IBM Security QRadar Vulnerability Manager
Version 7.2.0

Guide d'utilisation

Remarque : Avant d'utiliser le présent document et le produit associé, lisez les informations disponibles dans Avis et marques à la page 122.

SOMMAIRE

A PROPOS DE CE GUIDE

Le IBM Security QRadar Vulnerability Manager guide d'utilisation fournit des informations sur l'installation, la configuration et l'utilisation de QRadar Vulnerability Manager.

Public cible

Ce guide est destiné l'administrateur système chargé de configurer IBM Security QRadar Vulnerability Manager dans votre réseau.

Ce guide suppose que vous disposez d'un accès à IBM Security QRadar SIEM ou IBM Security QRadar Log Manager, un accès administrateur aux périphériques et pare-feux de votre réseau et que vous maîtrisez le réseau de votre entreprise et les technologies de mise à jour.

Conventions de la documentation

Les conventions suivantes s'appliquent dans ce guide :

Remarque : Indique que les informations fournies viennent compléter la fonction ou l'instruction associée.

ATTENTION : *Indique que les informations sont capitales. Une mise en garde vous avertit de l'éventuelle perte de données ou d'un éventuel endommagement de l'application, du système, du périphérique ou du réseau.*

AVERTISSEMENT : *Indique que les informations sont capitales. Un avertissement vous informe des éventuels dangers, des éventuelles menaces ou des risques de blessure. Lisez attentivement tous les messages d'avertissement avant de poursuivre.*

Documentation technique

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

Contacter le service clients

Pour savoir comment contacter le service clients, voir la ***note technique sur le support et le téléchargement.*** (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

Instructions sur les bonnes pratiques de sécuritaires

La sécurité du système informatique implique la protection des systèmes et des informations par l'intermédiaire de la prévention, la détection et la réponse à un accès incorrect à partir 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, les produits et services IBM sont destinés à être intégrés dans une approche de sécurité globale, qui impliqueront nécessairement des procédures opérationnelles et peuvent exiger à ce que d'autres systèmes produits ou services soient plus efficaces. IBM NE GARANTIT PAS QUE TOUS LES SYSTEMES, PRODUITS ET SERVICES SONT A L'ABRI DE, OU PROTEGERONT L'ENTREPRISE CONTRE LA CONDUITE MALICIEUSE OU ILLEGALE DE TOUTE PARTIE.

1 IBM SECURITY QRADAR VULNERABILITY MANAGER

IBM Security QRadar Vulnerability Manager est une plate-forme d'analyse de réseau qui détecte les vulnérabilités des applications, systèmes et appareils de votre réseau ou DMZ.

QRadar Vulnerability Manager gère les vulnérabilités qui sont détectées par son scanner intégré et par des scanners tiers. Les scanners tiers sont intégrés à QRadar et incluent IBM Security End Point Manager, Guardium, AppScan, Nessus, nCircle et Rapid 7.

QRadar Vulnerability Manager utilise le renseignement de sécurité pour livrer des analyses décisionnelles et rapides aux vulnérabilités. Par exemple, QRadar Vulnerability Manager vous aide à hiérarchiser les failles de sécurité en corrélant les résultats d'analyse de vulnérabilité aux flux réseau, données de journal, et pare-feu et données de configuration d'IPS provenant d'autres fonctionnalités QRadar. Vous pouvez utiliser QRadar Vulnerability Manager pour continuellement surveiller les vulnérabilités, améliorer la configuration de ressource, le correctif logiciel, et l'indentification et le blocage des ports ouverts.

QRadar Vulnerability Manager est complètement intégré à QRadar et peut être activé avec une clé de licence ne nécessitant aucune installation supplémentaire. Il peut utiliser des appareils QRadar existants pour mener des recherches d'actifs dynamiques axées sur des événements, alors que les analyses régulières permettent un affichage en temps réel de l'état de la sécurité de votre organisation.

Grâce à un contexte de sécurité riche provenant des données de flux de réseau, de configurations d'actifs et de sources d'intelligence de menace, QRadar Vulnerability Manager vous aide à identifier et à hiérarchiser plus efficacement les vulnérabilités de réseau.

Les fonctions de QRadar Vulnerability Manager sont gérées par QRadar SIEM ou la console QRadar Log Manager grâce à l'onglet **Vulnerabilities**. Pour plus d'informations sur le déploiement et l'accès à l'onglet **Vulnerabilities**, voir **Déploiement de QRadar Vulnerability Manager**.

Pour plus d'informations sur le système et la gestion des licences, voir *le guide d'administration IBM Security QRadar SIEM* ou le *guide d'administration IBM Security QRadar Log Manager*.

Vous pouvez accéder à QRadar Vulnerability Manager à partir de la console QRadar grâce à un navigateur Web pris en charge, et un nom d'utilisateur et un mot de passe qui vous sont affectés par votre administrateur. Pour plus d'informations, voir **Navigateurs Web pris en charge**.

QRadar Vulnerability Manager s'intègre avec IBM Security SiteProtector pour aider une politique directe d'IPS (Intrusion Prevention System). Pour plus d'informations, voir **Connexion à IBM Security SiteProtector**.

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

Analyse de vulnérabilité

Utilisez l'onglet **Vulnerabilities** pour configurer les profils d'analyse. Les profils d'analyse sont utilisés pour spécifier la façon dont vos actifs de réseau sont analysés pour la recherche de vulnérabilités.

Les administrateurs peuvent utiliser des données de résultat d'analyse pour effectuer les tâches suivantes :

- Analyser les résultats en regroupant les données par réseau, actif ou service ouvert.
- Évaluer les risques aux actifs et prioriser les vulnérabilités les plus critiques.
- Corriger les vulnérabilités et créer des exceptions de vulnérabilité.
- Rechercher chaque vulnérabilité et identifier les méthodes pour la correction de vulnérabilités.

Tableau de bord de gestion de vulnérabilité

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

QRadar Vulnerability Manager est distribué avec des éléments de tableau de bord par défaut qui vous permettent de rapidement examiner les risques pour votre organisation.

Vous pouvez créer un nouveau 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 IBM Security QRadar SIEM* ou le guide d'utilisation *IBM Security QRadar Log Manager*.

Notation des vulnérabilités

Chaque vulnérabilité est notée grâce à des algorithmes complexes pour indiquer avec précision la gravité de chaque vulnérabilité.

la notation de vulnérabilité vous permet de vous concentrer sur la correction des faiblesses de votre réseau qui posent le plus de risques d'opération.

Restauration de vulnérabilité

Vous pouvez automatiquement ou manuellement affecter les vulnérabilités aux utilisateurs QRadar pour une restauration.

Cela offre une visibilité de restauration de vulnérabilité car les utilisateurs peuvent mettre à jour leur progression dans la correction des faiblesses qui sont détectées sur les actifs de réseau.

Pour plus d'informations sur la restauration de vulnérabilité, voir **Gérer la résolution des vulnérabilités**.

Informations de vulnérabilité

Vous pouvez accéder aux informations détaillées de recherche sur les vulnérabilités publiées.

La recherche de données d'actualités, accessible à partir de site Web externe, est directement liée aux vulnérabilités qui sont détectées lorsque les analyses sont effectuées. Par exemple, la base de données nationale des vulnérabilités offre des informations sur la façon dont chaque vulnérabilité peut être examinée et corrigée.

