IBM Security QRadar Vulnerability Manager
Version 7.2.6

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 103.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.2.6 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Présentation d'IBM Security QRadar Vulnerability Manager

Ces informations portent sur l'utilisation d'IBM® Security 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 Security QRadar SIEM ou une console IBM Security QRadar Log Manager.

Utilisateurs concernés

Les administrateurs système responsables de la configuration d'IBM Security QRadar Vulnerability Manager doivent disposer d'un accès administratif à IBM Security 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 Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Contacter le service clients

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

Déclaration de pratiques de sécurité recommandées

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

Chapitre 1. Nouveautés pour les utilisateurs dans QRadar Vulnerability Manager version 7.2.6

IBM Security QRadar Vulnerability Managerversion 7.2.6 introduit des améliorations pour vous aider à contrôler les profils de sécurité de niveau domaine et à identifier les vulnérabilités de priorité élevée.

Améliorez votre situation en matière de sécurité en intégrant IBM BigFix à QRadar Vulnerability Manager

Utilisez QRadar Vulnerability ManageravecBigFix pour identifier les vulnérabilités de priorité élevée et déterminer celles qui doivent être corrigées en premier. Des fixlets sont des packages prêts à l'emploi que vous pouvez déployer pour éliminer des failles spécifique. QRadar Vulnerability Manager peut publier automatiquement les données de vulnérabilité de priorité élevée dans le tableau de bord de BigFix. Les utilisateurs peuvent facilement contrôler et corriger les vulnérabilités à partir d'BigFix qui sont classées par QRadar Vulnerability Manager.

En savoir plus...

Prise en charge des environnements multi-domaine

Utilisez les droits d'accès de profil de sécurité de niveau domaine pour vous assurer que le niveau d'accès approprié est en place pour les analyses de vulnérabilité. Vous pouvez maintenant associer un scanneur à un domaine, utiliser un domaine pour l'analyse dynamique, associer un domaine à un profil d'analyse et un résultat d'analyse, voir les ressources d'un domaine qui sont associées à une analyse, filtrer les rapports d'analyse par domaine et n'afficher que les résultats de l'analyse et les vulnérabilités qui se trouvent dans les domaines associés à votre profil de sécurité.

Chapitre 2. Installations et déploiements de QRadar Vulnerability Manager

L'onglet **Vulnérabilités** vous permet d'accéder à IBM Security QRadar Vulnerability Manager.

Accès à l'onglet Vulnérabilités

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

- 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.
- Selon le mode de mise à niveau de QRadar choisi, il est possible que l'onglet **Vulnérabilités** ne s'active pas.

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* de votre produit.

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

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 programme d'analyse des vulnérabilités vers un Collecteur d'événements 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.

Important : 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.**

Vérifiez que Java™ Runtime Environment (JRE) version 1.7 ou IBM 64-bit Runtime Environment for Java V7.0 est installé sur tous les systèmes de bureau que vous utilisez pour accéder à l'interface utilisateur du produit de QRadar.

Concepts associés:

«Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager», à la page 7
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 Security QRadar Vulnerability Manager.

«Options de déplacement du processeur de vulnérabilité dans votre déploiement QRadar Vulnerability Manager», à la page 5
Si nécessaire, vous pouvez déplacer le processeur de vulnérabilité de votre console QRadar vers un dispositif d'hôte géré QRadar Vulnerability Manager dédié.

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 Security QRadar SIEM pour sauvegarder et restaurer les données de vulnérabilité et de configuration de IBM Security 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 récupération, voir *IBM Security QRadar SIEM Administration Guide*.

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. Installer un dispositif de processeur QRadar Vulnerability Manager dédié.
2. Ajoutez le dispositif de processeur d'hôte géré à votre 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 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. Cliquez sur l'onglet **Admin**.
3. Dans le panneau **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. À 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 de l'hôte et le mot de passe.
6. Cliquez sur **Ajouter**.
7. Fermez la fenêtre Gestion du système et de la licence.
8. Dans la barre d'outils de l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.
9. Cliquez sur **OK**.

Concepts associés:

«Processeur de vulnérabilité et clés d'activation de dispositif de programme d'analyse», à la page 4
Vous pouvez analyser et traiter vos vulnérabilités à l'aide de dispositifs d'hôtes gérés QRadar Vulnerability Manager dédiés.

Tâches associées:

«Vérification du déploiement d'un processeur de vulnérabilité», à la page 7
Dans IBM Security QRadar Vulnerability Manager, vous pouvez vérifier que votre processeur de vulnérabilité est déployé sur une console QRadar ou un hôte géré QRadar Vulnerability Manager.

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 l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
2. Cliquez sur **Activer le processeur**.

3. Sélectionnez l'hôte géré ou la console dans la liste **Processeurs**.

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

Concepts associés:

«Processeur de vulnérabilité et clés d'activation de dispositif de programme d'analyse», à la page 4
Vous pouvez analyser et traiter vos vulnérabilités à l'aide de dispositifs d'hôtes gérés QRadar Vulnerability Manager dédiés.

Vérification du déploiement d'un processeur de vulnérabilité

Dans IBM Security 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 l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
3. 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 l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gestion du déploiement de vulnérabilité**.
3. Cochez la case **Activer le processeur** pour la désélectionner.
4. Cliquez sur **Retirer**.
5. Cliquez sur **Sauvegarder**.
6. Fermez la fenêtre Gestion du système et de la licence.
7. Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.
8. 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 Security 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 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 programme 'analyse des vulnérabilités à des hôtes gérés QRadar préexistants dans votre déploiement. Par exemple, un collecteur de flux, un processeur de flux ou un processeur d'événement.

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», à la page 58
Dans IBM Security 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», à la page 59
Dans IBM Security 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» , à la page 60
Dans IBM Security 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 l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Ajouter un hôte géré**.
2. Entrez l'adresse IP de l'hôte et le mot de passe du dispositif de scanner de l'hôte géré QRadar Vulnerability Manager.
3. Cliquez sur **Ajouter**.

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

Concepts associés:

«Processeur de vulnérabilité et clés d'activation de dispositif de programme d'analyse», à la page 4
Vous pouvez analyser et traiter vos vulnérabilités à l'aide de dispositifs d'hôtes gérés QRadar Vulnerability Manager dédiés.

Déploiement d'un programme d'analyse des vulnérabilités vers une console ou un hôte géré QRadar

Vous pouvez déployer un programme d'analyse QRadar Vulnerability Manager vers une console QRadar ou un hôte géré QRadar. Par exemple, un collecteur de flux, un processeur de flux, un collecteur d'événement ou un processeur d'événement.

Avant de commencer

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 l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
2. Cliquez sur **Ajouter des scanners de vulnérabilité supplémentaires**.

3. Cliquez sur l'icône **+**.
4. 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.
5. Cliquez sur **Sauvegarder**.
6. Fermez la fenêtre Gestion du système et de la licence.
7. Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.
8. Cliquez sur **OK**.
9. Consultez la liste **Serveur d'analyse** sur la page Configuration de profil d'analyse pour vérifier que le scanner a été ajouté.

   Pour plus d'informations, voir «Création d'un profil d'analyse», à la page 31.

Que faire ensuite

Exécutez une mise à jour automatique après avoir ajouté le scanner ou d'autres hôtes gérés avec des fonctions de numérisation. Vous pouvez également procéder à une analyse après que la mise à jour automatique quotidienne s'est exécutée.

Tâches associées:

«Déplacement de votre processeur de vulnérabilité sur un hôte géré ou une console», à la page 6
Si nécessaire, vous pouvez déplacer votre processeur de vulnérabilité entre un dispositif d'hôte géré QRadar Vulnerability Manager et votre console QRadar.

Analyse des actifs de votre zone démilitarisée

Dans IBM Security 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.

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

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

Procédure

1. Configurez un accès Internet sortant sur le port 443.

2. Envoyez les informations suivantes à `QRadar-QVM-Hosted-Scanner@hursley.ibm.com` :
   - L'adresse IP externe de votre organisation.

     Restriction : L'adresse IP doit être configurée préalablement à l'exécution des analyses externes.
   - La plage d'adresse IP des actifs dans votre DMZ.

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 l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
2. Cliquez sur **Utiliser le scanner externe**.
3. 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.
4. Facultatif : Si votre réseau est configuré pour utiliser un serveur proxy, cliquez sur **Activer le serveur proxy**, entrez les détails de votre serveur.
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**.

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

Navigateurs Web pris en charge

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

Lorsque vous accédez au système QRadar, vous êtes invité à entrer un nom d'utilisateur et un mot de passe. Les noms d'utilisateur et mot de passe doivent être configurés à l'avance par l'administrateur.

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

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

Navigateur Web	Versions prises en charge
Mozilla Firefox	38.0 Extended Support Release
3Microsoft Internet Explorer 32 bits avec les modes Document et Navigateur activés	10.0 11.0

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

Navigateur Web	Versions prises en charge
Google Chrome	Version 46

Activation du mode document et du mode navigateur dans Internet Explorer

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

Procédure

1. Dans votre navigateur Web Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre des Developer Tools.
2. Cliquez sur **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.

