dans la barre d'outils, sélectionnez **Actions** > **Créer**.
3. Cliquez sur **Hebdomadaire**, puis sur **Suivant**.
4. Cliquez sur la présentation de rapport qui s'affiche dans le coin supérieur gauche de l'assistant de création de rapports, puis cliquez sur **Suivant**.

5. Dans la zone **Titre du rapport**, entrez un titre de rapport.
6. Dans la liste **Type de graphique**, sélectionnez **Conformité des vulnérabilités** et entrez un **titre pour le graphique**.
7. Dans la liste **Profil d'analyse**, sélectionnez le profil d'analyse pour les actifs analysés.

   Avertissement : Si aucun profil d'analyse ne s'affiche, vous devez créer et exécuter une analyse PCI de votre réseau qui stockent ou traitent les informations PCI.
8. Dans la liste **Résultat de l'analyse**, sélectionnez la version du profil d'analyse à utiliser.

   A faire : Pour fournir une preuve de la conformité, vous devez sélectionner l'option **Dernier en date** dans la liste **Résultat de l'analyse**. Vous pouvez également générer un rapport de conformité en utilisant un profil d'analyse exécuté à une date antérieure.
9. Dans la liste **Type de rapport**, sélectionnez un type de rapport.

   Si vous sélectionnez **Récapitulatif global**, **Détails de la vulnérabilité** ou une combinaison des deux, l'attestation est jointe automatiquement à votre rapport de conformité PCI.
10. Renseignez les informations dans les volets **Informations sur le client de l'analyse** et **Informations de fournisseur d'analyse approuvé**.

    Important : Vous devez ajouter un nom dans la zone concernant l'**entreprise** pour les deux volets, car ces informations s'affichent dans la section Attestation du rapport.
11. Cliquez sur **Sauvegarder les détails du conteneur**, puis sur **Suivant**.
12. Utilisez l'assistant de création de rapports pour terminer le rapport de conformité PCI.

Résultats

Le rapport s'affiche dans la liste de rapports et est généré automatiquement.

Remarque :

Certaines colonnes de tableau du document PDF généré ne s'affichent pas lorsque vous créez un rapport PDF avec les paramètres suivants :

- Chart type - Vulnerabilities
- Graph type - Table
- Data to use - Current
- Group by - Instance

Le nombre important de colonnes de table ne pouvant pas être intégré sur une page au format US letter en mode paysage standard provoque cette erreur.

Pour éviter ce problème, n'utilisez pas de sortie PDF pour ce type de rapport. Affichez les rapports de vulnérabilité qui utilisent Group by Instance dans un tableur ou au format XML. Pour exporter le rapport, sélectionnez **XLS** ou **XML** en tant que format de rapport dans l'assistant.

Inclusion d'en-têtes de colonne dans les recherches d'actif

Limitez les recherches d'actif à l'aide de filtres incluant des profils d'actifs, un nom, un nombre de vulnérabilités et un score de risque.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le panneau de navigation, cliquez sur **Profils d'actifs** puis, dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
3. Dans la zone contenant les noms de colonne, dans la zone située à gauche, cliquez sur les en-têtes de colonne que vous voulez inclure dans votre recherche, puis cliquez sur le bouton fléché afin de déplacer les en-têtes sélectionnés vers la zone située à droite.

4. Cliquez sur boutons haut et bas pour modifier la priorité des en-têtes de colonne sélectionnés.
5. Lorsque la zone à droite contient tous les en-têtes de colonne sur lesquels vous voulez effectuer la recherche, cliquez sur **Rechercher**.

Chapitre 14. Analyse de nouveaux actifs qui communiquent avec Internet

Utilisez IBM QRadar Risk Manager pour créer des infractions lorsque de nouveaux actifs communiquent avec Internet, ce qui déclenche une analyse QRadar Vulnerability Manager des actifs.

Pour déclencher des analyses de nouveaux actifs qui communiquent avec Internet, procédez comme suit :

1. Créez une recherche enregistrée pour les nouveaux actifs.
2. Créez un profil d'analyse à la demande avec l'analyse dynamique activée.
3. Créez une question du moniteur de politique QRadar Risk Manager pour cibler les nouveaux actifs dans la recherche d'actifs enregistrée.
4. Surveiller la question du moniteur de politique QRadar Risk Manager.
5. Editez la règle créée par l'infraction.

Création d'une recherche d'actifs enregistrée pour les nouveaux actifs

Créez une recherche enregistrée pour capturer les nouveaux actifs qui ont été ajoutés à la base de données, au cours du nombre de jours que vous spécifiez.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Cliquez sur **Rechercher** > **Nouvelle recherche**.
4. Ajoutez vos critères de recherche dans le panneau **Paramètre(s) de recherche**.
5. Sélectionnez **Jours depuis la détection de l'actif**, **Est inférieur ou égal à**, puis entrez le nombre de jours.

   Vous pouvez spécifier d'autres critères, mais le plus important est **Jours depuis la détection de l'actif**.
6. Cliquez sur **Ajouter un filtre**.
7. Cliquez sur **Rechercher**.
8. Cliquez sur **Sauvegarder les critères**.
9. Entrez un nom pour la recherche, puis cliquez sur **OK** pour sauvegarder votre recherche.

Création d'un profil d'analyse à la demande

Pour déclencher une analyse en réponse à un événement de règle personnalisée, configurez un profil d'analyse à la demande et activez l'analyse dynamique.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Ajoutez un **Nom** et des **Adresses IP** dans l'onglet **Détails**.

© Copyright IBM Corp. 2012, 2020

Vous pouvez utiliser n'importe quelle adresse IP, car cette adresse IP est remplacée lorsque l'analyse dynamique est utilisée.

5. Cochez la case **Analyse à la demande activée**.
6. Cochez la case **Sélection de serveurs dynamiques**.

   Utilisez l'analyse dynamique dans IBM QRadar Vulnerability Manager pour associer les scanners individuels à une adresse IP, à des plages CIDR, à des plages d'adresses IP ou à un domaine que vous spécifiez dans le profil d'analyse. L'analyse dynamique est particulièrement utile lorsque vous déployez plusieurs scanners.
7. Cliquez sur **Sauvegarder**.

Concepts associés

Analyses de vulnérabilité dynamiques
Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse afin d'utiliser certains programmes d'analyse des vulnérabilités pour des plages CIDR spécifiques dans votre réseau. Par exemple, vos programmes d'analyse pourraient n'avoir accès qu'à certaines zones de votre réseau.

Détails relatifs au profil d'analyse

Tâches associées

Association de programmes d'analyse des vulnérabilités à des plages CIDR
Dans IBM QRadar Vulnerability Manager, pour effectuer une analyse dynamique, vous devez associer des programmes d'analyse des vulnérabilités à différents segments de votre réseau.

Analyse de plages CIDR avec différents programmes d'analyse des vulnérabilités
Dans IBM QRadar Vulnerability Manager, vous pouvez analyser des zones de votre réseau avec différents programmes d'analyse des vulnérabilités.

Création d'une question du moniteur de politique pour tester la communication avec Internet

Créez une question du moniteur de politique QRadar Risk Manager pour tester la communication entre les nouveaux actifs et Internet. Les nouveaux actifs sont définis dans une recherche d'actifs enregistrée.

Procédure

1. Cliquez sur l'onglet **Risks**.
2. Dans le menu de navigation, cliquez sur **Policy Monitor**.
3. Depuis le menu **Actions** , cliquez sur **New Asset Question**.
4. Dans la zone **What do you want to name this question**, entrez un nom pour la question.
5. Dans la liste **Evaluate On**, sélectionnez **Actual Communication**.
6. Dans la liste **Importance Factor**, sélectionnez le niveau d'importance que vous voulez associer à cette question.
7. Déterminez l'intervalle de temps pour la question.
8. Dans la zone **Which tests do you want to include in your question**, sélectionnez l'icône d'ajout (**+**) en regard des tests suivants :
   - **have accepted communication to the internet**
   - **and include only the following asset saved searches**
9. Configurez les paramètres pour vos tests dans la zone **Find Assets that**.
   a) Modifiez le test en **have accepted communication from the internet** en cliquant sur **to**.
   b) Cliquez sur **asset saved searches**, puis sélectionnez votre recherche sauvegardée.
10. Pour affecter l'appartenance à cette question, dans la zone des groupes, cochez les cases correspondantes.
11. Cliquez sur **Save Question**.

Surveillance de la communication entre les nouveaux actifs et l'Internet

Configurez la question du moniteur de politique pour générer une infraction lorsqu'un actif de la recherche d'actifs enregistrée communique avec Internet.

Procédure

1. Cliquez sur l'onglet **Risques**.
2. Dans le menu de navigation, cliquez sur **Moniteur de politique d'administration**.
3. Sélectionnez la question à surveiller.
4. Cliquez sur **Moniteur**.
5. Sélectionnez un intervalle dans **Policy evalutation interval**.
6. Entrez un nom dans la zone **Nom d'événement**.