Pour plus d'informations, voir **Research Vulnerabilities, News and Advisories**.

vulnérabilités d'alertes précoces

Les vulnérabilités sont détectées en analysant vos actifs de réseau et en comparant les résultats avec une base de données de définitions de vulnérabilité publiées.

Lorsque de nouvelles définitions de vulnérabilité sont publiées avant que vous n'ayez effectué une autre analyse de votre réseau, vous pouvez utiliser la fonction d'alerte précoce pour afficher les actifs à risque. Utilisez les alertes précoces pour maintenir la sensibilisation des actifs qui sont à risque sans avoir à effectuer de longues analyses de réseau nécessitant des ressources considérables.

Pour plus d'informations sur l'affichage et la recherche pour les vulnérabilités d'alertes précoces, voir **Paramètres de recherche de vulnérabilité**.

Exceptions de vulnérabilité

Lorsque les vulnérabilités présentent moins de risques à votre organisation ou que vous n'ayez pas besoin de notification de vulnérabilité, vous pouvez créer des règles d'exception de vulnérabilité.

Les règles d'exception indiquent les vulnérabilités qui ne sont pas affichées dans vos données de vulnérabilité. Vous pouvez spécifier l'adresse IP ou plage d'adresses auxquelles s'appliquent les règles d'exception.

Notation des résultats de vulnérabilité

Dans l'onglet **Vulnerabilities**, vous pouvez trier les données en cliquant sur un en-tête de colonne.

Un clic unique d'une colonne trie les résultats par ordre décroissant et un deuxième clic sur l'en-tête trie les résultats par ordre croissant. Une flèche au-dessus de la colonne indique la direction du tri.

Par exemple, pour trier les vulnérabilités par gravité de vulnérabilité, cliquez sur l'en-tête **Vulnerability Severity**. Une flèche s'affiche dans l'en-tête de colonne pour indiquer que les résultats sont triés par ordre décroissant. Cliquez à nouveau sur l'en-tête de colonne **Vulnerability Severity** pour trier les données par ordre croissant.

Navigateurs Web pris en charge

Vous pouvez accéder à QRadar Vulnerability Manager partir d'un navigateur Web standard. Lorsque vous accédez au système, une invitation s'affiche demandant un nom d'utilisateur et un mot de passe, qui doivent être configurés à l'avance par l'administrateur QRadar.

Tableau 1-1 Navigateurs Web pris en charge

Navigateur Web	Versions prises en charge
Mozilla Firefox	• 10.0 ESR • 17.0 ESR En raison du cycle de publication court de Mozilla, nous ne pouvons pas nous engager à l'essai sur les dernières versions du navigateur Mozilla Firefox. Toutefois, nous sommes pleinement engagés à étudier tous les problèmes qui sont signalés.
Microsoft® Windows Internet Explorer	• 8.0 • 9.0
Google Chrome	• Dernière version Nous sommes pleinement engagés à étudier tous les problèmes qui sont signalés.

Connexion à QRadar Vulnerability Manager

Vous pouvez accéder à la console QRadar à partir d'un navigateur Web standard et vous connecter grâce à un nom d'utilisateur et un mot de passe qui vous sont affectés par votre administrateur.

A propos de cette tâche

QRadar Vulnerability Manager est géré en utilisant l'onglet **Vulnerabilities**.

Utilisez les informations du tableau suivant pour vous connecter à votre console :

Tableau 1-2 Informations de connexion par défaut pour QRadar Vulnerability Manager

Informations de connexion	Par défaut
URL	https://<IP Address> où <IP Address> représente l'adresse IP de la consoleQRadar.
User Name	admin
Password	Le mot de passe qui vous est affecté par votre réseau ou l'administrateur QRadar. Si vous vous connectez et ne voyez pas l'onglet **Vulnerabilities**, assurez-vous que User Role pour QRadar Vulnerability Manager est activé pour votre compte.

Procédure

Etape 1 Ouvrez votre navigateur Web.

Etape 2 Entrez l'adresse suivante dans la barre d'adresse :

```
https://<IP Address>
```

Etape 3 Entrez votre nom d'utilisateur et votre mot de passe.

Etape 4 Cliquez sur **Login To QRadar**.

Remarque : Si vous utilisez un navigateur Web Mozilla Firefox, alors vous devez ajouter une exception à Mozilla Firefox pour vous connecter à QRadar. Pour plus d'informations, consultez votre documentation Mozilla Firefox. Si vous utilisez un navigateur Microsoft Internet Explorer, un message sur le certificat de sécurité de site Web s'affiche. Vous devez sélectionner l'option **Continue to this website** pour vous connecter à QRadar.

2 DÉPLOIEMENT DE QRADAR VULNERABILITY MANAGER

QRadar Vulnerability Manager est déployé à l'aide de QRadar SIEM et de QRadar Log Manager.

Si vous installez QRadar SIEM, l'onglet **Vulnerabilities** s'active par défaut avec une clé de licence temporaire. Si vous installez QRadar Log Manager, l'onglet **Vulnerabilities** ne s'active pas par défaut. Pour continuer à utiliserQRadar Vulnerability Manager après la période temporaire ou activer QRadar Vulnerability Manager avec QRadar Log Manager, vous devez installer et configurer une clé de licence.

Pour plus d'informations sur les clés de licence, voir le guide d'utilisation*IBM Security QRadar SIEM* ou le guide d'utilisation*IBM Security QRadar Log Manager*.

Si vous corrigez vers QRadar 7.2, consultez le guide d'utilisation *IBM Security QRadar SIEM* ou le guide de mise à niveau*IBM Security QRadar Log Manager.*

Vous pouvez déployerQRadar Vulnerability Manager de plusieurs façons. Par exemple, vous pouvez contrôler toute l'analyse et le traitement de vulnérabilité de votre console QRadar ou vous pouvez décider de débarquer votre traitement et votre analyse vers un processeur QRadar Vulnerability Manager ou des appareils d'analyse. Pour plus d'informations,
voir **Vulnérabilité de traitement et de scannage**.

Sauf indication contraire, toutes les références à SiteProtector se réfèrent à IBM Security SiteProtector.

Clés d'activation QRadar vulnerability manager

Si vous souhaitez effectuer une analyse ou un traitement de vulnérabilité en utilisant un hôte géré de QRadar Vulnerability Manager dédié, vous devez installer un processeur QRadar Vulnerability Manager ou un appareil d'analyse et entrer une clé d'activation.

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 d'appareil :

- L'appareil de processeur QRadar Vulnerability Manager inclut les composants de traitement et d'analyse de vulnérabilités.

- L'appareil d'analyse QRadar Vulnerability Manager inclut uniquement un composant d'analyse de vulnérabilité.

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

- Si vous achetez un logiciel QRadar Vulnerability Manager ou un téléchargement d'appareil virtuel, une liste de clés d'activation est incluse dans le document Getting Started joint à un e-mail de confirmation. Vous pouvez utiliser ce document pour faire une référence croisée du numéro de composant du dispositif qui vous a été fourni.
- Si vous avez acheté un dispositif qui est préchargé avec le logiciel QRadar Vulnerability Manager, la clé d'activation est incluse dans votre boîte ou CD d'expédition.