Extension de la période de licence temporaire QRadar Vulnerability Manager

Par défaut, lorsque vous installez IBM Security 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 l'onglet **Admin**, cliquez sur l'icône **Vulnerability Manager** dans la zone **Essayer**.
2. 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.

Chapitre 3. IBM Security QRadar Vulnerability Manager

IBM Security 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.

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

analyse des vulnérabilités

Dans IBM Security 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 le planning d'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.

Concepts associés:

«Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager», à la page 7
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 Security QRadar Vulnerability Manager.

«Options de déplacement du processeur de vulnérabilité dans votre déploiement QRadar Vulnerability Manager», à la page 5
Si nécessaire, vous pouvez déplacer le processeur de vulnérabilité de votre console QRadar vers un dispositif d'hôte géré QRadar Vulnerability Manager dédié.

Initiation à l'analyse de vulnérabilité

La configuration initiale du système IBM Security QRadar Vulnerability Manager pour la gestion de réseau et de la vulnérabilité requiert une planification systématique.

Il existe trois zones clés à prendre en compte lorsque vous utilisez QRadar Vulnerability Manager pour l'examen de la vulnérabilité :

- Le type d'analyse à exécuter et sa fréquence d'exécution.
- Le nombre de scanners à déployer et le nombre d'actifs à examiner à tout moment.
- Comment gérer les vulnérabilités détectées.

Types d'analyse

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

Les modèles les plus couramment utilisés sont les suivants :

Analyse de reconnaissance
Découvre les ressources réseau. Analyse ensuite les ports pour identifier des caractéristiques d'actifs clés, telles que le système d'exploitation, le type de périphérique, et des services fournis par l'actif. Les vulnérabilités ne sont pas analysées.

Analyse complète
Découvre des actifs réseau qui utilisent une plage de ports d'analyse rapide. Exécute un examen de port pouvant être configuré par l'utilisateur et un examen non authentifié des services reconnus comme FTP, Web, SSH et base de données. Si les données d'identification sont fournies, une analyse authentifiée est effectuée.

Analyse de correctif
Explore le réseau pour identifier les actifs, puis effectue une analyse rapide de port et un examen des données d'identification des actifs.

Analyses de reconnaissance

Une analyse de reconnaissance est une analyse sans données d'identification simple. Elle recherche un espace d'adresse pour les adresses IP actives, puis scanne leurs ports. Elle effectue des recherches DNS et NetBIOS pour découvrir quel système d'exploitation des actifs exécutent, quels services ouverts ils fournissent, et tous les noms de réseau qui leur sont assignés.

Généralement, vous effectuez des analyses de reconnaissance fréquemment. Elles s'exécutent souvent par semaine pour assurer une bonne visibilité des actifs du réseau et des informations sur les actifs, tels que les noms d'actifs, le système d'exploitation et les services ouverts, pour les utilisateurs SIEM et SOC.

Analyses complètes

Une analyse complète exécute la suite complète de tests QRadar Vulnerability Manager.

Une analyse complète comprend ces phases :

1. Une analyse de reconnaissance
2. Des vérifications sans données d'identification. Vérifie les services qui ne nécessitent pas de données d'identification, par exemple, la lecture des bannières et des réponses pour les informations de version, l'expiration de certificats SSL, test de comptes par défaut, test de réponses pour les vulnérabilités.
3. Des vérifications avec données d'identification. QRadar Vulnerability Manager se connecte à l'actif et recueille l'inventaire d'applications installées et la configuration requise et augmente (ou supprime) les vulnérabilités selon le cas. Les analyses authentifiées sont préférables aux analyses non authentifiées. Des analyses non authentifiées donnent un aperçu utile de la posture de vulnérabilité du réseau. L'analyse authentifiée, toutefois, est indispensable à un programme de gestion de vulnérabilité efficace et complet.

Remarque : Les analyses complètes peuvent parfois bloquer certains comptes d'administration, par exemple, SQL Server, lorsque QRadar Vulnerability Manager teste plusieurs informations d'identification par défaut sur ces comptes.

Analyse de correctifs

Vous utilisez des analyses de correctifs afin de déterminer quels correctifs et produits sont installés ou manquants sur le réseau.

Une analyse des correctifs comporte deux phases principales :

- Une analyse de reconnaissance
- Des vérifications sans données d'identification

Les analyses de correctifs s'exécutent plus rapidement et ont un impact moindre sur le réseau et les actifs en cours d'analyse parce qu'ils n'effectuent pas de contrôles sans données d'identification.

Moment de l'analyse

Ce qui suit est un calendrier typique pour chaque type d'analyse :

- Analyse de reconnaissance – Exécution hebdomadaire

- Analyse de correctif – Exécution toutes les 1 à 4 semaines
- Analyse complète – Exécution tous les 2 à 3 mois

Concepts associés:

«Planning d'analyse», à la page 37
Dans IBM Security QRadar Vulnerability Manager, vous pouvez planifier les dates et heures d'analyse de vos ressources réseau à la recherche des vulnérabilités connues.

Chapitre 5, «Analyse des vulnérabilités», à la page 31
Dans IBM Security 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.

«Règles d'analyse», à la page 60
Une politique d'administration d'analyse fournit un emplacement centralisé pour la configuration d'exigences d'analyse spécifiques.

Tâches associées:

«Création d'un profil d'analyse», à la page 31
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les profils d'analyse pour spécifier comment et quand les actifs de votre réseau sont analysés pour la recherche de vulnérabilités.

Déploiements de scanner à distance

Vous pouvez déployer un nombre illimité de scanners distants dans un réseau.

Lorsque vous concevez un déploiement du scanner à distance, vous devez considérer les facteurs suivants :

- Nombre d'actifs que vous devez scanner.
- Connectivité réseau entre le IBM Security QRadar Vulnerability Manager et les actifs qu'il analyse.
- Bande passante de réseau requise.
- Si vous souhaitez utiliser la numérisation dynamique.
- Combien de cartes d'interface réseau (NIC) à utiliser sur un scanner.

Scanners et actifs

Il n'y a pas de limite au nombre d'actifs que le scanner peut analyser, en principe. Chaque scanner a une bande passante et les demandes d'analyse sont en file d'attente lorsque cette bande passante est pleine.

Plus les actifs à analyser sont nombreux, plus l'analyse est longue. Par exemple, le déploiement des scanners pour numériser jusqu'à 4000 à 5000 actifs aboutit à des durées d'analyse acceptables (2 à 3 jours maximum).

Connectivité entre scanner et actifs

En général, évitez l'analyse à travers les pare-feux et sur des connexions WAN à faible bande passante.

Les instructions suivantes sont utiles :

- Gardez la charge faible sur vos pare-feux.

- Réduisez le risque d'interférence du pare-feu avec l'analyse. Par exemple, ne permettez pas que le pare-feu bloque les ports qui sont nécessaires pour effectuer l'analyse.
- Veillez à ce que vos analyses s'exécutent aussi vite que possible.
- Veillez à ce que la faible connectivité WAN n'affecte pas négativement vos analyses.

Paramètres de limite de la bande passante

Vous pouvez configurer la bande passante du réseau par profil de numérisation dans IBM Security QRadar Vulnerability Manager.

Lorsque vous augmentez la bande passante du réseau par profil d'analyse, QRadar Vulnerability Manager analyse plus d'outils de vulnérabilité en parallèle et donc les analyses s'exécutent plus rapidement. Vous pouvez régler la limite de bande passante sur la page Configuration d'analyse de profil. Les options suivantes sont disponibles :

Option	Paramètre de limite de la bande passante
Faible	100 kb/s
Moyen	1000 kb/s (valeur par défaut)
Elevé	5000 kb/s
Complet	maximum réseau

Si vous analysez des liaisons en bande passante limitée, n'augmentez pas la bande passante réseau à plus de 1000 kb/s. En règle générale, lorsque l'analyse de correctifs a un réglage **Moyen**, l'analyse de correctifs QRadar Vulnerability Manager analyse 10 actifs en parallèle. Avec un paramètre **Elevé**, 50 actifs sont analysés en parallèle.

Concepts associés:

«Détails relatifs au profil d'analyse», à la page 35
Dans IBM Security QRadar Vulnerability Manager, vous pouvez décrire votre analyse, sélectionner le scanner à utiliser, ainsi qu'un certain nombre d'options de politique d'analyse.

Tâches associées:

«Création d'un profil d'analyse», à la page 31
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les profils d'analyse pour spécifier comment et quand les actifs de votre réseau sont analysés pour la recherche de vulnérabilités.

Analyse dynamique

Dans l'analyse dynamique, IBM Security QRadar Vulnerability Manager sélectionne un scanner en fonction de l'adresse IO à examiner.

L'analyse dynamique réduit le nombre de travaux d'analyse que vous devez configurer. Par exemple, si vous déployez 10 scanners QRadar Vulnerability Manager et que vous n'utilisez pas l'analyse dynamique, vous devez configurer 10 travaux d'analyse individuels. Vous devez sélectionner un scanner par travail d'analyse. Si vous utilisez l'analyse dynamique, vous pouvez configurer un seul travail d'analyse pour utiliser 10 scanners en associant tous les plages CIDR avec chaque scanner. QRadar Vulnerability Manager sélectionne le scanner approprié pour chaque adresse IP en cours d'analyse.