   Si vous sélectionnez **Vérifier que l'événement attribué fait partie d'une infraction**, le *Nom d'événement* apparaît dans la zone **Description** pour une infraction, lorsque vous sélectionnez **Toutes les infractions** dans l'onglet **Infractions**.

   Le nom de la règle générée à partir d'une infraction est **Risk Question Monitor:** <*Nom d'événement*. Ce format pour le nom d'infraction apparaît sur l'onglet **Infractions** lorsqu'une infraction est générée.
7. Entrez une description du nom de l'événement.
8. Dans la section **Détails d'événements**, sélectionnez la case **Vérifier que l'événement attribué fait partie d'une infraction** et **(Correlate By: Actif)** dans le menu.
9. Dans la section **Additional Actions** :
   - **E-mail**

     Cette option est utile lorsque vous souhaitez obtenir une notification pour le premier événement qui est distribué comme une infraction. Vous pouvez modifier la règle qui est générée à partir de cette infraction pour déclencher une analyse. Si vous ne voulez pas être averti de chaque événement, après avoir configuré la règle qui est générée par l'infraction, vous pouvez désactiver cette notification.
   - **Send to SysLog**

     Si vous souhaitez que l'événement soit consigné, sélectionnez cette option.
   - **Envoyer une notification**

     Si vous souhaitez que l'événement apparaisse dans l'alerte **Notifications système** sur le tableau de bord, sélectionnez cette option.
10. Sélectionnez **Enable the monitor results function for this question/simulation**.
11. Cliquez sur **Sauvegarder le moniteur**.
12. Cliquez sur **Soumettre la question**.

Configuration d'une règle d'infraction pour déclencher une analyse

Pour déclencher une analyse de tous les actifs qui communiquent avec Internet, configurez la règle générée par l'infraction.

Avant de commencer

Une infraction doit être générée. Vous pouvez générer l'infraction manuellement ou attendre qu'un actif communique avec Internet. Pour générer l'infraction, vous pouvez effectuer l'une des étapes suivantes :

- Générez une infraction manuellement en connectant temporairement tout nouvel actif de la recherche d'actifs enregistrée à Internet.

- Recherchez les règles sur l'onglet **Infractions** et recherchez la règle après qu'une infraction est générée.
- Activez la notification par e-mail pour l'événement distribué qui crée une infraction. Vous pouvez modifier la règle lorsque vous obtenez cette notification.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans le menu de navigation, cliquez sur **Règles**.
3. Utilisez la zone de recherche de la barre d'outils pour rechercher la règle.

   Le nom de la règle est **Risk Question Monitor :** <*Nom d'événement*>.

   Vous pouvez rechercher par *Nom d'événement* dans la fenêtre **Monitor Question Results**.

   Le *Nom d'événement* pour une infraction apparaît dans la zone **Description** lorsque vous sélectionnez **Toutes les infractions**.
4. Cliquez deux fois sur le nom de la règle pour ouvrir l'**Assistant Règle**.
5. Cliquez sur **Suivant**.
6. Configurez les paramètres suivants :
   a) Cochez la case **Vérifier que l'élément événement détecté fait partie d'une infraction**.
   b) Sélectionnez **Adresse IP cible** dans le menu **Indexer l'infraction en fonction de**.
   c) Cochez la case **Envoyer au SysLog local**.
   d) Cochez la case **Déclencher l'analyse**.
   e) Sélectionnez le profil d'analyse que vous souhaitez utiliser dans le menu **Profil d'analyse à utiliser comme modèle**.

      Vous devez sélectionner l'option d'**analyse à la demande** dans le profil d'analyse que vous voulez utiliser avec cette règle.
   f) Cliquez sur le bouton d'option **Destination** pour la zone **Environnements locaux à analyser**.
   g) Entrez des valeurs pour le paramètre **Limiteur de réponse**.

      Configurez des intervalles appropriés afin d'éviter une surcharge possible sur votre système.
   h) Si vous ne souhaitez pas activer cette règle immédiatement, désactivez l'option **Activer la règle**, puis cliquez sur **Terminer**.

Chapitre 15. Intégrations de logiciels de sécurité

IBM QRadar Vulnerability Manager s'intègre à d'autres produits de sécurité afin de vous aider à gérer et hiérarchiser vos risques de sécurité. L'intégration avec d'autres logiciels étend les capacités de QRadar Vulnerability Manager.

Intégration à QRadar Vulnerability Manager

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

Installez QRadar Risk Manager en tant que dispositif distinct, puis ajoutez-le à votre console QRadar SIEM en tant qu'hôte géré à l'aide de l'outil **Gestion du système et de la licence** dans l'onglet **Admin**.

Pour plus d'informations sur l'installation de QRadar Risk Manager, voir *IBM QRadar Risk Manager Installation Guide*.

Politiques de risque et hiérarchisation des vulnérabilités

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

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

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

- Obtenir une visibilité immédiate des vulnérabilités ayant fait échouer une politique de risque.

  Par exemple, les nouvelles informations peuvent s'afficher sur le tableau de bord QRadar ou être envoyées par e-mail.
- Redéfinissez la priorité des vulnérabilités qui ont besoin d'une attention immédiate.

  Par exemple, un administrateur peut utiliser l'option **Score de risque** pour identifier rapidement les vulnérabilités à haut risque.

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

Pour plus d'informations sur la création et la surveillance des politiques de risque, voir *IBM QRadar Risk Manager User Guide*.

© Copyright IBM Corp. 2012, 2020

Chapitre 16. Intégration à IBM BigFix

IBM QRadar Vulnerability Manager s'intègre à IBM BigFix afin de vous permettre de filtrer et de hiérarchiser les vulnérabilités pouvant être corrigées.

Pourquoi utiliser les fonctions de BigFix avec la gestion des vulnérabilités ?

Antérieurement connu comme IBM Security Endpoint Manager, BigFix offre une visibilité et un contrôle partagés entre les opérations informatiques et la sécurité. BigFix applique des fixlets aux vulnérabilités de priorité élevée identifiées et envoyées par QRadar Vulnerability Manager à BigFix. Les fixlets sont des packages que vous déployez dans vos actifs ou noeuds finaux pour résoudre des vulnérabilités spécifiques. Vous pouvez déployer des fixlets sur plusieurs actifs ou noeuds finaux à la fois à l'aide du tableau de bord **Gestion des ordinateurs vulnérables** de la console BigFix.

Utilisez le tableau de bord **Gestion des ordinateurs vulnérables** sur la console BigFix pour gérer et contrôler un réseau de centaines de milliers d'actifs ou de noeuds finaux sur toute une gamme de plateformes et de périphériques, quel que soit leur emplacement géographique.

Comment résoudre les vulnérabilités avec BigFix?

BigFix fournit un tableau de bord qui est intégré à QRadar Vulnerability Manager. Utilisez ce tableau de bord sur la console BigFix pour afficher et résoudre les vulnérabilités détectées et envoyées par QRadar Vulnerability Manager.

Pour afficher les données de vulnérabilité de QRadar Vulnerability Manager dans la console BigFix, configurez QRadar Vulnerability Manager puis configurez BigFix pour traiter les données de vulnérabilité envoyées par QRadar Vulnerability Manager. Pour plus d'informations sur la configuration de BigFix, voir le document *IBM BigFix QRadar User Guide*.

Comment QRadar Vulnerability Manager et BigFix fonctionnent-ils ensemble ?

QRadar Vulnerability Manager analyse les vulnérabilités de vos actifs ou de vos noeuds finaux et assigne un score de risque qui correspond au niveau de risque qu'une vulnérabilité représente pour votre organisation. QRadar Vulnerability Manager utilise le paramètre de score de risque dans l'adaptateur BigFix pour filtrer les vulnérabilités à haut risque devant être envoyées à BigFix afin d'être résolues. QRadar Vulnerability Manager assigne un ID CVE à chaque vulnérabilité qu'il envoie à BigFix.

En savoir plus sur l'identification et le traitement des données de vulnérabilité :

La liste suivante décrit comment les données de vulnérabilité identifiées par CVE (Common Vulnerabilities and Exposures) sont traitées par QRadar Vulnerability Manager et BigFix

- QRadar Vulnerability Manager envoie uniquement les vulnérabilités possédant des ID CVE à BigFix.
- QRadar Vulnerability Manager envoie tous les ID CVE associés à une vulnérabilité unique à BigFix. Certaines vulnérabilités peuvent un grand nombre d'ID CVE.
- QRadar Vulnerability Manager envoie uniquement les CVE affichant le score de risque le plus élevé à BigFix lorsque ce CVE affiche deux vulnérabilités ou plus.