Pour plus d'informations sur l'installation d'un dispositif hôte géré, consultez les guides d'installation *IBM Security QRadar SIEM* ou *IBM Security QRadar Log Manager*.

Intégration d'IBM Security SiteProtector

QRadar Vulnerability Manager s'intègre avec IBM Security SiteProtector pour aider une politique directe d'IPS (Intrusion Prevention System).

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

Remarque : SiteProtector reçoit uniquement les données de vulnérabilité provenant des analyses de QRadar Vulnerability Manager qui sont effectuées après que l'intégration est configurée.

Pour plus d'informations, voir **Connexion à IBM Security SiteProtector**.

Éditeur de déploiement

En utilisant l'onglet **Admin**, vous pouvez accéder à Deployment Editor et configurer vos composants de vulnérabilité de traitement et d'analyse.

L'éditeur de déploiement nécessite Java™ Runtime Environment (JRE). Vous pouvez télécharger Java™ 1.6 ou 1.7 à l'adresse Web suivante : *https://www.java.com*. Si vous utilisez le navigateur Web Mozilla Firefox, vous devez configurer votre navigateur pour qu'il accepte les fichiers Java™ Network Language Protocol (JNLP).

Pour plus d'informations sur Deployment Editor, voir le guide d'administration *IBM Security QRadar SIEM* ou le guide d'administration *IBM Security QRadar Log Manager.*

Vulnérabilité de traitement et de scannage

Les composants de traitement et de scannage sont utilisés pour identifier les vulnérabilités de votre réseau.

Lorsque vous achetez une licence QRadar Vulnerability Manager sur une console QRadar, le processeur QRadar Vulnerability Manager est automatiquement déployé. Pour plus d'informations, voir **Vérification de déploiement de processeur**.

Le processeur QRadar Vulnerability Manager fournit un composant de scannage. Si nécessaire, vous pouvez déployer des scanners supplémentaires sur des dispositifs d'hôtes gérés du scanner dédié QRadar Vulnerability Manager ou sur des hôtes gérés QRadar.

Le traitement et le scannage de vulnérabilité peuvent être déployés selon les besoins de votre réseau et de votre métier. Vous pouvez déployer votre capacité de traitement et de scannage des manières suivantes :

- Déployez un traitement et un scannage de vulnérabilité vers une console QRadar ou vers un hôte géré. Pour plus d'informations, voir **Déploiement d'un processeur**.
- Déployez un traitement de vulnérabilité vers un hôte géré du processeur dédié QRadar Vulnerability Manager. Pour plus d'informations, voir **Déploiement d'un traitement vers un dispositif QRadar Vulnerability Manager**.
- Déployez un scannage de vulnérabilité vers un hôte géré QRadar. Pour plus d'informations, voir **Déploiement d'un scannage de vulnérabilité vers un hôte géré QRadar**.
- Déployez un scannage de vulnérabilité vers un hôte géré du scanner dédié QRadar Vulnerability Manager. Pour plus d'informations, voir **Déploiement d'un scannage vers un dispositif QRadar Vulnerability Manager**.
- Déploiement d'un scanner pour effectuer des analyses des actifs de votre DMZ. Pour plus d'informations, voir **Déploiement d'un scanner DMZ**.

Vérification de déploiement de processeur

Vous pouvez vérifier que votre processeur QRadar Vulnerability Manager est déployé sur une console ou sur un hôte géré.

A propos de cette tâche

Pour vérifier qu'un processeur QRadar Vulnerability Manager est déployé sur un hôte géré, vous devez accéder à la console QRadar.

Procédure

Etape 1 Connectez-vous à la console QRadar.

Etape 2 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 3 Sélectionnez l'onglet **Vulnerability View**.

Etape 4 Assurez-vous que **QVM Processor** est affiché dans le volet **Vulnerability View**.

Etape suivante

Si **QVM processor** n'est pas déployé, alors vous devez déployer le processeur. Suivez les étapes de la procédure, **Déploiement d'un processeur**.

Déploiement d'un processeur

Vous pouvez ajouter le processeur QRadar Vulnerability Manager à votre console QRadar ou à un hôte géré.

Procédure

Etape 1 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 2 Sélectionnez l'onglet **Vulnerability View**.

Etape 3 Dans le volet Vulnerability Components, cliquez sur **QVM Processor**.

Etape 4 Saisissez un nom unique pour le processeur QVM à ajouter. Le nom peut comporter jusqu'à 20 caractères et peut inclure des traits d'unions et caractères de soulignement. Cliquez sur **Next**.

Etape 5 Dans la zone de liste **Select a host**, sélectionnez la console ou l'hôte géré que vous souhaitez affecter au processeur QVM. Cliquez sur **Next**.

Etape 6 Cliquez sur **Finish**.

Etape 7 Dans la fenêtre d'invite de dialogue, cliquez sur **Yes**.

Etape 8 Dans le menu de l'éditeur de déploiement, sélectionnez **File > Save and close**.

Etape 9 Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration.**

Etape 10 Cliquez sur **OK**.

Suppression d'un processeur QRadar Vulnerability Manager

Vous pouvez supprimer le processeur QRadar Vulnerability Manager de la console ou de l'hôte géré.

Procédure

Etape 1 Accédez à la console QRadar.

Etape 2 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 3 Sélectionnez l'onglet **Vulnerability View**.

Etape 4 Sélectionnez **QVM Processor** sur le volet **Vulnerability View**.

Etape 5 Dans la fenêtre de dialogue Warning, cliquez sur **Yes**.

Etape 6 Dans le menu Deployment Editor, sélectionnez **Edit > Delete**.

Etape 7 Dans le menu de l'éditeur de déploiement, sélectionnez **File > Save and close**.

Etape 8 Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration.**

Etape 9 Cliquez sur **OK**.

Déploiement d'un traitement vers un dispositif QRadar Vulnerability Manager

Vous pouvez déployer un traitement de vulnérabilité vers un dispositif d'hôte géré et dédié QRadar Vulnerability Manager et effectuer un scannage et un traitement de vulnérabilité à l'aide de l'hôte géré.

Avant de commencer

Installez un hôte géré QRadar Vulnerability Manager à l'aide d'une clé d'activation d'un dispositif de processeur valide. Pour plus d'informations sur les clés d'activation de l'hôte géré, voir **Clés d'activation QRadar vulnerability manager**.

A propos de cette tâche

Vous ne pouvez avoir qu'un seul processeur QRadar Vulnerability Manager dans votre déploiement. Lorsque vous sélectionnez le processeur sur un hôte géré, le processeur est automatiquement supprimé de la console.

Remarque : Tous les profils de scannage ou les résultats d'analyse associés à un processeur de la console ne sont pas affichés après avoir déployé le traitement vers un hôte géré dédié. Vous pouvez continuer à rechercher des données de vulnérabilité, pour tout profil de scannage précédemment créé, à l'aide du paramètre de recherche **Found by scan profile** sur les pages **Manage Vulnerabilities**. Pour plus d'informations, voir **Paramètres de recherche de vulnérabilité**.

Le processeur QRadar Vulnerability Manager offre un composant d'analyse. Lorsque le processeur est déployé, vous n'êtes pas obligé de déployer un scanner séparé. Cependant, vous pouvez déployer un scanner sur un hôte géré QRadar séparément, voir **Déploiement d'un scannage de vulnérabilité vers un hôte géré QRadar**.