L'analyse dynamique est particulièrement utile lorsque vous déployez plusieurs scanners. Si vous avez, par exemple, plus de 5 scanners, l'analyse dynamique vous permet de gagner du temps. En règle générale, n'activez pas l'analyse dynamique lorsque vous effectuez la configuration initiale de vos analyses de test. Vous pouvez passer à l'analayse dynamique lorsque vous êtes satisfait des résultats et des durées d'analyse.

Concepts associés:

«Analyses de vulnérabilité dynamiques», à la page 58
Dans IBM Security 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:

«Création d'un profil d'analyse», à la page 31
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les profils d'analyse pour spécifier comment et quand les actifs de votre réseau sont analysés pour la recherche de vulnérabilités.

Cartes d'interface réseau sur les scanneurs

Dans IBM Security QRadar Vulnerability Manager, l'analyse n'est pas dépendante des cartes d'interface réseau (NIC) qui sont configurées sur le dispositif de scanneur.

Vous pouvez configurer plusieurs cartes NIC, bien que 4 à 5 NIC est 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'examen suit la configuration réseau standard sur une appliance.

Présentation de la gestion des vulnérabilités

IBM Security QRadar Vulnerability Manager fournit un processus pour gérer les vulnérabilités basées sur l'affectation des propriétaires de l'actif.

Vous pouvez configurer des propriétaires d'actif sur la page Affectation des vulnérabilités de l'onglet **Vulnérabilités** ou à l'aide d'une api. Une fois les actifs affectés, des vulnérabilités détectées sur les actifs sont affectées à ces utilisateurs ou groupes avec une date d'échéance basée sur le niveau de risque des vulnérabilités en question. Vous pouvez également configurer les dates d'exigibilité et le niveau de risque dans la page Affectation de vulnérabilité. Vous pouvez alors configurer des rapports de résolution à envoyer à ces utilisateurs sur une période donnée. Utilisez les rapports de résolution pour mettre en évidence les actions suivantes :

- Les correctifs que vous devez installer.
- Les étapes que vous devez suivre pour corriger la vulnérabilité.
- La vulnérabilité des actifs en retard.
- Les nouvelles vulnérabilités qui ont été reconnues depuis la dernière analyse.

Les rapports de résolution standard sont disponibles dans l'onglet **E-mail** de la page Configuration de profil d'analyse. Vous pouvez créer des rapports client supplémentaires à l'aide de recherches QRadar Vulnerability Manager. Utilisez un large éventail de critères de recherche afin de vous assurer que les rapports soient concentrés sur les activités de la résolution de vulnérabilité nécessaires pour répondre aux besoins de votre entreprise et de la conformité.

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

Lorsque les actifs sont réanalysés, des vulnérabilités résolues sont automatiquement détectées et signalées comme corrigées. Elles sont supprimées des rapports et des vues, sauf si des droits ont été explicitement configurés autrement. Les vulnérabilités précédemment corrigées et à nouveau détectées sont automatiquement rouvertes.

Concepts associés:

Chapitre 10, «Rapports de vulnérabilités», à la page 93
Dans IBM Security 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.

Tâches associées:

«Affectation d'un utilisateur technique comme propriétaire des groupes d'actifs», à la page 89
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer des groupes d'actifs et affecter automatiquement leurs vulnérabilités à des utilisateurs techniques.

«Configuration des délais de résolution pour les vulnérabilités dans les actifs affectés», à la page 91
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les délais de résolution des différents types de vulnérabilités.

«Envoi d'un e-mail aux propriétaires d'actif lors du démarrage et de l'arrêt des analyses de vulnérabilité», à la page 69
Envoyez un e-mail aux propriétaires techniques d'actif afin de les informer du planning d'analyse. Vous pouvez aussi envoyer des rapports aux propriétaires d'actif .

«Recherche des données de vulnérabilité», à la page 72
Dans IBM Security QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités importantes en recherchant vos données de vulnérabilité.

Tableau de bord de gestion des vulnérabilités

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

IBM Security 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. Facultatif : 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**.

Tâches associées:

«Enregistrement des critères de recherche de vulnérabilité», à la page 77
Dans IBM Security QRadar Vulnerability Manager, vous pouvez enregistrer vos critères de recherche de vulnérabilité pour une utilisation ultérieure.

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. Intégrations de logiciels de sécurité

IBM Security 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 d'QRadar Risk Manager et d'QRadar Vulnerability Manager

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

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 Security QRadar Risk Manager - Guide d'installation*.

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 du risque que vous définissez dans QRadar Risk Manager réussissent ou échouent, les scores du 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 Security QRadar Risk Manager - Guide d'utilisation*.

Tâches associées:

«Hiérarchisation des vulnérabilités à haut risque par l'application de règles du risque», à la page 81
Dans IBM Security QRadar Vulnerability Manager, vous pouvez signaler aux administrateurs les vulnérabilités à haut risque en appliquant à vos vulnérabilités

des règles du risque.

Intégration de BigFix

IBM Security QRadar Vulnerability Manager s'intègre à IBM BigFix afin de vous permettre de filtrer et de hiérarchiser les vulnérabilités pouvant être corrigées.

Fonctionnalités BigFix

Précédemment appelé IBM Security Endpoint Manager, BigFix offre une visibilité et un contrôle partagés entre les opérations informatiques et la sécurité. BigFix identifie les vulnérabilités de haute priorité et détermine celles qui nécessitent prioritairement des fixlets. Des fixlets sont des packages que vous pouvez déployer pour éliminer des failles spécifique. Les fixlets résolvent les problèmes et corrigent les vulnérabilités rapidement et efficacement. A partir de la console d'BigFix, vous pouvez déployer simultanément des fixlets sur un très grand nombre de terminaux ou d'actifs.

A partir d'une seule console, BigFix vous offre la possibilité de gérer et de contrôler un réseau de centaines de milliers de terminaux ou d'actifs à travers une gamme de plateformes et de périphériques, quelle que soit leur localisation géographique.

BigFix est utilisé pour la découverte d'actifs et la gestion des correctifs, la distribution de logiciels, l'inventaire des logiciels et la surveillance de l'utilisation des logiciels, la gestion du cycle de vie du système, le respect de la sécurité et l'exécution constante.

Intégration de QRadar Vulnerability Manager à BigFix

BigFix fournit un tableau de bord qui est intégré à QRadar Vulnerability Manager. Vous pouvez utiliser le tableau de bord pour corriger les vulnérabilités détectées par QRadar Vulnerability Manager.

Pour activer cette connexion et afficher les données QRadar Vulnerability Manager dans la console BigFix, vous devez effectuer les étapes de configuration dans QRadar Vulnerability Manager.

Séparément, vous devez exécuter certaines étapes de configuration dans BigFix pour traiter les données reçues de QRadar Vulnerability Manager. Pour plus d'informations sur la manière d'exécuter les étapes de configuration dans BigFix, voir *IBM BigFix QRadar User Guide*.

Résolution des vulnérabilités

Selon que vous avez installé et intégré BigFix, QRadar Vulnerability Manager fournit différents types d'informations pour vous aider à corriger vos vulnérabilités.

- Si BigFix n'est pas installé, QRadar Vulnerability Manager fournit des informations sur les vulnérabilités pour lesquelles un correctif est disponible.

  QRadar Vulnerability Manager assure la maintenance d'une liste d'informations de correctif des vulnérabilités. Ces informations sont corrélées au catalogue des vulnérabilités connues.

  Grâce à la fonction de recherche de QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités pour lesquelles un correctif est disponible.

- Si BigFix est installé, QRadar Vulnerability Manager fournit également des informations spécifiques sur le processus de correction des vulnérabilités. Par exemple, un correctif peut être planifié ou un actif peut déjà avoir été corrigé.

  Le serveur BigFix collecte les informations de correctif auprès de chacun des agents BigFix. Les informations d'état de correctif sont envoyées à QRadar Vulnerability Manager selon des intervalles de temps préconfigurés.

  Avec la fonction de recherche de QRadar Vulnerability Manager, vous pouvez identifier rapidement les vulnérabilités dont le correctif est planifié ou qui sont déjà corrigées.

Composants d'intégration

Une intégration standard comprend généralement les composants suivants :

- Une console IBM Security QRadar.
- Une installation sous licence de QRadar Vulnerability Manager.
- Une installation du serveur BigFix.
- Une installation d'agent BigFix sur chacune des cibles d'analyse de votre réseau.

Il existe deux façons différentes d'intégration de QRadar Vulnerability Managerà BigFix :

- Configurez BigFix pour l'intégrer à QRadar Vulnerability Manager de sorte que les informations de BigFix soient envoyées à QRadar Vulnerability Manager. Cette configuration nécessite une communication SSL.
- Configurez QRadar Vulnerability Manager pour l'intégrer à BigFix de sorte que les informations soient envoyées de QRadar Vulnerability Manager vers BigFix.