  Par exemple, l'ID CVE suivant, 2016-0015, affiche deux vulnérabilités différentes. Seul le CVE ayant la vulnérabilité à haut risque est envoyé à BigFix.

```
{
Name: CVE-2016-0015
- MS16-007 - Microsoft - DirectShow - Code Execution Issue
Vulnerability ID: 169296
CVE: 2016-0015
Risk: High

Name: Microsoft Windows DirectShow code execution
Vulnerability ID: 169243
CVE: 2016-0015
```

© Copyright IBM Corp. 2012, 2020

```
Risk: Medium
}
```

BigFix reçoit les données de vulnérabilité avec les scores de risque et ID CVE de QRadar Vulnerability Manager qui sont visibles sur le tableau de bord BigFix **Gestion des ordinateurs vulnérables**. Utilisez le tableau de bord **Gestion des ordinateurs vulnérables** de la console BigFix pour afficher et gérer les vulnérabilités envoyées par QRadar Vulnerability Manager. BigFix résout les vulnérabilités à haut risque pour lesquels il possède un fixlet en appliquant un fixlet directement à l'actif ou au noeud final. QRadar Vulnerability Manager obtient une mise à jour de l'état de correction de la vulnérabilité de BigFix Web Reports via l'API SOAP.

Comment étendre BigFix à QRadar Risk Manager ?
Si vous disposez d'une installation QRadar Risk Manager, vous pouvez utiliser les politiques d'administration de risque dans QRadar Risk Manager pour optimiser les score du risque de vos actifs. Lorsque les règles d'administration des risques que vous définissez dans QRadar Risk Manager réussissent ou échouent, les scores de risque des vulnérabilités sont ajustés dans QRadar Vulnerability Manager. Vous pouvez redéfinir la priorité des vulnérabilités qui demandent une attention immédiate. Si vous appliquez des politiques d'administration du risque à des actifs dans QRadar Risk Manager, les scores de risque de toutes les vulnérabilités de ces actifs seront ajustés. Pour plus d'informations, voir le guide d'utilisation QRadar Risk Manager.

Résolution des vulnérabilités

Suivant si vous avez installé et intégré BigFix, QRadar Vulnerability Manager fournit les informations suivantes sur vos vulnérabilités.

Si BigFix n'est pas installé
QRadar Vulnerability Manager fournit des mises à jour quotidiennes sur les vulnérabilités pour lesquelles un correctif est disponible.

QRadar Vulnerability Manager assure la maintenance d'une liste d'informations sur les correctifs des vulnérabilités. Ces informations sont corrélées au catalogue des vulnérabilités connues.

Utilisez la recherche dans QRadar Vulnerability Manager pour identifier les vulnérabilités possédant un correctif disponible.

Si BigFix est installé
QRadar Vulnerability Manager fournit également des détails spécifiques sur le processus de correction de la vulnérabilité. Par exemple, un correctif peut être planifié, ou un actif peut être déjà corrigé.

Le serveur BigFix collecte les informations de correctif auprès de chacun des agents BigFix. QRadar Vulnerability Manager obtient des mises à jour sur les informations de correction des vulnérabilités du serveur BigFix à des intervalles de temps préconfigurés.

Utilisez la recherche dans QRadar Vulnerability Manager pour identifier les vulnérabilités déjà corrigées ou dont la correction est planifiée.

Composants d'intégration

Un déploiement intégré typique comprend les composants suivants :

- Console IBM QRadar.
- QRadar Vulnerability Manager.
- Serveur BigFix.
- Agent BigFix sur chaque cible d'analyse de votre réseau.

Tâches associées
Identification de l'état de correctif des vulnérabilités
Information associée

Interactions entre IBM QRadar et IBM BigFix

Avant de configurer l'intégration entre IBM QRadar et BigFix, il est important de comprendre comment ils interagissent entre eux.

Le diagramme suivant offre un aperçu général de certaines interactions entre QRadar et BigFix, depuis l'analyse initiale des actifs à la résolution des vulnérabilités sur les actifs analysés.

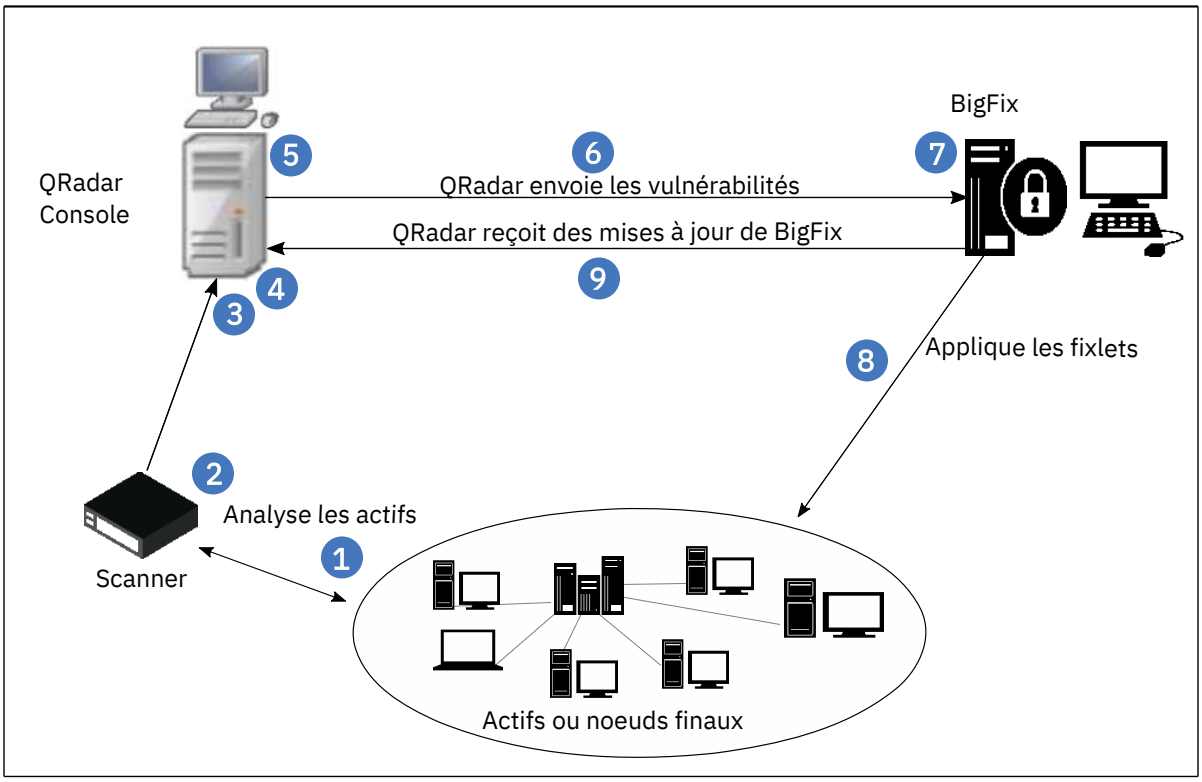

Figure 1. Interactions de QRadar Vulnerability Manager et BigFix

La liste suivante offre un bref compte-rendu des interactions entre QRadar et BigFix, depuis l'analyse initiale des vulnérabilités jusqu'à la résolution de ces vulnérabilités :

1. Le scanner QRadar Vulnerability Manager réalise une analyse authentifiée des actifs pour détecter des vulnérabilités. Seules les vulnérabilités des actifs configurés dans des profils d'analyse utilisant les politiques d'administration d'analyse Full (complet), Patch (correctif), ou PCI peuvent être traitées par BigFix.
2. Si un agent BigFix est installé sur un actif, QRadar Vulnerability Manager extrait l'*ID agent BES* de l'actif lorsqu'il détecte des vulnérabilités sur l'actif. L'*ID agent BES* est l'identificateur unique qui est utilisé par BigFix pour identifier l'actif et pour résoudre les vulnérabilités sur cet actif. BigFix se réfère aux actifs QRadar en tant qu'ordinateurs.
3. Les résultats d'analyse sont mis à jour dans le modèle d'actif QRadar qui inclut l'*ID agent BES* de tous les actifs ayant un agent BigFix. Lorsque l'état d'analyse du profil d'analyse affiche `progress=100%`, le modèle d'actif est mis à jour et les données de vulnérabilité sont envoyées à BigFix dans les 15 minutes qui suivent, par défaut.
4. Lorsque le modèle d'actif est mis à jour avec les données d'analyse, l'adaptateur BigFix qui est installé sur la console QRadar Console reçoit les données de vulnérabilité mises à jour avec les scores de risque du modèle d'actif. Les données contiennent l'*ID agent BES*. L'adaptateur BigFix traite uniquement les informations de vulnérabilité des actifs lorsqu'un *ID agent BES* est inclus.
5. Les données de vulnérabilité envoyées à BigFix sont filtrées par rapport aux paramètres "score de risque" qui sont configurés dans le fichier de propriétés de l'adaptateur (`/opt/qvm/adaptor/`

`config/adaptor.properties`) sur la console QRadar Console. Le score de risque par défaut est 0,0, ce qui signifie que toutes les vulnérabilités sont envoyées à BigFix.