Pour plus d'informations sur l'hôte géré NAT, le chiffrement et la compression, consultez les guides d'administration *IBM Security QRadar SIEM* ou *IBM Security QRadar Log Manager*.

Procédure

Etape 1 Accédez à la console QRadar.

Etape 1 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 2 Dans le menu, sélectionnez **Actions > Add a Managed Host**.

Etape 3 Cliquez sur **Next**.

Etape 4 Saisissez les valeurs des paramètres suivants :

- Dans la zone **Enter the IP of the server or appliance to add**, entrez l'adresse IP du dispositif de l'hôte géré du processeur QRadar Vulnerability Manager.
- Dans la zone **Enter the root password of the host,** entrez le mot de passe root du dispositif de l'hôte géré du processeurQRadar Vulnerability Manager.
- Dans la zone **Confirm the root password of the host**, entrez à nouveau le mot de passe.

Etape 5 Cliquez sur **Finish**.

Etape 6 Dans la boîte de dialogue **Adding Managed Host** cliquez sur **OK**.

Etape 7 Si une boîte de dialogue **Validation Error** est affichée, sélectionnez le processeur de l'hôte géré QRadar Vulnerability Manager et cliquez sur OK**.**

Etape 8 Cliquez sur **Yes**.

Etape 9 Dans le menu de l'éditeur de déploiement, sélectionnez **File > Save and close**.

Etape 10 Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration.**

Etape 11 Cliquez sur **OK**.

Etape suivante

Vérifiez que le processeur QRadar Vulnerability Manager est déployé sur l'hôte géré. Pour plus d'informations, voir **Vérification de déploiement de processeur**.

Déploiement d'un scannage de vulnérabilité vers un hôte géré QRadar

Vous pouvez déployer un scanner QRadar Vulnerability Manager vers 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

Vous devez disposer d'un hôte géré QRadar existant dans votre déploiement. Pour plus d'informations sur l'installation d'un hôte géré, consultez les guides d'installation *IBM Security QRadar SIEM* ou *IBM Security QRadar Log Manager*.

A propos de cette tâche

Les étapes de cette procédure expliquent la façon de déployer un scanner QRadar Vulnerability Manager vers un hôte géré QRadar. Vous pouvez également déployer un scanner vers un dispositif d'hôte géré du scanner QRadar Vulnerability Manager. Pour plus d'informations, voir **Déploiement d'un scannage vers un dispositif QRadar Vulnerability Manager**.

Procédure

Etape 1 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 2 Sélectionnez l'onglet **Vulnerability View**.

Etape 3 Dans le volet **Vulnerability Components**, cliquez sur **QVM Scanner**.

Etape 4 Entrez un nom unique pour le QVM Scanner que vous souhaitez ajouter. Le nom peut comporter jusqu'à 20 caractères et peut inclure des traits d'unions et caractères de soulignement. Cliquez sur **Next**.

Etape 5 Dans la liste déroulante **Select a host**, sélectionnez l'adresse IP de l'hôte géré QRadar à ajouter au scanner QVM.

Etape 6 Cliquez sur **Next**.

Etape 7 Cliquez sur **Finish**.

Etape 8 Dans le menu de l'éditeur de déploiement, sélectionnez **File > Save and close**.

Etape 9 Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration.**

Etape 10 Cliquez sur **OK**.

Etape suivante

Vérifiez que le scanner externe est répertorié dans la boîte de liste **Scan Server** dans le volet extensible **Scan Profile Details**. Pour plus d'informations, voir **Configuration du profil d'analyse**.

Déploiement d'un scannage vers un dispositif QRadar Vulnerability Manager

Vous pouvez déployer un scanner vers un dispositif de scannage d'hôte géré dédié QRadar Vulnerability Manager et effectuer un scannage de vulnérabilité à l'aide de l'hôte géré.

Avant de commencer

Installez un dispositif d'hôte géré du scanner QRadar Vulnerability Manager à l'aide d'une clé d'activation du dispositif valide. Pour plus d'informations sur les clés d'activation d'hôte géré, voir **Clés d'activation QRadar vulnerability manager**.

Procédure

Etape 1 Accédez à la console QRadar.

Etape 1 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 2 Dans le menu, sélectionnez **Actions > Add a Managed Host**.

Etape 3 Cliquez sur **Next**.

Etape 4 Saisissez les valeurs des paramètres suivants :

- Dans la zone **Enter the IP of the server or appliance to add**, entrez l'adresse IP du dispositif de l'hôte géré du scanner QRadar Vulnerability Manager.
- Dans la zone **Enter the root password of the host,** entrez le mot de passe root du dispositif de l'hôte géré du scanner QRadar Vulnerability Manager.
- Dans la zone **Confirm the root password of the host**, entrez à nouveau le mot de passe.

Etape 5 Cliquez sur **Finish**.

Etape 6 Dans la boîte de dialogue **Adding Managed Host** cliquez sur **OK**.

Etape 7 Si une boîte de dialogue **Validation Error** s'affiche, sélectionnez le processeur à ajouter à votre déploiement et cliquez sur **OK**.

Etape 8 Cliquez sur **Yes**.

Etape 9 Dans le menu de l'éditeur de déploiement, sélectionnez **File > Save and close**.

Etape 10 Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration.**

Etape 11 Cliquez sur **OK**.

Déploiement d'un scanner DMZ

Vous pouvez déployer un scanner externe et analyser les vulnérabilités des actifs de votre DMZ.

A propos de cette tâche

Pour analyser les actifs dans DMZ afin de détecter des vulnérabilités, il n'est pas nécessaire de déployer un scanner dans votre DMZ. Vous devez configurer QRadar Vulnerability Manager à l'aide d'un scanner IBM géré situé à l'extérieur de votre réseau. Lorsque votre DMZ est analysé, toutes les vulnérabilités détectées sont traitées par le processeur QRadar Vulnerability Manager hébergé dans votre console QRadar ou dans un hôte géré.

Avant de commencer

Pour analyser des actifs dans votre DMZ, vous devez procéder comme suit :

- Déployer un processeur QRadar Vulnerability Manager. Pour plus d'informations, voir **Déploiement d'un processeur**.
- Configurer un accès Internet sortant sur le port 443.
- Envoyer un courrier électronique à : QRadar-QVM-Hosted-Scanner@hursley.ibm.com. Inclure les informations suivantes :
  - Votre adresse IP de passerelle.
  - La plage d'adresse IP des actifs dans votre DMZ.

Procédure

Etape 1 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 2 Sélectionnez l'onglet **Vulnerability View**.

Etape 3 Dans le volet **Vulnerability Components**, cliquez sur **External Scanner**.

Etape 4 Entrez un nom unique pour le External Scanner que vous souhaitez ajouter. Le nom peut comporter jusqu'à 20 caractères et peut inclure des traits d'unions et caractères de soulignement. Cliquez sur **Next**.

Etape 5 Entrez votre adresse IP de passerelle et cliquez sur **Next**.

Etape 6 Cliquez sur **Finish**.

Etape 7 Dans le menu de l'éditeur de déploiement, sélectionnez **File > Save and close**.

Etape 8 Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration.**

Etape 9 Cliquez sur **OK**.