Tâches associées:

«Identification de l'état de correctif des vulnérabilités», à la page 83
Dans IBM Security QRadar Vulnerability Manager, vous pouvez identifier l'état de correctif de vos vulnérabilités.

Configuration de BigFix pour envoyer des informations à QRadar Vulnerability Manager

Vous pouvez configurer IBM BigFix pour l'intégrer à IBM Security QRadar Vulnerability Manager. Dans ce scénario, les informations sont envoyées de BigFix vers QRadar Vulnerability Manager.

Cette configuration nécessite la communication SSL et des étapes de configuration de l'adaptateur BigFix.

Avant de commencer

Les composants suivants doivent être installés sur votre réseau :

- Serveur BigFix.
- Agent BigFix dans chaque actif de votre réseau faisant partie de l'analyse.

Si vous utilisez le chiffrement SSL (Secure Socket Layer), vérifiez que SSL est configuré pour l'intégration avec BigFix.

Procédure

1. Pour configurer la communication SSL, procédez comme suit :
   a. Téléchargez le certificat de clé publique, ouvrez votre navigateur Web et saisissez `https://`*`adresse_IP_serveur_BigFix`*`/webreports`

b. Cliquez sur **Add Exception**, et dans la fenêtre Add Security Exception, cliquez sur **View**.
c. Cliquez sur l'onglet **Details**, puis sur **Export**.
d. Dans la zone **File name**, entrez `iemserver_cert.der`
e. Dans la zone **Save as type**, sélectionnez **X.509 Certificate (DER)** et cliquez sur **Save**.
f. Copiez le certificat de clé publique sur votre console QRadar.
g. Pour créer un fichier de clés certifiées QRadar Vulnerability Manager, utilisez SSH pour vous connecter à la console QRadar en tant qu'utilisateur root.

   Entrez la commande suivante : `keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias iem`

   Aux invites, entrez les informations appropriées pour créer le magasin de clés de confiance.
h. Pour importer le certificat de clé publique dans votre magasin de clés de confiance, entrez la commande suivante :

   `keytool -importcert -file iemserver_cert.der -keystore truststore.jks -storepass <votre_mot_de_passe_fichier_de_clés_certifiées> -alias iem_crt_der`
i. A l'invite **Trust this certificate?**, entrez **Yes**.

2. Pour configurer SSL et l'adaptateur BigFix pour QRadar Vulnerability Manager, procédez comme suit.
   a. Utilisez le protocole SSH pour vous connecter à la console QRadar comme utilisateur root.
   b. Accédez au répertoire à l'emplacement suivant :

      `/opt/qvm/iem`
   c. Entrez `./iem-setup-webreports.pl` et, lorsque vous y êtes invité, entrez les informations du serveur BigFix.
   d. Si vous utilisez SSL, à l'invite **Use SSL encryption?**, entrez la réponse appropriée.
   e. Entrez l'emplacement de votre magasin de clés de confiance.
   f. Entrez le mot de passe de votre magasin de clés de confiance.

Configuration de QRadar Vulnerability Manager pour envoyer des informations à BigFix

Dans cette option de configuration, IBM Security QRadar Vulnerability Manager envoie des informations à IBM BigFix. Cette option de configuration requiert un certain nombre d'étapes de configuration pour l'adaptateur BigFix, et certaines procédures de vérification.

Procédure

1. Connectez-vous au terminal IBM Security QRadar SIEM en tant que superutilisateur.
2. Pour configurer l'installation, procédez comme suit :
   a. Accédez à `/opt/qvm/adaptor/config` et exécutez le script de configuration `./setup-adaptor.sh`
   b. Entrez un nouveau mot de passe pour créer le fichier de clés certifiées qui est chargé de stocker les certificats.
   c. Aux invites, entrez les informations appropriées pour le serveur BigFix.

d. Redémarrez l'assetprofiler en accédant au répertoire `/opt/qradar/init` et en exécutant la commande suivante : `./assetprofiler restart`

   Pour assurer une performance optimale, ne redémarrez pas l'assetprofiler lorsque des analyses QRadar Vulnerability Manager sont en cours d'exécution ou lorsque vous attendez des importations de vulnérabilité depuis un scanner VIS tiers.

3. Pour vérifier que le processus d'installation a abouti, procédez comme suit :
   a. Dans le fichier `/opt/qvm/adaptor/config/adaptor.properties`, vérifiez que ces deux propriétés 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 à l'aide des propriétés suivantes, incluses dans le fichier `adaptor.properties` :

Tableau 2.

Nom de propriété	Description
`qvm.adaptor.minimum.asset.riskscore=n`	La propriété **`qvm.adaptor.minimum.asset.riskscore`** est la combinaison pondérée de tous les scores CVSS des vulnérabilités sur cet actif. Les actifs ayant un score inférieur à cette valeur ne sont pas envoyés vers BigFix.
`qvm.adaptor.assetupdate.limit=n`	La propriété **`qvm.adaptor.assetupdate.limit`** définit la façon dont les ressources de données de BigFix Dashboard sont divisées. Une scission n'interviendra pas avant que tous les ID CVE du dernier actif ne soient remplis. • Par exemple, si **`qvm.adaptor.assetupdate.limit=20`**, l'actif 1 contient 19 ID CVE, et l'actif 2 en contient 30. Une ressource de données est générée et contient les deux actifs, avec un total de 49 ID CVE. • Par exemple, si **`qvm.adaptor.assetupdate.limit=19`**, l'actif 1 contient 19 ID CVE, et l'actif 2 en contient 30. Deux ressources de données sont générées, chacune contenant un actif.
`qvm.adaptor.minimum.vuln.riskscore=n`	La propriété **`qvm.adaptor.minimum.vuln.riskscore`** définit le seuil de chaque score de risque de vulnérabilité. Ces vulnérabilités, égales à ou supérieures à la valeur définie, sont envoyées vers BigFix.

   c. Vérifiez que la configuration du plug-in BigFix a créé les répertoires suivants :
      - `/store/qvm/adaptor`
      - `/store/qvm/adaptor/data`
      - `/store/qvm/adaptor/bigfix`
   d. Vérifiez que la consignation est activée dans le fichier `log4j.xml`. Les fichiers journaux sont générés dans les fichiers `/var/log/qvm-integration-adaptor.log` et `/var/log/qvm-adaptor-cron.log`.

Traitement des problèmes de configuration d'BigFix

Vous pouvez résoudre les problèmes d'échec de connexion et de réinitialisation de mot de passe qui peuvent se produire lorsque vous configurez l'intégration de BigFix et QRadar Vulnerability Manager.

Echec de connexion au serveur IBM BigFix

Si un problème de connexion au serveur BigFix se produit, vous verrez peut-être le message d'erreur suivant :

```
ERREUR [TrustStoreConfig] Impossible de configurer le fichier de clés certifiées
avec des certificats homologues :
Connexion interrompue java.net.ConnectException : Connexion interrompue.
```

La configuration a abouti, mais elle ne dispose pas des certificats autorisés. Vous devez charger manuellement les certificats lorsque vous avez accès au serveur.

1. Accédez au répertoire `/store/qvm/adaptor`.
2. Exécutez le script de configuration : `./install-cert.sh` *<emplacement_fichier_de_clés_certifiées>* *<mot_de_passe_fichier_de_clés_certifiées>*<*adresse_IP_fichier_de_clés_certifiées:port*> Le port est le port de service auquel appartient le certificat.

Modification de mot de passe

Si vos détails BigFix changent, vous pouvez avoir besoin de modifier votre mot de passe.

1. Déchiffrez le mot de passe, entrez la commande suivante : `_decrypt.bes.rest.password=lUb5qzr7FIVH+J319erc+g==`.
2. Pour entrer un nouveau mot de passe, entrez la commande suivante : `_encrypt.bes.rest.password=`*nouveau_mot_de_passe*.
3. Exécutez le script suivant pour chiffrer votre nouveau mot de passe : `./password-property-encrypt.sh plugin-bigfix.properties`

Intégration de IBM Security SiteProtector

QRadar Vulnerability Manager s'intègre à IBM Security SiteProtector afin d'optimiser les règles du système de prévention des intrusions.

Lorsque vous configurez IBM Security SiteProtector, les vulnérabilités qui sont détectées par les analyses sont automatiquement transmises à SiteProtector.

IBM Security SiteProtector ne reçoit les données de vulnérabilité provenant des analyses QRadar Vulnerability Manager qu'après la configuration de l'intégration.

Connexion à IBM Security SiteProtector

Vous pouvez transmettre des données de vulnérabilité de IBM Security QRadar Vulnerability Manager à IBM Security SiteProtector afin de conduire la politique du système de prévention des intrusions.

Procédure

1. Dans l'onglet **Admin**, cliquez sur **Gestion du système et de la licence** > **Actions de déploiement** > **Gérer le déploiement de vulnérabilité**.
2. Cliquez sur **Utiliser SiteProtector**.