6. L'adaptateur BigFix utilise l'API REST BigFix pour envoyer les informations de vulnérabilité à BigFix et il associe les CVE aux fixlets. Par défaut, les données sont envoyées à BigFix à intervalles de 15 minutes.
7. Les informations de vulnérabilité envoyées par l'API REST peuvent être affichées sur le tableau de bord **Gestion des ordinateurs vulnérables** de BigFix. Vous pouvez déployer des fixlets pour les actifs ayant des vulnérabilités à haut risque dans le tableau de bord **Gestion des ordinateurs vulnérables** de BigFix. BigFix utilise l'*ID agent BES* comme unique référence pour l'actif lorsqu'il applique les fixlets directement à l'actif.
8. BigFix applique les fixlets aux actifs qui ont des vulnérabilités.
9. L'API SOAP (Web Reports) est utilisé pour obtenir l'état des correctifs de vulnérabilités de BigFix. Utilisez les recherches sauvegardées et les filtres de l'onglet **Vulnérabilités** pour afficher ces informations de vulnérabilité mises à jour.

   Vous devez réanalyser les actifs corrigés pour mettre à jour le modèle d'actif avec l'état de vulnérabilité révisé de vos actifs.

Configuration de la communication chiffrée entre IBM BigFix et QRadar

Pour permettre à IBM QRadar Vulnerability Manager de recevoir les mises à jour de statut de correctif de vulnérabilité à l'aide de Web Reports à partir de IBM BigFix, configurez Transport Layer Security (TLS).

Lorsque QRadar Vulnerability Manager reçoit des mises à jour des états des fixlets de BigFix, il utilise l'API SOAP des Web Reports BigFix pour solliciter les mises à jour à l'aide de requêtes utilisant le langage BigFix Relevance. Les requêtes sont utilisées pour extraire les données de la base de données des Web Reports BigFix en mémoire. QRadar analyse et enregistre les données. Vous pouvez utiliser les recherches sauvegardées pour afficher les mises à jour BigFix dans QRadar. BigFix n'utilise pas le protocole TLS Web Reports par défaut. Vous configurez la communication TLS et BigFix Web Reports.

Avant de commencer

Les composants suivants doivent être installés sur votre réseau :

- Serveur BigFix.
- Console BigFix.
- Agent BigFix dans chaque actif de votre réseau faisant partie de l'analyse.
- Console IBM QRadar.
- Installation sous licence de QRadar Vulnerability Manager.

Vous devez posséder QRadar V7.2.6 ou une version ultérieure avec les mises à jour les plus récentes.

Remarque : Pour vous préparer à cette intégration, il est recommandé d'exécuter la **Mise à jour automatique** sous l'onglet **Admin** pour obtenir les outils d'analyse les plus récents.

Procédure

1. Pour configurer TLS, effectuez les étapes suivantes :
   a) Téléchargez le certificat de clé publique à partir de BigFix dans votre console QRadar Console en entrant la commande suivante à l'invite shell de votre console QRadar Console.

   ```
   openssl x509 -in <(openssl s_client -connect <adresse IP bigfix>:<port> -
   prexit 2>/dev/null) > /opt/qvm/iem/iem_cert.pem
   ```

   Généralement, BigFix écoute sur le port 52312.

   b) Pour créer un magasin de clés de confiance dans QRadar, entrez la commande suivante :

```
keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias
iem_webreports
```

c) Importez le certificat de clé publique BigFix dans votre magasin de clés de confiance QRadar en tapant la commande suivante :

```
keytool -importcert -file /opt/qvm/iem/iem_cert.pem -
keystore /opt/qvm/iem/truststore.jks -storepass
<mot_passe_magasin_de_clés> -alias BigFix_webreports
```

d) A l'invite **Trust this certificate?**, entrez **Yes**.

2. Pour configurer TLS et BigFix Web Reports pour QRadar Vulnerability Manager, effectuez les étapes suivantes :

a) Utilisez le protocole SSH pour vous connecter à la console QRadar comme utilisateur root.

b) Entrez `./iem-setup-webreports.pl` et, lorsque vous y êtes invité, entrez le nom d'hôte, le port d'hôte, le nom d'utilisateur et le mot de passe du serveur BigFix.

Vous pouvez utiliser cette commande à partir de n'importe quel répertoire. Les fichiers sont créés dans le répertoire `/opt/qvm/iem`.

c) A l'invite **Use SSL/TLS encryption?**, entrez la réponse appropriée.

d) Suivez les invites.

e) Pour afficher le contenu du fichier `webreports.properties`, entrez la commande suivante à l'invite du shell :

```
more /opt/qvm/iem/webreports.properties
```

Le fichier `webreports.properties` contient les protocoles SSL/TLS de transport autorisés, par exemple `webreports.tls.protocols=TLSv1.2` ou une liste de valeurs séparées par des virgules `webreports.tls.protocols=TLSv1.2,TLSv1.1`

Vérifiez que la ligne suivante contient un numéro de port qui suit l'adresse IP :

```
webreports.endpoint=http://<IP_address>:<port>/webreports
```

Si vous souhaitez utiliser un port différent, éditez le fichier `/opt/qvm/iem/webreports.properties` et modifiez le numéro de port.

Configuration de QRadar Vulnerability Manager pour l'envoi des données de vulnérabilité à BigFix

Installez et configurez l'adaptateur BigFix sur la console QRadar Console pour activer IBM QRadar Vulnerability Manager afin d'envoyer les données de vulnérabilité avec les scores de risque à IBM BigFix.

Procédure

1. Connectez-vous à la console QRadar Console en tant qu'utilisateur root.
2. Configurez les paramètres de l'adaptateur BigFix :

a) Accédez au répertoire `/opt/qvm/adaptor/config` et exécutez le script de configuration : `./setup-adaptor.sh`

b) Entrez un nouveau mot de passe pour créer le magasin de clés de confiance stockant le certificat serveur BigFix.

Le magasin de clés de confiance est créé dans `/opt/qvm/adaptor/truststore.jks`

Les fichiers de propriétés suivants sont créés dans le répertoire `/opt/qvm/adaptor/config`.

- `adaptor.properties`
- `adaptor-bigfix.properties`
- `plugin-bigfix.properties`

c) Vérifiez que le fichier `plugin-bigfix.properties` comporte une entrée TLS, par exemple `TLSv1.2` ou une liste de valeurs TLS séparées par une virgule `TLSv1.2,TLSv1.1,SSLv1.3`

La première entrée de la liste est utilisée pour créer le contexte de sécurité : `bes.rest.allowed.protocols=TLSv1.2`

d) A l'invite, fournissez des détails sur le serveur d'API REST BigFix en entrant le nom d'hôte ou l'adresse IP, le nom d'utilisateur et le mot de passe du serveur BigFix.

Le nom d'utilisateur et le mot de passe que vous entrez correspondent aux données d'identification utilisées pour l'API REST BigFix. L'API REST est utilisée pour envoyer les données de vulnérabilité à BigFix.

e) Redémarrez le profileur d'actifs à l'aide de la commande suivante :

```
/opt/qradar/init/assetprofiler restart
```

Pour assurer une performance optimale, ne redémarrez pas le profileur d'actifs lorsque des analyses QRadar Vulnerability Manager sont en cours d'exécution ou lorsque vous attendez des importations de vulnérabilités d'un scanner tiers.

Le fichier `adaptor.properties` est créé. Ce fichier contient les paramètres de configuration des données de vulnérabilité envoyées à BigFix.

3. Vérifiez que le processus de configuration a réussi :

a) Dans le fichier `/opt/qvm/adaptor/config/adaptor.properties`, vérifiez que les propriétés suivantes sont définies :

```
qvm.adaptor.listener.enabled=true
```

```
qvm.adaptor.process.daemon=false
```

b) Définissez le score de risque et la granularité de la mise à jour d'actif dans le fichier `adaptor.properties` en éditant les propriétés suivantes :

Tableau 14. Propriétés et descriptions de l'adaptateur

Nom de la propriété (API)	**Description**
`qvm.adaptor.minimum.vuln.riskscore=n`	Définit le seuil de chaque score de risque de vulnérabilité. Ces vulnérabilités, égales à ou supérieures à la valeur définie, sont envoyées à BigFix. Par exemple, si vous définissez la valeur 5, seules les vulnérabilités dont les scores de risque sont égaux ou supérieurs à 5 sont envoyées à BigFix.