Etape suivante

Vérifiez que le scanner externe est répertorié dans la boîte de liste **Scan Server** dans le volet extensible **Scan Profile Details**. Pour plus d'informations, voir **Configuration du profil d'analyse**.

Connexion à IBM Security SiteProtector

Vous pouvez transmettre des données de vulnérabilité à IBM Security SiteProtector pour aider une politique directe d'IPS (Intrusion Prevention System).

Procédure

Etape 1 Dans l'onglet **Admin**, cliquez sur **Deployment Editor**.

Etape 2 Dans la boîte de dialogue Opening adminconsole.cgi, cliquez sur **OK**.

Etape 3 Dans la boîte de dialogue Security Information, cliquez sur **Run**.

Etape 4 Dans la boîte de dialogue Warning Security, cliquez sur **No**.

Etape 5 Sélectionnez l'onglet **Vulnerability View**.

Etape 6 Dans le volet **Vulnerability Components**, cliquez sur **SiteProtector Adapter**.

Etape 7 Saisissez un nom unique pour l'adaptateur SiteProtector à ajouter. Le nom peut comporter jusqu'à 20 caractères et peut inclure des traits d'unions et caractères de soulignement. Cliquez sur **Next**.

Etape 8 Entrez l'adresse IP du serveur de gestionnaire d'agent IBM Security SiteProtector.

Etape 9 Cliquez sur **Next**.

Etape 10 Cliquez sur **Finish**.

Etape 11 Dans le menu de l'éditeur de déploiement, sélectionnez **File > Save and close**.

Etape 12 Dans la barre d'outils de l'onglet **Admin**, sélectionnez **Advanced > Deploy Full Configuration.**

Etape 13 Cliquez sur **OK**.

Etape suivante

Effectuez une analyse des actifs de votre réseau pour déterminer si les données de vulnérabilité sont affichées dans votre installation SiteProtector.

Pour plus d'informations sur les profils d'analyse, voir **Configuration du profil d'analyse**.

3 GESTION DES PROFILS D'ANALYSE

Un profil d'analyse permet de déterminer comment et à quel moment QRadar Vulnerability Manager analyse les actifs de votre réseau pour les vulnérabilités connues.

Vous pouvez créer plusieurs profils d'analyse et configurer chacun d'entre eux de manière différente pour tenir compte des besoins spécifiques de votre réseau. Lors de la configuration d'un profil d'analyse, vous pouvez sélectionner des informations de configuration facultatives à partir des volets extensibles. Pour plus d'informations, voir **Configuration du profil d'analyse**.

Vous pouvez exécuter des analyses manuelles ou les planifier pour une exécution aux moments opportuns pour l'environnement de votre réseau. Vous pouvez également indiquer les noeuds réseau, les domaines, ou les domaines virtuels que vous souhaitez analyser. S'il le faut, vous pouvez inclure Windows, UNIX, ou une analyse corrective authentifiée par Linux.

QRadar Vulnerability Manager s'intègre à QRadar pour offrir la possibilité d'analyser des actifs faisant partie d'une recherche d'actif enregistrée. Pour plus d'informations, voir **Planification d'analyses de nouveaux actifs**.

Grâce aux profils d'analyse, vous pouvez :

- consulter les informations concernant les profils d'analyse existant. Pour plus d'informations, voir **Affichage des profils d'analyse**.
- Indiquez les actifs réseaux que vous souhaitez exclure de toute analyse. Pour plus d'informations, voir **Scan exclusions**.
- Créez des fenêtres opérationnelles, qui définissent les heures auxquelles les analyses peuvent être effectuées. Pour plus d'informations, voir **Fenêtre opérationelle**.
- Configurez plusieurs profils d'analyse et personnalisez l'analyse de votre réseau. Pour plus d'informations, voir **Création des profils d'analyse**.
- Exécutez manuellement les profils d'analyse. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.

Barre d'outils des profils d'analyse

Une barre d'outils est fournie à la page **Scan Profiles** sur l'onglet **Vulnerabilities**.

La zone de liste **Actions** de la barre d'outils des profils d'analyse offre les options suivantes :

Tableau 3-1 Options de la barre d'outils des profils d'analyse

Option	Description
Create	Sélectionnez cette option pour créer un profil d'analyse. Pour plus d'informations, voir **Création des profils d'analyse**.
Delete	Sélectionnez cette option pour supprimer un profil d'analyse. Pour plus d'informations, voir **Suppression d'un profil d'analyse**.
Edit	Sélectionnez cette option pour modifier un profil d'analyse. Pour plus d'informations, voir **Modification d'un profil d'analyse**.
Run Now	Sélectionnez cette option pour exécuter manuellement une analyse. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**. ***Remarque :*** *Vous pouvez aussi exécuter manuellement un profil d'analyse programmé pour s'exécuter à une date ultérieure.*
Print	Sélectionnez cette option pour imprimer une liste des profils d'analyse. Pour plus d'informations, voir **Impression de profils d'analyse**.
Export to XML	Sélectionnez cette option pour exporter une liste des profils d'analyse au format Extensible Markup Language (XML). Pour plus d'informations, voir **Export de profils d'analyse**.
Export to CSV	Sélectionnez cette option pour exporter une liste des profils d'analyse au format valeurs séparées par une virgule (CSV). Pour plus d'informations, voir **Export de profils d'analyse**.

Affichage des profils d'analyse

Vous pouvez afficher des profils d'analyse existants, surveiller la progression des analyses, et déterminer le temps mis par une analyse.

Remarque : Si vous changez le traitement de votre vulnérabilité et le déploiement d'analyse le message suivant peut s'afficher : **QVM est en cours de déploiement.** Vous devez attendre la configuration complète du déploiement, avant de poursuivre. Pour plus d'informations,
voir **Vulnérabilité de traitement et de scannage**.

A propos de cette tâche

La page Scan Profiles affiche les informations suivantes :

Tableau 3-2 Paramètres des profils d'analyse

Paramètre	Description
Nom de profil	Nom du profil d'analyse. Déplacez votre souris sur **Profile Name** pour afficher les informations relatives au profil d'analyse et au statut des analyses terminées ou en cours d'exécution.
Scanner	Nom du scanner qui exécute le profil d'analyse.

Tableau 3-2 Paramètres des profils d'analyse (suite)

Paramètre	Description
Planning	Planning d'exécution appliqué au profil d'analyse. par défaut, lors de la configuration d'un profil d'analyse, l'analyse est réglée pour s'exécuter automatiquement. Pour plus d'informations, voir **Configuration du profil d'analyse**. Pour plus d'informations sur l'exécution d'une analyse, voir **Exécution manuelle d'un profil d'analyse**.
Status	Statut du profil d'analyse. Les statuts incluent : • **Stopped** - Indique que l'analyse a réussi ou a été annulée. Pour plus d'informations, voir **Annulation des analyses de vulnérabilité**. • **Running** - Indique que l'analyse est en cours d'exécution. • **Paused** - Indique que l'analyse a été mise en pause. • **Not Started** - Indique que l'analyse n'est pas lancée. Pour plus d'informations sur l'exécution d'une analyse, voir **Exécution manuelle d'un profil d'analyse**.
Progress	Indique l'état d'avancement de l'analyse. Déplacez votre souris sur la barre de progression lors de l'exécution d'analyse pour afficher la progression d'analyse. Par exemple, vous pouvez visualiser les informations relatives aux outils d'analyse en cours d'exécution et en attente.
End of Last Run	Date et heure de la dernière exécution d'analyse.
Duration	Durée de la dernière analyse complète. La durée s'affiche en jours, en heures, et en minutes.