3. Dans la zone **Adresse IP SiteProtector**, entrez l'adresse IP du serveur du gestionnaire de l'agent IBM Security SiteProtector.
4. Cliquez sur **Enregistrer**, puis sur **Fermer**.
5. Dans la barre d'outils de l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.
6. 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.

Chapitre 5. Analyse des vulnérabilités

Dans IBM Security 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», à la page 45
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.

Création d'un profil d'analyse

Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les profils d'analyse pour spécifier comment et quand les actifs de votre réseau sont analysés pour la recherche de 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 de 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 à cocher **Dynamic Server Selection**, vous pouvez choisir le scanner le plus approprié qui est disponible. 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 Security QRadar SIEM Administration Guide*.

4. Cliquez sur **Sauvegarder**.

Concepts associés:

«Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager», à la page 7
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 Security QRadar Vulnerability Manager.

«Règles d'analyse», à la page 60
Une politique d'administration d'analyse fournit un emplacement centralisé pour la configuration d'exigences d'analyse spécifiques.

«Analyses de vulnérabilité dynamiques», à la page 58
Dans IBM Security 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», à la page 59
Dans IBM Security 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», à la page 35
Dans IBM Security QRadar Vulnerability Manager, vous pouvez effectuer rapidement une nouvelle analyse d'un actif à l'aide de l'option de menu contextuel.

«Configuration d'une règle d'analyse pour gérer les analyses des vulnérabilités», à la page 62
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer une stratégie d'analyse pour contrôler vos analyses de vulnérabilité.

Création d'un profil d'analyse de scanner externe

Dans IBM Security 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 de 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 une **analyse complète** ou une **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 à cocher **Dynamic server selection**.

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

7. Sous l'onglet de **planification d'analyse**, définissez le planning d'exécution, l'heure de début d'analyse et les éventuelles périodes d'exécution définies.
8. Sous l'onglet **E-mail**, définissez les informations à envoyer à ropos d e 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», à la page 45
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.

Exécuter manuellement des profils d'analyse

Dans IBM Security 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 «Planning d'analyse», à la page 37.

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», à la page 35
Dans IBM Security QRadar Vulnerability Manager, vous pouvez décrire votre analyse, sélectionner le scanner à utiliser, ainsi qu'un certain nombre d'options de politique d'analyse.

Tâches associées:

«Gestion des résultats d'analyse», à la page 67
Dans IBM Security 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.

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

Dans IBM Security 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 QRadar, ou la vue d'actif de sous-reseau 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 de 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», à la page 79
Dans IBM Security QRadar Vulnerability Manager, vous pouvez afficher un récapitulatif des données relatives aux vulnérabilités regroupées par actif analysé.

Détails relatifs au profil d'analyse

Dans IBM Security 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 de profil d'analyse.

Vérifiez plus particulièrement les options suivantes :

Tableau 3. Options de configuration des détails de 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.
Dynamic server selection	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 «Règles d'analyse», à la page 60.

Concepts associés:

«Analyses de vulnérabilité dynamiques», à la page 58
Dans IBM Security 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.

«Règles d'analyse», à la page 60
Une politique d'administration d'analyse fournit un emplacement centralisé pour la configuration d'exigences d'analyse spécifiques.

Planning d'analyse

Dans IBM Security QRadar Vulnerability Manager, vous pouvez planifier les dates et heures d'analyse de vos ressources réseau à la recherche des vulnérabilités connues.

Pour cela, il existe un panneau permettant de **planifier l'analyse** à la page Configuration de 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 un planning d'analyse, vous pouvez l'affiner en configurant un intervalle d'analyse autorisé.

Tâches associées:

«Configuration d'un intervalle d'analyse autorisé», à la page 56
Dans IBM Security QRadar Vulnerability Manager, vous pouvez créer une fenêtre opérationnelle pour indiquer les heures auxquelles une analyse peut s'exécuter.

«Consultation des analyses planifiées au format agenda», à la page 39
Dans IBM Security QRadar Vulnerability Manager, l'agenda des analyses planifiées fournit un emplacement central auquel vous pouvez consulter des informations sur les analyses planifiées.

Analyser les domaines sur une base mensuelle

Dans IBM Security 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 de profil d'analyse. Pour configurer des analyses mensuelles, vous devez également suivre les étapes restantes de cette procédure.
4. Cliquez sur le panneau de **planification d'analyse**.
5. Dans la liste **Exécuter la planification**, sélectionnez **Mensuelle**.
6. Dans la zone **Heure de début**, sélectionnez l'heure de début et de fin 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. Facultatif : 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 Security 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 de 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 de **planification d'analyse**, 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», à la page 72
Dans IBM Security QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités importantes en recherchant vos données de vulnérabilité.

Consultation des analyses planifiées au format agenda

Dans IBM Security 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. Facultatif : 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. Facultatif : Double-cliquez sur une analyse planifiée pour modifier le profil d'analyse.

Cibles d'analyse réseau et exclusions

Dans IBM Security 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 de 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 de 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» , à la page 60
Dans IBM Security 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 Security 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», à la page 38
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les analyses planifiées des actifs réseau non analysés découverts récemment.

«Analyser les domaines sur une base mensuelle», à la page 37
Dans IBM Security QRadar Vulnerability Manager, Vous pouvez configurer un profil d'analyse des domaines de votre réseau tous les mois.

Exclusion d'actifs de toutes les analyses

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

Utilisez le panneau concernant **le mode d'analyse** sur la page Configuration de profil d'analyse pour définir les protocoles d'analyse et les ports à analyser.

Vous pouvez configurer les protocoles de port de votre profil d'analyse à l'aide des options suivantes :

Tableau 4. Options de protocole d'analyse et de port

Protocole	Description
TCP et UDP	Protocole d'analyse par défaut qui analyse les ports courants dans la plage 1 - 1024. **A faire :** Par rapport aux autres protocoles d'analyse, les protocoles TCP et UDP peuvent générer plus d'activité réseau.
TCP	Protocole d'analyse le plus courant. Lorsque l'analyse TCP est associée à l'analyse de la plage IP, vous pouvez localiser un hôte qui exécute des services exposés à des vulnérabilités. La plage de ports par défaut est 1 - 65535.

Tableau 4. Options de protocole d'analyse et de port (suite)

Protocole	Description
SYN	Envoie un paquet à tous les ports spécifiés. Si la cible est en mode écoute, elle répond avec un caractère de synchronisation et un accusé de réception (ACK). Si la cible ne l'est pas, elle répond avec une table de services remédiable (réinitialisation). en principe, le port de destination est fermé et une table de services remédiable est renvoyée. La plage de ports par défaut est 1 - 65535.
ACK	Similaire à SYN, mais dans ce cas un indicateur ACK est défini. L'analyse ACK ne permet pas de déterminer si le port est ouvert ou fermé, mais permet de tester s'il est filtré ou non filtré. Le test de port est utile lorsque vous recherchez l'existence d'un pare-feu et ses ensembles de règles. Le filtrage simple de module active des connexions établies (modules associés au bit ACK défini), tandis qu'un pare-feu plus sophistiqué ne peut le faire. La plage de port par défaut est 1-65535.
FIN	Paquet TCP utilisé pour interrompre une connexion, ou utilisé en tant que méthode pour identifier les ports ouverts. FIN envoie des modules erronés vers un port et attend que les ports d'écoute ouverts renvoient des messages d'erreur différents des ports fermés. Le scanner envoie un module FIN, ce qui peut interrompre une connexion ouverte. Les ports fermés répondent à un module FIN à l'aide de RST. Les ports ouverts ignorent le module en question. La plage de port par défaut est 1 - 65535.

Analyser une plage entière de port

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

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 de profil d'analyse. Pour analyser une plage complète des ports, vous devez également suivre les étapes restantes de cette procédure.
4. Cliquez sur le panneau concernant le **mode d'analyse**.
5. Dans la zone **Protocole**, acceptez les valeurs par défaut de **TCP & UDP**.
6. 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).
7. 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.

8. Cliquez sur **Sauvegarder**.
9. Dans la page Profils d'analyse, cliquez sur **Exécuter**.

Analyser les actifs avec des ports ouverts

Dans IBM Security 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 de 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 de **planification d'analyse**, 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, «Exécuter manuellement des profils d'analyse», à la page 34.

Analyse des correctifs authentifiés

Dans IBM Security 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.

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 de correctif Windows retourne 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`.

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 à analyser.

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», à la page 46
Pour analyser les systèmes d'exploitation Linux avec l'authentification par clé publique sécurisée, vous devez configurer la console IBM Security 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.

«Configuration d'une analyse authentifiée des systèmes d'exploitation Linux ou UNIX», à la page 47
Dans IBM Security 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.

«Configuration d'une analyse authentifiée du système d'exploitation Windows», à la page 49
Dans IBM Security 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.

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», à la page 47
Dans IBM Security 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.

«Configuration d'une analyse authentifiée du système d'exploitation Windows», à la page 49
Dans IBM Security 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.