Tableau 14. Propriétés et descriptions de l'adaptateur (suite)

Nom de la propriété (API)	Description
qvm.adaptor.minimum.asset.riskscore =n	Score de risque cumulé de toutes les vulnérabilités de cet actif. Les vulnérabilités des actifs ayant un score inférieur à cette valeur ne sont pas envoyées à BigFix, sauf si l'actif a des vulnérabilités égales ou supérieures à la valeur définie pour **minimum.vuln.riskscore**. **Remarque : minimum.vuln.riskscore** remplace **minimum.asset.riskscore**. Si la valeur 0 est attribuée à **minimum.vuln.riskscore**, toutes les vulnérabilités sont alors envoyées à IBM BigFix, quelle que soit la valeur de **minimum.asset.riskscore**. Utilisez le paramètre **minimum.asset.riskscore** pour capturer les vulnérabilités des actifs ayant plusieurs vulnérabilités à faible risque, générant un score de risque cumulé élevé pour un actif. Lorsque vous définissez cette valeur, vous devez avoir conscience de l'impact de la valeur **minimum.vuln.riskscore** sur ce paramètre.
qvm.adaptor.assetupdate.limit=n	Définit la façon dont les ressources de données du tableau de bord BigFix sont divisées. Une scission n'interviendra pas avant que tous les ID CVE du dernier actif ne soient remplis. • Par exemple, **qvm.adaptor.assetupdate.limit=20**, l'actif 1 possède 19 ID CVE et l'actif 2 possède 30 ID CVE. Une ressource de données est générée et contient les deux actifs, avec un total de 49 ID CVE. • Par exemple, **qvm.adaptor.assetupdate.limit=19**, l'actif 1 possède 19 ID CVE et l'actif 2 possède 30 ID CVE. Deux ressources de données sont générées, chacune contenant un actif.
qvm.adaptor.source.data.delay=n	Définit la fréquence à laquelle les données sont envoyées à BigFix. Par exemple, si n=15, les données de vulnérabilité sont envoyées à BigFix toutes les 15 minutes, s'il existe des données de vulnérabilité pouvant être envoyées à BigFix.

En éditant le fichier `adaptor.properties`, les données de vulnérabilité que vous envoyez à BigFix sont filtrées.

c) Vérifiez que la configuration du plug-in BigFix crée les répertoires suivants :

- `/store/qvm/adaptor/data`

- `/store/qvm/adaptor/bigfix`

d) Vérifiez que la consignation est activée dans le fichier `/opt/qvm/adaptor/log4j.xml`.

Les fichiers journaux se trouvent dans les fichiers `/var/log/qvm-integration-adaptor.log` et `/var/log/qvm-adaptor-cron.log`.

Remarque : Si vous ne téléchargez pas le certificat parce que le serveur BigFix est inaccessible, la configuration n'échoue pas. Vous pouvez télécharger le certificat ultérieurement en exécutant la commande suivante :

`./install-cert.sh <truststore_location> <truststore_password><truststore_IP_address: port>`

Par exemple, utilisez le format de commande suivant :

```
./install-cert.sh /opt/qvm/adaptor/truststore.jks <abc3password>
<192.0.2.0>:<63455>
```

Traitement des problèmes d'intégration de BigFix et QRadar Vulnerability Manager

Résolvez les problèmes qui peuvent se produire lorsque vous configurez votre intégration de BigFix et QRadar Vulnerability Manager.

Traitement des problèmes de contenus

Le certificat BigFix n'est pas importé en raison d'un échec de connexion au serveur IBM BigFix

Si le certificat n'est pas importé dans QRadar en raison d'un échec de connexion au serveur BigFix, le message d'erreur suivant peut s'afficher :

```
ERREUR [TrustStoreConfig] Impossible de configurer le fichier de clés certifiées
avec des certificats homologues :
```

```
Connexion interrompue java.net.ConnectException : Connexion interrompue.
```

La configuration a réussi mais les certificats ne sont pas présents dans le magasin de clés de confiance.

Vous devez charger les certificats manuellement en effectuant les étapes suivantes si vous avez accès au serveur BigFix.

1. Accédez au répertoire `/store/qvm/adaptor`.
2. Exécutez le script de configuration : `./install-cert.sh <truststore_location> <truststore_password><truststore_IP_address:port>` Le port est le port de service auquel le certificat appartient.

Vérifiez la connectivité avec IBM BigFix

Pour vérifier la connectivité avec IBM BigFix, effectuez les étapes suivantes :

1. Entrez l'URL suivante dans un navigateur Web :

   `https://`*`IP_address or DNS_hostname for BigFix:8080`*`/webreports?page=QNA`
2. Entrez la chaîne suivante sur une seule ligne, sur l'invite de commande :

   ```
   (id of site of it,id of it,name of it,cve id list of it) of fixlets whose
   (cve id list of it as lowercase contains "cve") of bes sites
   ```
3. Cliquez sur **Evaluate**

La chaîne suivante constitue un exemple de sortie d'un résultat :

```
2, 104301, MS01-043: NNTP Service in Windows NT 4.0
Contains Memory Leak, CVE-2001-0543
```

Le tableau suivant décrit la répartition de ce résultat :

Tableau 15. Résultat de la requête

Résultat	Paramètre de requête	Description
2	(id of site of it)	ID de site du fixlet
104301	(id of it)	ID du fixlet
MS01-043: NNTP Service in Windows NT 4.0 Contains Memory Leak	(name of it)	Nom du fixlet
CVE-2001-0543	(cve id list of it)	ID CVE

Les outils d'analyse les plus récents sont-ils installés ?

Vous devez exécuter des mises à jour automatiques pour obtenir les outils d'analyse les plus récents pour les nouvelles installations de QRadar car ils sont nécessaires au fonctionnement de cette intégration. Exécutez la mise à jour automatique sous l'onglet **Admin**, en cliquant sur l'icône **Mise à jour automatique**.

Pour en savoir plus sur l'installation des mises à jour automatiques de QRadar, voir le manuel *IBM QRadar Administration Guide*.

La fonction d'analyse de BigFix est-elle installée ?

Exécutez la commande suivante pour tester si la fonction d'analyse de BigFix est installée sur QRadar :

```
grep -rl 'BIG_FIX_AGENT_ID' /opt/qvm
```

Les résultats suivants sont renvoyés si la fonction d'analyse de BigFix est installée :

- `/opt/qvm/sys/perl/scanner/FusionVM/smb_patch_scanning.pm`
- `/opt/qvm/bin/ssh/packages/bin/ssh-packages`

Si vous ne voyez pas ces fichiers, exécutez une mise à jour automatique sous l'onglet **Admin** en cliquant sur l'icône **Mise à jour automatique**.

Réinitialisation du mot de passe

Si vos détails de BigFix changent, vous pouvez avoir besoin de modifier votre mot de passe.

1. Editez le fichier `plugin-bigfix.properties` situé dans le répertoire `/opt/qvm/adaptor/config`.
2. Remplacez la ligne suivante :

   `_decrypt.bes.rest.password=lUb5qzr7FIVH+J319erc+g==`

   par la ligne suivante :

   `_encrypt.bes.rest.password=newpassword`

   où `newpassword` correspond à votre nouveau mot de passe.
3. Exécutez le script suivant pour chiffrer votre nouveau mot de passe :

   `./password-property-encrypt.sh plugin-bigfix.properties`

Erreur d'exception de mot de passe dans le fichier /var/log/iem-cron.log

Vous pourriez voir l'erreur suivante dans le fichier `/var/log/iem-cron.log`.

```
Exception in thread "main" java.lang.NoClassDefFoundError:
com.sun.org.apache.xerces.internal.dom.ElementNSImpl
```

Cette erreur d'exception de mot de passe se produit lorsque le fichier `/opt/qvm/iem/webreports.properties` utilise un mot de passe incorrect.

Pour corriger cette erreur, à l'invite du shell, exécutez `/opt/qvm/iem/iem-setup-webreports.pl`, puis entrez le mot de passe correct.

Les données d'analyse de vulnérabilité ne sont pas envoyées à BigFix

Vérifiez que le scanner peut s'authentifier sur l'actif et accéder aux informations requises.

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Sur la ligne du nom de l'analyse, cliquez sur le numéro qui s'affiche dans la colonne **Actifs**.
3. Survolez les symboles d'avertissement qui s'affichent dans la colonne avec l'icône du drapeau.
4. Vérifiez si des problèmes existent au niveau des données d'identification dans le profil d'analyse ou si un problème au niveau de la configuration des actifs empêche le scanner d'accéder aux informations requises.

Le modèle d'actif est-il actualisé ?

Pour vérifier que le modèle d'actif est actualisé avec vos résultats d'analyse :

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Sur le menu de navigation, cliquez sur **Résultats d'analyse**.

   Si vous voyez un triangle d'avertissement rouge, le modèle d'actif n'est pas mis à jour avec vos résultats d'analyse.

Désactivation de l'intégration à BigFix et à QRadar Vulnerability Manager

Procédez comme suit si vous souhaitez désactiver l'intégration à BigFix et à QRadar Vulnerability Manager.

Procédure

1. Connectez-vous à la console QRadar Console en tant qu'utilisateur root.
2. Pour désactiver l'adaptateur QRadar Vulnerability Manager, entrez les commandes suivantes :

   - `systemctl stop qvmadaptor.timer`

- `systemctl disable qvmadaptor.timer`
- `systemctl daemon-reload`

3. Entrez la commande suivante pour renommer le répertoire `/store/qvm/adaptor` :
   `mv /store/qvm/adaptor /store/BigFix.old/`
4. Entrez la commande suivante pour redémarrer le profileur d'actif :
   `systemctl restart assetprofiler`

   Conseil : Si vous souhaitez activer à nouveau l'intégration BigFix ultérieurement, exécutez la procédure ci-dessus en sens inverse.