Procédure

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

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Configuration du profil d'analyse

Configurez les profils d'analyse en sélectionnant à partir des options qui s'affichent dans les volets extensibles de la page **Scan Profile Configuration**.

Pour plus d'informations sur la création des profils d'analyse, y compris des exemples, voir **Création des profils d'analyse**.

Détails du profil d'analyse

Dans le volet extensible **Scan Profile Details** vous pouvez décrire votre analyse, sélectionner le scanner que vous souhaitez utiliser, et choisir parmi un certain nombre d'options de type d'analyse.

Vous pouvez configurer les options suivantes sur les détails du profil d'analyse :

Tableau 3-3 Analyse des paramètres de configuration pour les détails du profil

Paramètre	Description
Nom de profil	Indique le nom de votre profil d'analyse. Le nom de profil d'analyse doit avoir plus de quatre caractères.
Active	Sélectionnez cette case à cocher si vous souhaitez exécuter l'analyse automatiquement à une date ultérieure. La case à cocher est sélectionnée par défaut. **Remarque :** Si vous décochez la case à cocher **Active**, le nouveau profil d'analyse s'affiche dans la liste Scan Profiles, mais ne peut pas s'exécuter avant son lancement manuel. Pour plus d'informations sur l'exécution d'analyses manuelles, voir **Exécution manuelle d'un profil d'analyse**.
Update asset model	Sélectionnez la case à cocher **Update asset model** si vous souhaitez envoyer les résultats d'analyse à QRadar et si vous souhaitez mettre à jour le modèle d'actif. La case à cocher est sélectionnée par défaut. *Pour plus d'informations sur les Actifs, consultez les guides d'utilisation IBM Security QRadar SIEM ou IBM Security QRadar Log Manager.*
Profile Description	Indique la description de profil de l'analyse. ***Remarque :** Pour vous permettre d'identifier correctement les profils d'analyse à l'avenir, vous pouvez entrer une description qui décrit les actions d'analyse effectuées par votre profil d'analyse.*
Scan Server	Indique le scanner utilisé pour exécuter le profil d'analyse. Le scanner sélectionné dépend de la configuration de votre réseau. Par exemple, si vos actifs sont présents dans votre DMZ, sélectionnez alors un scanner ayant accès à cette zone de votre réseau. Pour plus d'informations, voir **Déploiement d'un scanner DMZ**. Le serveur d'analyse **Controller** correspond au scanner qui est automatiquement déployé avec le processeur QRadar Vulnerability Manager sur votre console ou hôte géré. ***Remarque :** Il est possible qu'un seul processeur soit déployé, mais vous avez la possibilité de déployer plusieurs scanners soit sur des dispositifs d'hôte géré du scanner dédié QRadar Vulnerability Manager, soit sur des hôtes gérés QRadar. Par exemple collecteur de flux, collecteur d'événement, processeur d'événement, et processeurs de flux. Pour plus d'informations, voir* **Vulnérabilité de traitement et de scannage**.

Tableau 3-3 Analyse des paramètres de configuration pour les détails du profil (suite)

Paramètre	Description
Bandwidth Limit	Indique la bande passante de votre analyse. Le paramètre par défaut est Medium. Si vous sélectionnez une valeur supérieure à 1000 kbps, vous risquez d'affecter les performances du réseau. L'option inclut : • **Bas** - 200 Kbps • **Moyen** - 1000 Kbps • **Elevé** - 3000 Kbps • **Complet** - 5000 Kbps
Type d'analyse	Indique le type d'analyse que vous souhaitez effectuer. Les options incluent : • **Full Scan** - Découvre des actifs de réseau et effectue une analyse de port configurable d'utilisateur et une analyse non authentifiée d'analyse de FTP, web, ssh, et des services de base de données. Si vous fournissez des données d'identification, une analyse authentifiée est alors effectuée. • **Discovery Scan** - Découvre des actifs de réseau et effectue une analyse de port afin d'identifier le système d'exploitation, le type d'unité, et les services fournis par l'actif. Aucune analyse de vulnérabilité effectuée. • **Patch Scan** - Observe le réseau pour découvrir les actifs, puis effectuer une analyse rapide de port et une analyse des données d'identification des actifs. Pour plus d'informations sur l'analyse de port, voir **Comment analyser**. • **PCI Scan** - Une analyse nécessaire pour la conformité Payment Card Industry (PCI). L'analyse PCI effectue une analyse complète de la plage de port TCP/IP 0-65535. • **Database Scan** - Effectue une analyse de port pour identifier Oracle, MSSQL Server, DB2, Informix, et les bases de données MySQL. Les bases de données découvertes sont testées pour les paramètres de serveur faible et les configurations par défaut. ***Remarque :*** *L'analyse de vulnérabilité est effectuée sur des actifs où une base de données est identifiée.* • **Web Scan** - Analyse les ports 80, 81, 443, 8080, et 8081 pour identifier les applications Web. L'analyse teste le scriptage de site croisé, l'injection sql, les paramètres de serveur Web faible, et les scripts vulnerable Common Gateway Interface (CGI). ***Remarque :*** *L'analyse de l'application Web est effectuée sur des actifs où une application Web est identifiée.*

Quand est-ce qu'il faut procéder à une analyse

Dans le volet extensible **When To Scan**, vous pouvez planifier les dates et les heures d'analyse de vos actifs, ou accepter le planning par défaut **Manual**.

Un profil d'analyse configuré avec un paramètre manuel doit être exécuté manuellement. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.

Remarque : Vous pouvez également exécuter manuellement un profil d'analyse qui doit s'exécuter à une date ultérieure.

Lorsque vous sélectionnez une option de planning d'analyse, autre que manual, vous pouvez alors améliorer votre planning d'analyse en configurant une fenêtre opérationnelle. Pour plus d'informations, voir **Fenêtre opérationelle**.

Vous pouvez configurer votre planning d'analyse à l'aide des options suivantes :

Tableau 3-4 Moment d'analyse des paramètres

Paramètre	Description
Manual	Manual est la sélection par défaut. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.
Run Once	Sélectionnez cette option pour exécuter automatiquement une analyse à la date de début et de fin indiquée.
Daily	Sélectionnez cette option pour exécuter automatiquement une analyse à la même heure chaque jour.
Weekly	Sélectionnez cette option pour exécuter automatiquement une analyse sur un ou plusieurs jours de la semaine et aux heures indiquées.
Monthly	Sélectionnez cette option pour exécuter automatiquement une analyse chaque mois, au jour et à l'heure indiquée.

Qu'est-ce qu'il faut analyser

Dans le volet extensible **What To Scan**, vous pouvez fournir des informations relatives aux actifs, aux domaines, ou aux toiles virtuelles sur votre réseau que vous souhaitez analyser.

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. Pour plus d'informations, voir **Planification d'analyses de nouveaux actifs**.

Insérez les noeuds réseau

Vous pouvez indiquer les actifs que vous souhaitez analyser sur votre réseau en définissant un intervalle CIDR, une adresses IP, ou une plage d'adresses IP.