«Création d'un profil de test de performances», à la page 33
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 Security 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. Cliquez sur l'onglet **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. Facultatif : 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 Security 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 configurer la clé publique sur le périphérique sur lequel le programme de traitement des vulnérabilités est installé. Pour plus d'informations, voir «Vérification du déploiement d'un processeur de vulnérabilité», à la page 7.

Procédure

1. Avec le protocole SSH, connectez-vous à la console QRadar ou à l'hôte géré comme utilisateur root.
2. Générez un paire de clés DSA publiques en entrant la commande suivante :

   ```
   su -m -c 'ssh-keygen -t dsa' qvmuser
   ```
3. Acceptez le fichier par défaut en appuyant sur **Entrée**.
4. Acceptez le mot de passe par défaut pour la clé DSA en appuyant sur la touche **Entrée**.
5. Appuyez de nouveau sur la touche **Entrée** pour confirmer.

6. Copiez la clé publique dans la cible d'analyse en entrant la commande suivante :

   ```
   ssh-copy-id -i /home/qvmuser/.ssh/id_dsa.pub root@<adresse IP>
   ```

   Remplacez *<adresse IP>* par l'adresse IP de la cible de l'analyse.
7. Tapez le phrase de passe pour la cible de l'analyse.
8. Vérifiez que le compte *qvmuser* sur la console peut se connecter par SSH à la cible d'analyse, sans une phrase de passe en tapant la commande suivante :

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

   Remplacez *<adresse IP>* par l'adresse IP de la cible de l'analyse.

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

Que faire ensuite

Créez un profil d'analyse dans QRadar Vulnerability Manager avec le nom d'utilisateur *root* sans spécifier de mot de passe et exécutez une analyse des correctifs.

Tâches associées:

«Configuration d'une analyse authentifiée des systèmes d'exploitation Linux ou UNIX»
Dans IBM Security 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.

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

Dans IBM Security 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 46.

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 de profil d'analyse. Pour configurer une analyse authentifiée, vous devez également suivre les étapes restantes de cette procédure.
4. Facultatif : 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.

S'il existe un jeu de données d'identification pour les hôtes que vous analysez, les données d'identification que vous spécifiez manuellement dans l'onglet **Données d'identification supplémentaires** remplacent votre jeu de données d'identification.

5. Cliquez sur l'onglet de **planification d'analyse**.
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», à la page 45
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.

Tâches associées:

«Configuration d'un ensemble de données d'identification», à la page 46
Dans IBM Security 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», à la page 46
Pour analyser les systèmes d'exploitation Linux avec l'authentification par clé publique sécurisée, vous devez configurer la console IBM Security 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.

Activation des droits pour les analyses de correctif Linux ou UNIX

Les comptes utilisateur non superutilisateur doivent avoir le droit d'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

Pour affecter les droits appropriés pour l'analyse des correctifs Linux ou UNIX, procédez comme suit.

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 :

Système d'exploitation	Commandes

Linux	Lisez le contenu des fichiers suivants en fonction de votre distribution :
	1. /etc/redhat-release
	2. /etc/SuSE-release
	3. /etc/debian-version
	4. /etc/slackware-version
	5. /etc/mandrake-version
	6. /etc/gentoo-version
	Par exemple, sur Red Hat Enterprise Linux, utilisez les commandes suivantes :
	`ls /etc/redhat-releasecat /etc/redhat-release`
	`rpm -qa --qf '%{NAME}--%{VERSION}---%{RELEASE} |%{EPOCH}--%{ARCH}---%{FILENAMES}--%{SIGPGP}---%{SIGGPG}\n'`
	`rpm -qa --qf '%{NAME}-%{VERSION}-%{RELEASE}|%{EPOCH}\n'`

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`

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

Dans IBM Security 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.

Si les résultats de votre analyse Windows renvoient une vulnérabilité d'erreur de vérification locale, qui signale des problèmes de connexion WMI (Windows Management Interface), vous devez configurer vos systèmes Windows.

Pour plus d'informations sur la connectivité Windows, voir :

- «Activation de l'accès distant du registre aux actifs sur le système d'exploitation Windows», à la page 52.
- «Configuration de Windows Management Instrumentation», à la page 53.

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 de profil d'analyse. Pour configurer une analyse authentifiée du système d'exploitation Windows, vous devez également suivre les étapes restantes de cette procédure.
4. Facultatif : 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.

   S'il existe un jeu de données d'identification pour les hôtes que vous analysez, les données d'identification que vous spécifiez manuellement dans l'onglet **Données d'identification supplémentaires** remplacent votre jeu de données d'identification.
5. Cliquez sur le panneau de **planification d'analyse**.
6. Dans la liste **Exécuter la planification**, sélectionnez **Manuelle**.
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 (**>**).
9. Cliquez sur **Sauvegarder**.
10. Dans la page Profils d'analyse, cliquez sur **Exécuter**.

Concepts associés:

«Ensembles de données d'identification centralisés», à la page 45
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.

«Analyse des correctifs authentifiés», à la page 44
Dans IBM Security 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.

Analyse des correctifs Windows

L'*analyse des correctifs Windows* est une méthode réseau authentifiée qui permet d'interroger l'ordinateur cible au sujet des correctifs et mises à jour de sécurité manquants.

L'analyse des correctifs Windows a besoin d'accéder à 3 services Windows clés :

- Registre à distance
- WMI
- Partages administratifs

Il est possible de rechercher les correctifs Windows sur les ordinateurs sans utiliser les services WMI et Partages administratifs, mais les résultats ne seront pas complets et pourraient contenir des faux positifs.

Utilisez des mots de passe complexes. Cependant, certains caractères spéciaux peuvent entraîner des problèmes. Limitez les caractères spéciaux aux nombres, points, virgules, points virgules, apostrophes, signes pour cent et espaces.

Registre à distance

Le service Registre à distance 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 à distance n'est pas accessible, l'analyse des correctifs Windows échoue complètement.

Si QRadar Vulnerability Manager ne peut pas accéder au registre à distance, 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 **Registre à distance**.
5. Faites un clic droit sur le service **Registre à distance**, 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 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 à distance 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 Windows Management Instrumentation

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 WMI, de nombreuses applications tierces sont oubliées. 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.

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. Facultatif : 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.

Autorisation des demandes WMI via un pare-feu Windows

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 le pare-feu Windows (également appelé Pare-feu de connexion Internet) qui est installé sur les ordinateurs Windows XP et Windows 2003, vous devez configurer le pare-feu afin qu'il autorise les demandes WMI distantes.

Pour configurer le pare-feu Windows afin qu'il autorise les demandes WMI distantes, ouvrez une invite de commande et entrez la commande suivante :

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

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 accorder des droits d'accès distant 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 ces droits sur l'ordinateur B afin d'autoriser un utilisateur ou un groupe qui ne fait pas partie du groupe Administrateurs sur l'ordinateur B à se connecter 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. Sous **Autorisations d'accès**, cliquez sur **Modifier les limites**.
5. Dans la boîte de dialogue **Autorisations d'accès**, sélectionnez le nom **ANONYMOUS LOGON** dans la zone **Noms d'utilisateurs ou de groupes**. Dans la colonne **Autoriser** sous **Autorisations pour utilisateur**, sélectionnez **Accès à distance**, puis cliquez sur **OK**.

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 précédante 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 défait 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 **Contôle 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 d'un intervalle d'analyse autorisé

Dans IBM Security 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. I knowok
6. Choisissez une planification pour les fenêtres opérationnelles dans la liste des **planifications**.
7. Facultatif : Sélectionnez les heures où l'analyse est autorisée.
8. Facultatif : Sélectionnez votre fuseau horaire.

9. Si vous avez sélectionné **Hebdomadaire** dans la liste des **planifications**, cochez les jours de la semaine dans le panneau **Hebdomadaire**.
10. Si vous avez sélectionné **Mensuelle** dans la liste des **planifications**, sélectionnez un jour dans la liste **Jour du mois**.
11. Cliquez sur **Sauvegarder**.

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

    Si vous affectez deux fenêtres opérationnelles se chevauchant à un profil d'analyse, celle-ci s'exécute entre l'heure de début de la première fenêtre opérationnelle et l'heure de fin de la seconde. 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.

Procéder à des analyses durant les heures autorisées

Dans IBM Security 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 de 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 de **planification d'analyse**.
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 Security 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 de **planification d'analyse**.
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 Security 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 7.
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 **Dynamic server selection** dans l'onglet **Détails** de la page Configuration de profil d'analyse.

Concepts associés:

«Analyse dynamique», à la page 17
Dans l'analyse dynamique, IBM Security QRadar Vulnerability Manager sélectionne un scanner en fonction de l'adresse IO à examiner.

«Options d'ajout de programmes d'analyse à votre déploiement QRadar Vulnerability Manager», à la page 7
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 Security QRadar Vulnerability Manager.

«Détails relatifs au profil d'analyse», à la page 35
Dans IBM Security QRadar Vulnerability Manager, vous pouvez décrire votre analyse, sélectionner le scanner à utiliser, ainsi qu'un certain nombre d'options de politique d'analyse.

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

Dans IBM Security 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 7.

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», à la page 7
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 Security QRadar Vulnerability Manager.