Chapitre 17. Intégration à IBM Security SiteProtector

QRadar Vulnerability Manager peut être intégré à IBM Security SiteProtector afin d'optimiser les règles du système de prévention des intrusions.

Lorsque vous configurez IBM Security SiteProtector, les vulnérabilités détectées par les analyses QRadar Vulnerability Manager sont automatiquement transmises à SiteProtector.

QRadar Vulnerability Manager réachemine vers IBM Security SiteProtector les vulnérabilités provenant des résultats de l'analyse et associées à des ID ISS X-Force. QRadar Vulnerability Manager utilise l'agent MSL pour réacheminer les vulnérabilités.

Connexion à IBM Security SiteProtector

Vous pouvez transmettre des données de vulnérabilité d'IBM QRadar Vulnerability Manager à IBM Security SiteProtector pour conduire la politique du système de prévention des intrusions.

Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
3. Cliquez sur **Utiliser SiteProtector**.
4. Dans la zone **Adresse IP SiteProtector**, entrez l'adresse IP du serveur du gestionnaire de l'agent IBM Security SiteProtector.

   Le port par défaut pour cette connexion est 3995.
5. Cliquez sur **Enregistrer**, puis sur **Fermer**.
6. Dans la barre d'outils de l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.
7. Cliquez sur **OK**.

Que faire ensuite

Effectuez une analyse des actifs de votre réseau pour déterminer si les données de vulnérabilité sont affichées dans votre installation IBM Security SiteProtector.

© Copyright IBM Corp. 2012, 2020

Chapitre 18. Recherche de vulnérabilités, articles et avis

Utilisez les outils proposés dans IBM QRadar Vulnerability Manager pour demeurer conscient du niveau de menace des vulnérabilités et gérer la sécurité dans votre organisation.

Une bibliothèque de vulnérabilités contient les vulnérabilités courantes qui sont collectées à partir d'une liste de sources externes. La ressource externe la plus importante est NVD (National Vulnerability Database). Vous pouvez rechercher des vulnérabilités particulières en utilisant des critères tels que le fournisseur, le produit et la plage de dates. Par exemple, vous pouvez être intéressé par des vulnérabilités spécifiques qui existent dans des produits ou des services utilisés dans votre entreprise.

QRadar Vulnerability Manager propose également une liste d'avis et d'articles sur la sécurité, établie à partir d'une liste externe de ressources et de fournisseurs. Cette source d'informations de sécurité provenant du monde entier est utile car elle vous permet de demeurer informé des risques de sécurité actuels.

Affichage d'informations détaillées sur les vulnérabilités publiées

Dans IBM QRadar Vulnerability Manager, vous pouvez afficher des informations détaillées sur les vulnérabilités.

Sur la page **Recherche de vulnérabilités**, vous pouvez examiner en détail les mesures CVSS et accéder aux informations publiées par l'équipe de recherche et développement IBM X-Force.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez **Recherche** > **Vulnérabilités**.
3. Si aucune vulnérabilité ne s'affiche, sélectionnez une autre plage de temps dans la liste **Affichage des vulnérabilités de :**.
4. Pour rechercher les vulnérabilités, dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
5. Identifiez la vulnérabilité que vous voulez examiner en détail.
6. Cliquez sur le lien de la vulnérabilité dans la colonne **Vulnérabilité**.

Rester informé sur les développements globaux en matière de sécurité

Dans IBM QRadar Vulnerability Manager, vous pouvez afficher les nouveautés pour la sécurité dans le monde pour rester informer des développements actuels en matière de sécurité.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Recherche** > **Articles**.
3. Si aucun article ne s'affiche, sélectionnez une autre plage de temps dans la liste d'**affichage**.
4. Pour rechercher les articles, dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
5. Identifiez l'article qui vous intéresse.
6. Cliquez sur le lien vers l'article dans la colonne **Titre de l'article**.

© Copyright IBM Corp. 2012, 2020

Affichage des recommandations de sécurité provenant des fournisseurs de vulnérabilités

Dans IBM QRadar Vulnerability Manager, vous pouvez afficher les recommandations relatives aux vulnérabilités qui sont publiées par les fournisseurs de logiciels. Utilisez-les pour identifier les risques de votre technologie et comprendre leurs implications.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur **Recherche** > **Recommandations**.
3. Si aucune recommandation ne s'affiche, sélectionnez une autre plage de temps dans la liste d'**affichage**.
4. Pour rechercher des instructions de sécurité, dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
5. Cliquez sur le lien vers la recommandation dans la colonne **Recommandation**.

   Chaque recommandation relative à la sécurité peut inclure des références aux vulnérabilités, des solutions et des méthodes pour y remédier.

Recherche de vulnérabilités, de nouvelles et d'avis

Dans IBM QRadar Vulnerability Manager, vous pouvez rechercher les nouvelles et les recommandations les plus récentes relatives aux vulnérabilités qui sont publiées par les fournisseurs de logiciels.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'une des options suivantes :
   - **Recherche** > **Vulnérabilités**.
   - **Recherche** > **Articles**.
   - **Recherche** > **Recommandations**.
3. Dans la barre d'outils, sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Entrez une phrase de recherche dans la zone **Phrase**.
5. Si vous recherchez des articles, sélectionnez une source d'articles dans la liste **Source**.
6. Dans la zone **Par plage de dates**, spécifiez la période de dates correspondant aux articles ou aux recommandations qui vous intéressent.
7. Si vous recherchez une vulnérabilité publiée, indiquez un fournisseur, un produit et une version de produit dans la zone **Par produit**.
8. Si vous recherchez une vulnérabilité publiée, indiquez un CVE, une vulnérabilité ou un ID OSVDB dans la zone **Par ID**.

Flux de nouvelles

Utilisez les éléments de tableau de bord **Flux RSS** pour voir les dernières informations de sécurité, les conseils, les informations sur la vulnérabilité publiées et les mises à jour IBM sur les analyses qui sont terminées ou en cours.

Les éléments du tableau de bord **Flux RSS** font tourner les 10 dernières nouvelles et résultats d'analyse de sorte que vous n'avez pas besoin de rechercher des informations dans les pages **Recherche** ou **Résultats d'analyse** sur l'onglet **Vulnérabilités**.

Dans l'onglet **Tableau de bord**, utilisez le menu **Ajouter un article** > **Rapports** > **Flux RSS** pour ajouter des flux RSS à votre tableau de bord.

Chapitre 19. IBM QRadar Vulnerability Manager Engine for OpenVAS Network Vulnerability Tests

IBM QRadar Vulnerability Manager (QVM) Engine for OpenVAS Network Vulnerability Tests (NVT) implémente la règle Full Scan Plus qui ajoute une dimension supplémentaire à l'analyse sans données d'identification.

A propos de QVM Engine for OpenVAS NVTs

Le projet open source OpenVAS fournit environ 50 000 tests de vulnérabilité réseau individuels via le flux de communauté. Ces tests individuels peuvent évaluer une vulnérabilité. QVM Engine for OpenVAS NVTs permet d'exécuter ces tests pendant une analyse QVM.

Fonctions

QVM Engine for OpenVAS NVTs installe une nouvelle règle d'analyse appelée Full Scan Plus, distincte de vos règles d'analyse existantes. Etant donné que cette règle inclut un plus grand nombre de tests de vulnérabilité, les analyses sont plus longues. Les analyses précédemment configurées utilisent Opencast Nets en plus des fonctions de QRadar Vulnerability Manager.

La règle Full Scan Plus inclut des milliers de tests de vulnérabilité supplémentaires fournis par le projet OpenVAS.

Les tests de vulnérabilité réseau sont mis à jour automatiquement toutes les nuits. Aucune configuration supplémentaire n'est requise.

Configuration requise

Pour QVM Engine for OpenVAS NVTs, vous devez disposer de QRadar 7.3.1, Patch 3 ou version ultérieure avec une licence QRadar Vulnerability Manager.

L'installation nécessite l'accès à la console et des mises à jour automatiques. Voir «Ajout de la règle d'analyse Full Scan Plus à IBM QRadar Vulnerability Manager», à la page 138.

Foire aux questions

QVM Engine for OpenVAS NVTs permet-il d'importer des vulnérabilités dans QRadar Vulnerability Manager à partir d'un déploiement OpenVAS autonome ?
Non. Ce plug-in permet à QVM d'exécuter des tests de vulnérabilité réseau OpenVAS lors des analyses QVM mais il n'est pas conçu pour permettre l'intégration à une instance d'OpenVAS fournie séparément.

La règle Full Scan Plus exécute-t-elle uniquement des tests de vulnérabilité réseau OpenVAS ?
Non. La règle Full Scan Plus utilise plusieurs tests d'analyse QVM avec les tests de vulnérabilité réseau pour garantir une couverture maximale.

A propos de la règle Full Scan Plus

Full Scan Plus exécute les tests de vulnérabilité réseau (NVT) OpenVAS ainsi que les outils de la règle Full Scan existante. Par conséquent, la détection des vulnérabilités est améliorée lorsque des analyses non authentifiées sont requises et que vous disposez de suffisamment de temps pour exécuter ces tests supplémentaires.