Dans la zone **CIDR Range/IP/IP Range,** les administrateurs peuvent combiner l'une des options suivantes :

- **CIDR Range**. Vous pouvez indiquer les hôtes que vous souhaitez analyser à l'aide de l'intervalle CIDR. Par exemple : **212.43.43.33/27**.
- **IP** - Vous pouvez indiquer un hôte que vous souhaitez analyser à l'aide d'une adresse IP.
- **IP Range** - Vous pouvez indiquer les hôtes que vous souhaitez analyser à l'aide d'une plage d'adresses IP. Par exemple : **10.100.77.116-120**.

Pour plus d'informations sur l'analyse d'actifs, voir **Configuration d'une analyse manuelle d'actif.**

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 pour 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 le transfert de zone DNS sont sensibles et donc 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.

Pour plus d'informations sur la configuration d'une analyse de domaine, voir **Analyse des domaines sur une base mensuelle.**

Insérez des recherches enregistrées

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

A l'aide de l'onglet **Assets**, si vous recherchez vos actifs réseaux et enregistrez les critères de recherche, la recherche enregistrée s'affiche dans le volet **Include Saved Searches**.

Pour plus d'informations sur la sauvegarde d'une recherche d'actif, consultez les guides d'utilisation *IBM Security QRadar SIEM* ou *IBM Security QRadar Log Manager.*

Pour plus d'informations sur la configuration d'un profil d'analyse avec une recherche d'actif enregistrée, voir **Planification d'analyses de nouveaux actifs.**

Retirez les noeuds réseau

Vous pouvez indiquer les actifs qui ne doivent pas être analysés. Par exemple, si vous souhaitez éviter l'analyse d'un serveur très chargé, instable, ou sensible.

Dans la zone **CIDR Range/IP/IP Range,** vous pouvez combiner l'une des options suivantes :

- **CIDR Range**. Vous pouvez indiquer les hôtes que vous souhaitez exclure de votre analyse à l'aide de l'intervalle CIDR. Par exemple : **212.43.43.33/27**.
- **IP** - Vous pouvez indiquer un hôte que vous souhaitez exclure de votre analyse à l'aide de l'adresse IP.
- **IP Range** - Vous pouvez indiquer les hôtes que vous souhaitez exclure de votre analyse à l'aide d'une plage d'adresses IP. Par exemple : **10.100.85.110-120**.

Toiles virtuelles

Vous pouvez configurer un profil d'analyse pour analyser différentes adresses Uniform Resource Locators (URLs) hébergées sur la même adresse IP.

Lorsque vous effectuez une analyse Virtual Web, QRadar Vulnerability Manager vérifie chaque page web pour l'injection SQL ainsi que les vulnérabilités de scriptage de site croisé.

Comment analyser

Dans le volet extensible **How To scan**, vous pouvez personnaliser votre profil d'analyse pour analyser divers plages de ports en indiquant des protocoles d'analyse différents.

Par défaut, les analyses s'effectuent rapidement à l'aide des protocoles Transmission Control Protocol (TCP) et User Datagram Protocol (UDP). Une analyse rapide inclut plus de ports dans la plage 1 - 1024.

Remarque : Environ 2000 ports courants sont analysés lorsque vous choisissez l'analyse rapide.

Vous pouvez indiquer les plages de ports communes. Les plages de ports doivent être configurées en ordre séparé par un tableau de bord, délimité par une virgule, consécutif, croissant, et non superposé. Plusieurs plages de ports doivent être séparées par une virgule. Par exemple : (1-1024, 1055, 2000-65535).

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

Tableau 3-5 Analyse du profil d'analyse des paramètres du protocole

Paramètre	Description
TCP & UDP	TCP & UDP correspond au protocole d'analyse par défaut et analyse la plupart des ports présents dans la plage 1 - 1024.
TCP	TCP correspond au protocole d'analyse le plus commun. Lorsque l'analyse TCP est associée à l'analyse de la plage IP, vous pouvez localiser un hôte qui exécute des services sujets à des vulnérabilités. La plage de port par défaut est 1 - 65535.
UDP	L'option UDP envoie un module UDP à tous les ports indiqués. Pour les ports communs, un contenu spécifique au protocole est envoyé, mais d'une manière générale, le module envoyé est vide. La plage de ports par défaut est 1-15000.

Tableau 3-5 Analyse du profil d'analyse des paramètres du protocole (suite)

Paramètre	Description
SYN	SYN envoie un module à tous les ports indiqués. 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	ACK est 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	Le terme FIN ou ‘Finish’ est un module TCP utilisé pour interrompre une connexion, ou utilisé en tant que méthode pour identifier des 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.

Configuration de l'analyse

Dans le volet extensible **Scan Setup**, vous pouvez analyser les noms de communauté et effectuer une analyse corrective authentifiée pour les systèmes d'exploitation Windows, Linux, et UNIX.

Noms de communauté SNMP

Vous pouvez analyser les actifs de votre réseau à l'aide des noms de communauté SNMP.

Lorsque vous effectuez une analyse, QRadar Vulnerability Manager s'authentifie avec les services SNMP trouvés et effectue une analyse de vulnérabilité plus détaillée.

Windows Patch Scanning

Vous pouvez effectuer une analyse corrective de n'importe quel système d'exploitation Windows de votre réseau.

Si vous n'indiquez pas un nom de domaine, une analyse corrective s'effectue sur les hôtes qui sont en cours d'analyse, étant donné que le nom d'utilisateur et le mot de passe sont corrects et que vous disposez des droits appropriés pour l'actif.

Pour effectuer une analyse corrective Windows, l'accès au registre distant ainsi que l'interface de gestion Windows (WMI) doivent être activés. Si les résultats de votre analyse corrective Windows renvoient une vulnérabilité d'erreur, et les détails de problèmes de connectivité WMI vous devez configurer vos systèmes Windows. Pour plus d'informations, voir **Connectivité d'analyse de correctif Windows.**

Linux/Unix Patch Scanning

Vous pouvez effectuer une analyse corrective de n'importe quel système d'exploitation Linux ou UNIX de de votre réseau, étant donné que le nom d'utilisateur et le mot de passe sont corrects et que vous disposez des droits appropriés pour l'actif.

Pour plus d'informations, voir **Configuration d'une analyse authentifiée Linux/UNIX**.

Fenêtre opérationelle

Créez et attribuez une fenêtre opérationnelle à un profil d'analyse planifié pour définir une période durant laquelle l'analyse doit s'exécuter.

Si vous attribuez deux fenêtres opérationnelles à un profil d'analyse, celui-ci s'exécute à l'intersection temporelle de la fenêtre opérationnelle. Si les fenêtres opérationnelles ne sont pas configurées avec un chevauchement d'emploi du temps, les analyses ne sont pas effectuées.

Grâce aux fenêtres opérationnelles, vous pouvez :

- consulter les informations relatives aux fenêtres opérationnelles existantes. Pour plus d'informations, voir **Affichage de la fenêtre opérationnelle**.

- associer une fenêtre opérationnelle à un profil d'analyse planifié. Pour plus d'informations, voir **Analyse pendant les heures autorisées**.

Barre d'outils de la fenêtre opérationnelle

Une barre d'outils est fournie à la page **Operational Windows** de l'onglet **Vulnerabilities**.