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

Dans IBM Security 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 7.

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 à cocher **Dynamic server selection**.

   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. Facultatif : 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**.

Règles d'analyse

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

Vous pouvez utiliser des règles 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 Security QRadar Vulnerability Manager, une *règle d'analyse* est associée à un profil d'analyse et utilisée pour contrôler une analyse des vulnérabilités. Vous

utilisez la liste **Règles d'analyse** sur l'onglet **Détails** de la page Configuration de profil d'analyse pour associer une règle d'analyse avec un profil d'analyse.

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

Stratégies d'analyse préconfigurées

Les stratégies d'analyse préconfigurés suivantes sont distribuées avec QRadar Vulnerability Manager :

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

Une description de chaque stratégie d'analyse préconfigurée figure dans la pageStratégies d'analyse.

Tâches associées:

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

«Configuration d'une règle d'analyse pour gérer les analyses des vulnérabilités», à la page 62
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer une stratégie d'analyse pour contrôler vos analyses de vulnérabilité.

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

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

Utilisez les règles 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 règles d'analyse sur votre système, accédez à **Administration** > **Règles d'analyse** dans l'onglet **Vulnérabilités**.

Vous ne devez pas modifier les règles 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 règle d'analyse qui est fournie par mise à jour automatique, elle peut être récupérée seulement par le support client QRadar.

Modification d'une stratégie d'analyse préconfigurée

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

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

   Important : Si vous modifiez la nouvelle stratégie d'analyse, vous devez mettre à jour les informations de la description.
9. Pour modifier la règle 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'administration d'analyse.

Configuration d'une règle d'analyse pour gérer les analyses des vulnérabilités

Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer une stratégie d'analyse pour contrôler vos analyses de vulnérabilité.

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 stratégie d'analyse.

   Pour configurer une stratégie d'analyse, les seules zones obligatoires dans la fenêtre Nouvelle politique d'administration d'analyse sont les zones **Nom** et **Description**.
5. Dans la liste **Type d'analyse**, sélectionnez le type d'analyse sur lequel baser votre stratégie d'analyse.
6. Pour inclure des vulnérabilités spécifiques dans votre règle d'analyse, procédez comme suit.
   a. Dans la fenêtre Nouvelle politique d'administration d'analyse, cochez la case **Correctif**.
   b. Cliquez sur l'onglet **Vulnérabilités**.
   c. Cliquez sur **Ajouter**.

      Par défaut, toutes les vulnérabilités découvertes au cours de l'année écoulée sont affichées.
   d. Filtrez la liste des vulnérabilités.

e. Cliquez sur les vulnérabilités que vous voulez inclure dans votre stratégie d'analyse et cliquez sur **Soumettre** dans la barre d'outils.

7. Pour inclure ou exclure des groupes d'outils d'une politique d'administration complète ou non reconnue, cliquez sur l'onglet **Groupe d'outils**.
8. Pour inclure ou exclure des d'outils d'une politique d'administration complète ou non reconnue, cliquez sur l'onglet **Outils**.

   Important :

   Si vous ne modifiez pas les outils ou les groupes d'outils et que vous avez sélectionné l'option **Complète** pour le type d'analyse, tous les outils et les groupes d'outils associés à une analyse complète sont inclus dans votre politique d'administration d'analyse.
9. Cliquez sur **Sauvegarder**.

Chapitre 6. Examen détaillé de l'analyse de vulnérabilité

Dans IBM Security 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. Le risque est affiché dans la colonne **Score** et indique le score CVSS (Common Vulnerability Scoring System) total associé au profil d'analyse terminée.
- 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.

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 Security 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.

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:

«Planning d'analyse», à la page 37
Dans IBM Security QRadar Vulnerability Manager, vous pouvez planifier les dates et heures d'analyse de vos ressources réseau à la recherche des vulnérabilités connues.

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

Limitez les recherches d'actif à l'aide de filtres incluantdes 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 Security 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. Facultatif : 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. Facultatif : 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. Facultatif : 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**.

Niveaux de risque et catégories de vulnérabilités associés aux actifs

Dans IBM Security 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 écchouées** 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 Security 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:

Chapitre 8, «Règles d'exception relatives aux vulnérabilités», à la page 87
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer des règles d'exception afin de réduire le nombre de faux positifs en matière de vulnérabilités.

Afficage 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 Security 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**.

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 du planning d'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 Security QRadar SIEM 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 des **éléments à envoyer par 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 7. Gestion des vulnérabilités

Dans IBM Security QRadar Vulnerability Manager, vous pouvez gérer, rechercher et filtrer vos données de vulnérabilité afin de vous concentrer sur celles qui 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.

Examen détaillé des scores du risque des vulnérabilités

Dans IBM Security 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. Facultatif : 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 Security QRadar Vulnerability Manager, les scores du risque des vulnérabilités fournissent une indication du risque que pose une vulnérabilité à votre organisation.

Avec IBM Security 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 sous licence, la colonne **Score de risque** affiche le score de la métrique environnementale CVSS avec une valeur maximale de 10.

Sous-score d'exploitabilité

L'exploitabilité est calculée comme un sous-ensemble du score de base CVSS en s'appuyant sur les éléments suivants :

- Le vecteur d'accès (Access Vector/AV) fournit une indication du risque basée sur l'éloignement (local, réseau adjacent ou réseau éloigné) de l'attaquant.
- La complexité d'accès (Access Complexity) fournit une indication du risque basée sur la complexité de l'attaque. Moins la complexité est grande et plus le risque est élevé.
- L'authentification (Authentication) fournit une indication du risque basée sur les tentatives d'authentification. Moins les tentatives sont nombreuses et plus le risque est élevé.

Ajustements du risque

Si IBM Security 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 d'QRadar Risk Manager et d'QRadar Vulnerability Manager», à la page 23
IBM Security QRadar Vulnerability Manager s'intègre à IBM Security QRadar Risk Manager pour vous aider à hiérarchiser les risques et vulnérabilités dans votre réseau.

Tâches associées:

«Hiérarchisation des vulnérabilités à haut risque par l'application de règles du risque», à la page 81
Dans IBM Security QRadar Vulnerability Manager, vous pouvez signaler aux administrateurs les vulnérabilités à haut risque en appliquant à vos vulnérabilités des règles du risque.

Recherche des données de vulnérabilité

Dans IBM Security 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. Facultatif : Sélectionnez un groupe dans la liste **Groupe**.
   b. Facultatif : 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. Facultatif : 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», à la page 74
Dans IBM Security 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 Security 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 5. 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», à la page 77
Dans IBM Security QRadar Vulnerability Manager, vous pouvez enregistrer vos critères de recherche de vulnérabilité pour une utilisation ultérieure.

Paramètres de recherche de vulnérabilités

Dans IBM Security 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 6. Paramètres de recherche de vulnérabilités

Option	Description
Complexité d'accès	Niveau de complexité de l'attaque qui est requis pour exploiter une vulnérabilité.

Tableau 6. Paramètres de recherche de vulnérabilités (suite)

Option	Description
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 Security QRadar pour les systèmes multi-domaines, utilisez cette option pour spécifier le domaine dans lequel vous souhaitez rechercher des vulnérabilités.
Par service ouvert	Utilisez ce paramètre pour rechercher les vulnérabilités qui sont associées à des services ouverts tels que 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	Vulnérabilités nouvellement publiées qui ont été détectées sur votre réseau sans analyses supplémentaires.

Tableau 6. Paramètres de recherche de vulnérabilités (suite)

Option	Description
Inclure les exceptions de vulnérabilité	Vulnérabilités avec application d'une règle d'exception.
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 Security 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	Utilisez ce paramètre pour n'inclure que les vulnérabilités récemment publiées qui sont détectées sur votre réseau sans analyse supplémentaire dans votre recherche.
Inclure uniquement les exceptions de vulnérabilité	Utilisez ce paramètre pour n'inclure que les vulnérabilités avec une règle d'exception appliquée dans votre recherche.
En retard (jours)	Utilisez ce paramètre pour rechercher des vulnérabilités qui sont en retard pour la résolution d'un nombre de jours spécifié.
Statut du correctif	Utilisez ce paramètre pour filtrer les vulnérabilités par état des correctifs. Pour plus d'informations, voir «Identification de l'état de correctif des vulnérabilités», à la page 83.
Gravité PCI	Utilisez ce paramètre pour rechercher les vulnérabilités par niveau de gravité PCI (élevé, moyen ou faible) attribué 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	Utilisez ce paramètre pour rechercher les vulnérabilités par niveau de risque (élevé, moyen, faible, avertissement).
Non affecté	Utilisez ce paramètre pour rechercher les vulnérabilités sans utilisateur assigné pour les corriger.

Tableau 6. Paramètres de recherche de vulnérabilités (suite)

Option	Description
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.
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	Utilisez ce paramètre pour filtrer les vulnérabilités par les 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 Security 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. Facultatif : Pour inclure votre recherche enregistrée dans la liste **Recherches rapides** sur la barre d'outils, cliquez sur **Inclure dans mes recherches rapides**.
7. Facultatif : Pour partager vos critères de la recherche enregistrée avec tous les utilisateurs QRadar, cliquez sur **Partager avec tout le monde**.
8. Facultatif : 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. Facultatif : 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**.