Remarque : Pour pouvoir utiliser cette règle d'analyse, vous devez installer la règle RPM Full Scan Plus.

© Copyright IBM Corp. 2012, 2020

Cette règle utilise un flux mis à jour quotidiennement d'environ 50 000 tests NVT individuels fournis par le projet open source OpenVAS.

Par défaut, la règle détecte les actifs réseau en utilisant une plage de ports d'analyse FAST. Une analyse authentifiée est exécutée lorsque des données d'identification sont fournies.

Une analyse complète est composée des phases suivantes :

Type d'analyse	Description
Analyse de reconnaissance.	Détecte les actifs réseau puis analyse les ports afin d'identifier les principales caractéristiques des actifs, comme par exemple le système d'exploitation, le type de périphérique, et les services. Les vulnérabilités ne sont pas analysées.
Analyse sans données d'identification	Vérifie les services n'ayant pas besoin de données d'identification, par exemple la lecture des bannières et des réponses en vue d'obtenir des informations de version, la date d'expiration des certificats SSL, le test des comptes par défaut et le test des réponses en vue de détecter les vulnérabilités. **Remarque :** L'analyse sans données d'identification complète constitue la fonction la plus puissante de l'analyse Full Scan Plus. Elle exécute un plus grand nombre de tests que la règle Full Scan (analyse complète) mise à disposition par la communauté open source. Cette analyse est plus détaillée que l'analyse complète mais elle est plus longue et utilise plus de ressources. Exécutez cette analyse pendant des périodes de faible activité de votre réseau, dans l'idéal la nuit ou pendant les week-ends.
Analyse avec données d'identification	QRadar Vulnerability Manager se connecte à l'actif et rassemble des informations sur l'inventaire d'application installé et la configuration requise et augmente ou supprime des vulnérabilités.

Ajout de la règle d'analyse Full Scan Plus à IBM QRadar Vulnerability Manager

Pour ajouter la règle d'analyse Full Scan Plus à IBM QRadar Vulnerability Manager, vous devez télécharger QVM Engine for OpenVAS NVTs RPM Package Manager (RPM) à partir d'IBM Fix Central et l'installer sur votre console IBM QRadar Console.

Avant de commencer

- Vérifiez que QRadar version 7.3.1, Patch 3 ou version ultérieure est installé.
- Vérifiez que le scanner et le processeur QRadar Vulnerability Manager sont activés.

Procédure

1. Téléchargez l'élément RPM à partir d'IBM Fix Central et sauvegardez-le dans le répertoire `/store/rpms` sur la console.
2. Entrez la commande suivante pour installer l'élément RPM dans la console QRadar Console :

   ```
   rpm -ivh /store/rpms/qvm-openvas-x.x-x.noarch.rpm
   ```

   Remarque : Dans un environnement à haute disponibilité, effectuez cette étape uniquement sur la console principale.
3. Entrez la commande suivante pour activer la règle d'analyse Full Scan Plus :

   ```
   /store/qvm/openvas/openvas_switch.sh enable
   ```

   Remarque : Procédez comme suit sur la console uniquement. Ainsi, la configuration est déployée dans l'ensemble du système. Aucune action n'est requise sur les hôtes gérés.
4. Exécutez des mises à jour automatiques en procédant comme suit :

a) Dans le menu de navigation (☰), cliquez sur **Admin**. pour ouvrir l'onglet d'administration.

b) Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.

c) Cliquez sur **Obtenir de nouvelles mises à jour**.

d) Si de nouvelles mises à jour apparaissent dans la liste, cliquez sur **Installer** > **Toutes les mises à jour**.

Important : Vous devez déclencher la mise à jour automatique pour effectuer l'installation de la règle Full Scan Plus. Des outils supplémentaires sont alors téléchargés et installés. La règle d'analyse sera disponible dans l'interface utilisateur une fois l'installation terminée. Vous devez effectuer cette étape même si la mise à jour automatique a déjà été effectuée pour le jour en cours.

Exécution d'une analyse

Suivez la procédure ci-dessous pour exécuter une analyse avec la règle Full Scan Plus.

Procédure

1. Configurez la nouvelle règle Full Scan Plus en fonction des besoins.

   Des instructions décrivant comment configurer une règle d'analyse sont présentées ci-dessous.
2. Créez un profil d'analyse et sélectionnez **Full Scan Plus** ou la règle que vous avez créée à l'étape 1 en utilisant le menu **Règles d'analyse**.

   Des instructions décrivant comment créer une règle d'analyse sont disponibles ci-dessous.

Configuration d'une politique d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une politique d'analyse pour répondre à toutes les exigences spécifiques de vos analyses de vulnérabilité. Vous pouvez copier et renommer une politique d'analyse préconfigurée ou vous pouvez ajouter une nouvelle politique d'analyse. Vous ne pouvez pas modifier une politique d'analyse préconfigurée.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, sélectionnez l'option d'**administration** > **Politiques d'administration d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Saisissez le nom et la description de votre politique d'analyse.

   Pour configurer une politique d'analyse, vous devez au moins configurer les zones obligatoires dans la fenêtre **New Scan Policy** qui sont les zones **Name** et **Description**.
5. Dans la liste **Scan Type**, sélectionnez le type d'analyse.
6. Pour gérer et optimiser le processus de reconnaissance d'actifs, cliquez sur l'onglet **Asset Discovery**.
7. Pour gérer les ports et les protocoles qui sont utilisés pour une analyse, cliquez sur l'onglet **Analyse du port**.
8. Pour inclure des vulnérabilités spécifiques dans votre politique d'analyse de correctifs, cliquez sur l'onglet **Vulnérabilités**.

   Remarque : L'onglet **Vulnérabilités** est disponible uniquement lorsque vous sélectionnez une analyse de correctif.
9. Pour inclure ou exclure des groupes d'outils de votre politique d'analyse, cliquez sur l'onglet **Tool Groups**.

   Remarque : L'onglet **Tool Groups** est disponible uniquement lorsque vous sélectionnez une politique sans donnée d'identification ou d'analyse complète (full-scan ou full-scan plus).

10. Pour inclure ou exclure des outils d'une politique d'analyse, cliquez sur l'onglet **Tools**.

    Remarque : Cet onglet est disponible uniquement lorsque vous sélectionnez une règle Full Scan Plus ou Full Scan sans données d'identification.

    Important : Si vous ne modifiez pas les outils ou les groupes d'outils, et que vous sélectionnez l'option **Full** comme type analyse, tous les outils et les groupes d'outils qui sont associés à une analyse complète sont inclus dans votre politique d'analyse.
11. Cliquez sur **Save**.

Création d'un profil d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer les profils d'analyse pour spécifier comment et quand les actifs de votre réseau seront analysés en vue de détecter des vulnérabilités.

Procédure

1. Cliquez sur l'onglet **Vulnérabilités**.
2. Dans le panneau de navigation, cliquez sur l'option d'**administration** > **Profils d'analyse**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.

   Lorsque vous créez un profil d'analyse, les seules zones obligatoires sont **Nom** et **Adresses IP** dans l'onglet **Détails** de la page **Configuration du profil d'analyse**. En outre, vous pouvez également configurer les paramètres facultatifs suivants.

   - Si vous avez ajouté d'autres scanners à votre déploiement QRadar Vulnerability Manager, sélectionnez un scanner de la liste **Serveur d'analyse**. Cette étape n'est pas nécessaire si vous souhaitez utiliser l'analyse dynamique.
   - Pour activer ce profil pour l'analyse à la demande, cliquez sur la case à cocher **Analyse à la demande activée**.

     En sélectionnant cette option, vous mettez à disposition le profil à utiliser si vous voulez déclencher une analyse en réponse à un événement de règle personnalisée. Elle permet également une analyse de vulnérabilité à la demande en utilisant le menu contextuel sur la page **Actifs**.
   - En sélectionnant la case **Sélection de serveur dynamique**, vous pouvez choisir le scanner disponible le plus approprié. Assurez-vous que vous définissez les scanners dans la page **Administrative** > **Scanners**.

     Les profils de sécurité doivent être mis à jour avec un domaine associé. Les restrictions de niveau domaine ne sont pas appliquées tant que les profils de sécurité ne sont pas mis à jour et les modifications ne sont pas déployées.
   - Pour analyser votre réseau en utilisant un jeu prédéfini de critères d'analyse, sélectionnez un type d'analyse dans la liste **Politiques d'administration d'analyse**.
   - Si vous avez configuré des données d'identification centralisées pour les actifs, sélectionnez la case à cocher **Utiliser les données d'identification centralisées**. Pour plus d'informations, voir *IBM QRadar Administration Guide*.
4. Cliquez sur **Sauvegarder**.

Concepts associés

Bande passante du réseau pour les analyses d'actifs simultanées
En ajustant la configuration de la bande passante du réseau, vous pouvez modifier le nombre d'actifs pouvant être analysés simultanément et le nombre d'outils de vulnérabilité pouvant être utilisés simultanément pour analyser les actifs. Certaines analyses utilisent plusieurs outils de vulnérabilité pour analyser, ce qui affecte le nombre d'actifs pouvant être analysés en même temps.