Supprimer les critères de recherche enregistrés de vulnérabilités

Dans IBM Security 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 Security 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», à la page 71
Dans IBM Security QRadar Vulnerability Manager, les scores du risque des vulnérabilités fournissent une indication du risque que pose une vulnérabilité à votre organisation.

Vulnérabilités des réseaux

Dans IBM Security 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 Security 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 Security 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 Security 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. Facultatif : 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», à la page 72
Dans IBM Security QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités importantes en recherchant vos données de vulnérabilité.

Réduction du nombre de faux positifs de vulnérabilité

Dans IBM Security 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. Facultatif : 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

En fonction de votre sélection de type de serveur, les vulnérabilités suivantes sont automatiquement définies en tant que règles d'exceptions de faux positif :

Tableau 7. 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 Security 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», à la page 71
Dans IBM Security QRadar Vulnerability Manager, les scores du risque des vulnérabilités fournissent une indication du risque que pose une vulnérabilité à votre organisation.

Hiérarchisation des vulnérabilités à haut risque par l'application de règles du risque

Dans IBM Security QRadar Vulnerability Manager, vous pouvez signaler aux administrateurs les vulnérabilités à haut risque en appliquant à vos vulnérabilités des règles du risque.

Lorsque vous appliquez une règle du risque à une vulnérabilité, le score du risque est ajusté, ce qui permet aux administrateurs d'identifier plus précisément les vulnérabilités qui exigent une attention immédiate.

Dans cet exemple, 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 hiérarchiser.

Concepts associés:

«Intégration d'QRadar Risk Manager et d'QRadar Vulnerability Manager», à la page 23
IBM Security QRadar Vulnerability Manager s'intègre à IBM Security QRadar Risk Manager pour vous aider à hiérarchiser les risques et vulnérabilités dans votre réseau.

Tâches associées:

«Enregistrement des critères de recherche de vulnérabilité», à la page 77
Dans IBM Security QRadar Vulnerability Manager, vous pouvez enregistrer vos critères de recherche de vulnérabilité pour une utilisation ultérieure.

Configuration de couleurs d'affichage personnalisées pour les scores de risque

Configurez un code couleur personnalisé pour les scores de risque IBM Security QRadar Vulnerability Manager afin d'afficher ces scores de risque codées en couleur dans les interfaces de QRadar Vulnerability Manager.

Procédure

1. Dans IBM Security 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.

Identification des vulnérabilités ayant un correctif BigFix

Dans IBM Security 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. Facultatif : Classez les vulnérabilités en fonction de leur importance en cliquant sur l'en-tête de colonne **Score de risque**.
6. Facultatif : Pour avoir des détails sur le correctif d'une vulnérabilité, cliquez sur un lien de vulnérabilité dans la colonne **Vulnérabilité**.
7. Facultatif : 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 Security 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 de BigFix», à la page 24
IBM Security QRadar Vulnerability Manager s'intègre à IBM BigFix afin de vous permettre de filtrer et de hiérarchiser les vulnérabilités pouvant être corrigées.

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 scanneur
- 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 scanneur, 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 scanneur 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 scanneur 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 Security 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 8. Règles d'exception relatives aux vulnérabilités

Dans IBM Security 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.

Tâches associées:

«Réduction du nombre de faux positifs de vulnérabilité», à la page 80
Dans IBM Security QRadar Vulnerability Manager, vous pouvez créer automatiquement des règles d'exception pour les vulnérabilités qui sont associées à un type de serveur spécifique.

Application d'une règle d'exception de vulnérabilité

Dans IBM Security 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. Facultatif : 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**.

   Pour appliquer une règle d'exception de vulnérabilité, la seule zone obligatoire est la zone de texte **Commentaire**. Tous les autres paramètres sont facultatifs.
7. Facultatif : Dans la fenêtre Gestion de la règle d'exception, sélectionnez l'une des options suivantes :
   - Entrez une date à laquelle l'exception de vulnérabilité doit expirer.

- Si l'exception de vulnérabilité ne doit jamais expirer, cliquez sur **N'expire jamais**.

8. Dans la section Notes de la fenêtre Gestion de la règle d'exception, entrez du texte dans la zone de saisie **Commentaires**.
9. Cliquez sur **Sauvegarder**.

Tâches associées:

«Recherche des données de vulnérabilité», à la page 72
Dans IBM Security QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités importantes en recherchant vos 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**.

Rechercher des exceptions de vulnérabilités

Dans IBM Security 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 9. 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.

Tâches associées:

«Configuration des délais de résolution pour les vulnérabilités dans les actifs affectés», à la page 91
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les délais de résolution des différents types de vulnérabilités.

Affectation des vulnérabilités individuelles à un utilisateur technique pour qu'elles soient résolues

Dans IBM Security 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. Facultatif : 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».
7. Facultatif : 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 valeur de la zone **Date d'échéance** est définie comme la date actuelle.
8. Facultatif : 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 Security 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.

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 Security 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. Facultatif : 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. Facultatif : 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. Facultatif : 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. Facultatif : 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 Security 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 10. Rapports de vulnérabilités

Dans IBM Security 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 Security QRadar SIEM - 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 Security 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 Security 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 :

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 89
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 72

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. Facultatif : 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. Facultatif : 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», à la page 89
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer des groupes d'actifs et affecter automatiquement leurs vulnérabilités à des utilisateurs techniques.

«Recherche des données de vulnérabilité», à la page 72
Dans IBM Security QRadar Vulnerability Manager, vous pouvez identifier les vulnérabilités importantes en recherchant vos données de vulnérabilité.

Génération de rapports de conformité PCI

Dans IBM Security 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 31.
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», à la page 31
Dans IBM Security QRadar Vulnerability Manager, vous pouvez configurer les profils d'analyse pour spécifier comment et quand les actifs de votre réseau sont analysés pour la recherche de vulnérabilités.

Mise à jour des plans de conformité des actifs et des déclarations logicielles

Dans IBM Security 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 Security 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.

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

Limitez les recherches d'actif à l'aide de filtres incluantdes 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 11. Recherche de vulnérabilités, articles et avis

Utilisez les outils proposés dans IBM Security 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 Security 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. Facultatif : Si aucune vulnérabilité ne s'affiche, sélectionnez une autre plage de temps dans la liste **Affichage des vulnérabilités de :**.
4. Facultatif : 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 Security 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**.

Affichage des recommandations de sécurité provenant des fournisseurs de vulnérabilités

Dans IBM Security 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 Security 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.

Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

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

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

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

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

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de service 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.

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

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

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

UNIX est une marque de The Open Group aux Etats-Unis et/ou dans certains autres pays.

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

Remarques sur les règles de confidentialité

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

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

Si les configurations déployées pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres personnes via des cookies et d'autres technologies, vous devez vous renseigner sur l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

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

Glossaire

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

Les renvois suivants y sont utilisés :

- *Voir* vous renvoie d'un terme non privilégié au terme privilégié ou d'une abréviation à la forme complète.
- *Voir aussi* vous renvoie à un terme connexe ou contraire.

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

A

conseil
Document qui contient des informations et une analyse sur une menace ou une vulnérabilité.

actif Objet gérable qui est déployé ou destiné à être déployé dans un environnement opérationnel.

C

CDP Voir Collateral Damage Potential.

CIDR Voir routage CIDR.

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.

client Programme logiciel ou ordinateur qui demande des services à un serveur.

Collateral Damage Potential (CDP)
Mesure de l'impact possible d'une vulnérabilité exploitée à des fins malveillantes sur un actif physique ou sur une organisation.

Common Vulnerability Scoring System (CVSS)
Système d'évaluation qui mesure la gravité d'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.

D

DNS Voir système de noms de domaine (DNS).

transfert de zone DNS
Transaction qui permet de répliquer une base de données DNS (Domain Name System).

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

E

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.

F

règle de faux positif d'exception
Règle spécifique aux vulnérabilités à faible risque qui réduit le volume des vulnérabilités gérées.

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

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.

IP Voir protocole IP.

N

National Vulnerability Database (NVD)
Référentiel des données de gestion des vulnérabilités normalisé aux Etats-Unis.

NVD Voir National Vulnerability Database.

O

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.

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.

fenêtres opérationnelles
Période de temps configurée pendant laquelle une analyse est autorisée à s'exécuter.

P

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.

PCI DSS
Voir Norme de sécurité pour les données de cartes bancaires.

niveau de gravité PCI
Niveau de risque que présente une vulnérabilité pour le secteur des cartes de paiement.

R

processus de résolution
Processus d'affectation, de suivi et de correction des vulnérabilités qui ont été identifiées sur un actif.

S

liste d'exclusion d'analyse
Liste d'actifs, de groupes réseau et de plages CIDR ignorés par les analyses.

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.

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).

T

TCP Voir Transmission Control Protocol (TCP).

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

L

M

N

O

P

Q

R

S

T

U

V

W