Analyse dynamique
Utilisez l'analyse dynamique dans IBM QRadar Vulnerability Manager pour associer les scanners individuels à une adresse IP, à des plages CIDR, à des plages d'adresses IP ou à un domaine que vous

spécifiez dans le profil d'analyse. L'analyse dynamique est particulièrement utile lorsque vous déployez plusieurs scanners. Par exemple, si vous déployez plus de 5 scanners, vous pouvez gagner du temps en utilisant l'analyse dynamique.

Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager

Politiques d'administration d'analyse

Analyses de vulnérabilité dynamiques

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une analyse afin d'utiliser certains programmes d'analyse des vulnérabilités pour des plages CIDR spécifiques dans votre réseau. Par exemple, vos programmes d'analyse pourraient n'avoir accès qu'à certaines zones de votre réseau.

Tâches associées

Association de programmes d'analyse des vulnérabilités à des plages CIDR

Dans IBM QRadar Vulnerability Manager, pour effectuer une analyse dynamique, vous devez associer des programmes d'analyse des vulnérabilités à différents segments de votre réseau.

Nouvelle analyse d'un actif à l'aide de l'option de menu contextuel

Configuration d'une politique d'analyse

Dans IBM QRadar Vulnerability Manager, vous pouvez configurer une politique d'analyse pour répondre à toutes les exigences spécifiques de vos analyses de vulnérabilité. Vous pouvez copier et renommer une politique d'analyse préconfigurée ou vous pouvez ajouter une nouvelle politique d'analyse. Vous ne pouvez pas modifier une politique d'analyse préconfigurée.

Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

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

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties tacites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Toute référence à ces informations sur des sites web non-IBM est fournie par souci de commodité uniquement et ne constitue en aucun cas une adhésion au contenu de ces sites web. Les documents sur ces sites web ne font pas partie des documents de ce produit IBM et l'utilisation de ces sites web se fait à vos propres risques.

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

© Copyright IBM Corp. 2012, 2020

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

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

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

Les données de performance et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

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

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

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 Etats-Unis et/ou dans certains autres pays.

Dispositions relatives à la documentation du produit

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

Applicabilité

Ces dispositions s'ajoutent à toute autre condition d'utilisation applicable au site Web IBM.

Utilisation personnelle

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ou publier tout ou partie de ces publications ou en produire des oeuvres dérivées sans le consentement exprès d'IBM.

Utilisation commerciale

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

Droits

Exception faite des droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, tacite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité en ligne

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des 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 à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/fr/fr, la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details/fr/fr ainsi que la page “IBM Software Products and Software-as-a-Service Privacy Statement” à l'adresse http://www.ibm.com/software/info/product-privacy.

Règlement général sur la protection des données

Il appartient à chaque entreprise de se conformer aux lois et réglementations, notamment relatives à la protection des données personnelles. Il relève de la seule responsabilité du client de consulter les services juridiques compétents aussi bien pour identifier et interpréter les lois et règlements susceptibles d'affecter son activité, que pour toute action à entreprendre pour se mettre en conformité avec ces lois et réglementations. Les produits, services et autres fonctionnalités décrits ici ne sont pas adaptés à toutes les situations client et ne pourront être proposés que sous réserve de disponibilité. IBM ne fournit ni audit ni conseil juridique, ni déclaration, ni garantie que ses services ou produits assurent au client d’être en conformité avec la loi.

Pour en savoir plus sur la mise en conformité d'IBM avec le RGPD, ainsi que sur nos offres et fonctionnalités liées au RGPD, visitez https://ibm.com/gdpr

Glossaire

Ce glossaire contient les termes des logiciels et des produits IBM QRadar Vulnerability Manager, et leur définition.

Les renvois suivants y sont utilisés :

- *Voir* renvoie d'un terme non privilégié au terme privilégié ou d'une abréviation à la forme complète.
- *Voir aussi* renvoie à un terme connexe ou contraire.

Pour d'autres termes et définitions, voir le site Web IBM Terminology (s'affiche dans une nouvelle fenêtre).

A

actif
Objet gérable qui est déployé ou destiné à être déployé dans un environnement opérationnel.

analyse à la demande
Analyse qui s'exécute uniquement si elle est lancée par l'utilisateur. Les types d'analyse sont notamment les analyses complètes, les analyses de découvertes, les analyses de correctifs, les analyses PCI, les analyses de bases de données et les analyses Web.

C

CDP
Voir dommages collatéraux potentiels.

chiffrement
En sécurité informatique, processus consistant à transformer les données en un format non intelligible afin que les données originales ne puissent pas être obtenues ou puissent l'être uniquement à l'aide d'un processus de déchiffrement.

CIDR
Voir routage CIDR.

client
Programme logiciel ou ordinateur qui demande des services à un serveur.

Common Vulnerability Scoring System (CVSS)
Système d'évaluation qui mesure la gravité d'une vulnérabilité.

conseil
Document qui contient des informations et une analyse sur une menace ou une vulnérabilité.

console
Interface Web à partir de laquelle un opérateur peut contrôler et observer le fonctionnement du système.

CVSS
Voir Common Vulnerability Scoring System.

© Copyright IBM Corp. 2012, 2020

D

DNS
Voir système de noms de domaine (DNS).

dommages collatéraux potentiels (CDP)
Mesure de l'impact possible d'une vulnérabilité exploitée à des fins malveillantes sur un actif physique ou sur une organisation.

F

fenêtre opérationnelle
Période de temps configurée pendant laquelle une analyse est autorisée à s'exécuter.

H

HA
Voir haute disponibilité.

haute disponibilité (HA)
Se dit d'un système en cluster reconfiguré en cas de défaillance d'un noeud ou d'un démon de telle sorte que les charges de travail puissent être redistribuées entre les autres noeuds du cluster.

I

infraction
Message envoyé ou événement généré en réponse à une condition surveillée. Par exemple, une infraction vous donne des renseignements informant de l'infraction d'une règle ou d'une attaque du réseau.

IP
Voir protocole IP.

L

liste d'exclusion d'analyse
Liste d'actifs, de groupes réseau et de plages CIDR ignorés par les analyses.

N

National Vulnerability Database (NVD)
Référentiel des données de gestion des vulnérabilités normalisé aux Etats-Unis.

niveau de gravité PCI
Niveau de risque que présente une vulnérabilité pour le secteur des cartes de paiement.

norme de sécurité pour les données de cartes bancaires (PCI DSS)
Standard de sécurité des informations mondial, édicté par le comité de normalisation PCI SSC (Payment Card Industry Security Standards Council). Il a été créé dans le but d'aider les organisations qui traitent des paiements par carte à prévenir les fraudes à la carte de crédit en mettant en place des contrôles accrus au niveau des données, ainsi qu'à en limiter l'exposition. Ce standard s'applique à l'ensemble des organisations qui détiennent, traitent ou transmettent des informations relatives aux titulaires de cartes portant le logo de l'une des marques de carte.

NVD
Voir National Vulnerability Database.

P

PCI DSS
Voir norme de sécurité pour les données de cartes bancaires.

processus de résolution
Processus d'affectation, de suivi et de correction des vulnérabilités qui ont été identifiées sur un actif.

profil d'analyse
Informations de configuration qui déterminent quand et comment les actifs sur un réseau sont analysés en vue de la détection des vulnérabilités.

protocole IP
Protocole qui achemine les données par le biais d'un réseau ou de réseaux interconnectés. Ce protocole sert d'intermédiaire entre les couches supérieures des protocoles et le réseau physique. Voir aussi protocole TCP.

R

règle de faux positif d'exception
Règle spécifique aux vulnérabilités à faible risque qui réduit le volume des vulnérabilités gérées.

routage CIDR
Méthode d'ajout d'adresses IP de classe C. Les adresses CIDR sont communiquées aux fournisseurs de services Internet (ISP) pour leurs clients. Elles diminuent la taille des tables de routage et augmentent le nombre d'adresses IP disponibles dans les organisations.

S

Simple Network Management Protocol (SNMP)
Groupe de protocoles de surveillance des systèmes et des unités dans des réseaux complexes. Les informations relatives aux unités gérées sont définies et stockées dans une base d'informations de gestion.

SNMP
Voir Simple Network Management Protocol (SNMP).

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

T

TCP
Voir Transmission Control Protocol (TCP).

transfert de zone DNS
Transaction qui permet de répliquer une base de données DNS (Domain Name System).

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

U

UDP
Voir User Datagram Protocol (UDP).

User Datagram Protocol (UDP)
Protocole Internet qui fournit un service de datagramme sans connexion et non fiable. Il permet à un programme d'application sur une machine ou un processus d'envoyer un datagramme à un autre programme d'application sur une autre machine ou processus.

V

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

Index

G

H

I

L

M

N

P

Q

R

S

T

U

V

W