La zone de liste **Actions** de la barre d'outils Operational Windows fournit les options suivantes :

Tableau 3-6 Options de la barre d'outils pour la fenêtre opérationnelle

Option	Description
Add	Sélectionnez cette option pour créer une fenêtre opérationnelle. Pour plus d'informations, voir **Création d'une fenêtre opérationnelle**.
Edit	Sélectionnez cette option pour modifier une fenêtre opérationnelle. Pour plus d'informations, voir **Modification d'une fenêtre opérationnelle**.
Delete	Sélectionnez cette option pour supprimer une fenêtre opérationnelle. Pour plus d'informations, voir **suppression d'une fenêtre opérationnelle**.
Print	Sélectionnez cette option pour imprimer une fenêtre opérationnelle.

Affichage de la fenêtre opérationnelle

Vous pouvez afficher la fenêtre opérationnelle qui indique les heures auxquelles les analyses s'exécutent.

Avant de commencer

La page de liste Operational Windows affiche une liste de fenêtres opérationnelles. Si la liste est vide, il n'existe alors aucune fenêtre opérationnelle. Pour plus d'informations, voir **Création d'une fenêtre opérationnelle**.

A propos de cette tâche

La page Operational Windows affiche les informations suivantes :

Tableau 3-7 Paramètres de la fenêtre opérationnelle

Paramètre	Description
Name	Indique le nom de la fenêtre opérationnelle.
Description	Indique une description de la fenêtre opérationnelle.
Date de mise à jour	Indique la date de création de la fenêtre opérationnelle ou de la dernière mise à jour.
Mis à jour par	indique le nom de l'utilisateur QRadar ayant effectué la création ou la dernière mise à jour de la fenêtre opérationnelle.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Operational Window**.

Création d'une fenêtre opérationnelle

Vous pouvez créer une fenêtre opérationnelle pour indiquer les heures auxquelles une analyse peut s'exécuter.

A propos de cette tâche

Utilisez les informations contenues dans le tableau suivant pour créer une fenêtre opérationnelle :

Tableau 3-8 Paramètres de la fenêtre opérationnelle

Paramètre	Description
Name	Entrez le nom de la fenêtre opérationnelle. Le nom doit avoir plus de cinq caractères et ne doit pas dépasser 101 caractères.
Planning	Sélectionnez votre planning obligatoire.
Start Time	Sélectionnez une heure de début au format HH:MM
End Time	Sélectionnez une heure de fin au format HH:MM
Time Zone	Sélectionnez un fuseau horaire pour votre fenêtre opérationnelle.
Weekly	Sélectionnez les jours de la semaine durant lesquels votre analyse peut s'exécuter. ***Remarque :*** *Ces options s'affichent uniquement si vous sélectionnez* ***Weekly*** *dans la zone de liste* ***Schedule****.*
Monthly	Sélectionnez le jour du mois durant lequel votre analyse peut s'exécuter. ***Remarque :*** *Cette option s'affiche uniquement si vous sélectionnez* ***Monthly*** *dans la zone de liste* ***Schedule****.*

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Operational Window**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Add**.

Etape 4 Entrez les valeurs pour les paramètres décrits dans**Tableau 3-8**.

Etape 5 Cliquez sur **Save**.

Etape suivante

Facultatif. Associez une fenêtre opérationnelle à un profil d'analyse. Pour plus d'informations, voir **Analyse pendant les heures autorisées**.

Modification d'une fenêtre opérationnelle

Vous pouvez modifier une fenêtre opérationnelle pour changer les heures auxquelles une analyse peut s'exécuter.

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

A propos de cette tâche

Utilisez les informations contenues dans le tableau suivant pour modifier une fenêtre opérationnelle :

Tableau 3-9 paramètres de la fenêtre opérationnelle

Paramètre	Description
Name	Entrez le nom de la fenêtre opérationnelle. Le nom doit avoir plus de cinq caractères et ne doit pas dépasser 101 caractères.
Planning	Sélectionnez votre planning obligatoire.
Start Time	Sélectionnez une heure de début au format HH:MM
End Time	Sélectionnez une heure de fin au format HH:MM
Time Zone	Sélectionnez un fuseau horaire pour votre fenêtre opérationnelle.
Weekly	Sélectionnez les jours de la semaine durant lesquels votre analyse peut s'exécuter. ***Remarque :*** *Ces options s'affichent uniquement si vous sélectionnez* ***Weekly*** *dans la zone de liste* ***Schedule****.*
Monthly	Sélectionnez le jour du mois durant lequel votre analyse peut s'exécuter. ***Remarque :*** *Cette option s'affiche uniquement si vous sélectionnez* ***Monthly*** *dans la zone de liste* ***Schedule****.*

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Operational Window**.

Etape 3 Sélectionnez la fenêtre opérationnelle que vous souhaitez modifier.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Edit**.

Etape 5 Modifiez les paramètres décrits dans **Tableau 3-9**.

Etape 6 Cliquez sur **Save**.

Suppression d'une fenêtre opérationnelle

Vous pouvez supprimer une fenêtre opérationnelle pour retirer les restrictions de temps concernant l'exécution d'une analyse.

Avant de commencer

Il n'est pas possible de supprimer une fenêtre opérationnelle si elle est associée à un profil d'analyse. Pour retirer une fenêtre opérationnelle d'un profil d'analayse, voir **Retrait d'une fenêtre opérationnelle**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Operational Window**.

Etape 3 Sélectionnez la fenêtre opérationnelle que vous souhaitez supprimer.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Delete**.

Etape 5 Cliquez sur **OK**.

Retrait d'une fenêtre opérationnelle

Vous pouvez retirer une fenêtre opérationnelle d'un profil d'analyse.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Sélectionnez le profil d'analyse que vous souhaitez modifier.

Etape 4 Cliquez sur le panneau extensible **When To Scan**

Etape 5 Dans le volet **Operational Windows**, sélectionnez la **fenêtre opérationnelle** que vous souhaitez retirer.

Etape 6 Cliquez sur **Remove Selected**.

Etape 7 Cliquez sur **Save**.

Etape suivante

Si nécessaire, vous pouvez supprimer une fenêtre opérationnelle qui n'est pas associée à un profil d'analyse. Pour plus d'informations, voir **Suppression d'une fenêtre opérationnelle**.

Scan exclusions

Vous pouvez créer une exclusion d'analyse pour exclure une adresse IP ou une plage d'adresses IP d'une analyse.

Les exclusions d'analyse s'appliquent à toutes les configurations de profil d'analyse existantes et peuvent être utilisées pour exclure une activité d'analyse des serveurs instables ou sensibles.

Barre d'outils des exclusions d'analyse

Une barre d'outils est fournie à la page **Scan Exclusions** de l'onglet **Vulnerabilities**.

Grâce à la zone de liste **Actions** de la barre d'outils Scan Exclusions, vous pouvez accéder aux options suivantes :

Tableau 3-10 Options de la barre d'outils d'exclusion d'analyse

Option	Description
Add	Sélectionnez cette option pour créer une exclusion d'analyse. Pour plus d'informations, voir **Création d'exclusions d'analyse**
Edit	Sélectionnez cette option pour modifier une exclusion d'analyse. Pour plus d'informations, voir **Modification des exclusions d'analyse**
Delete	Sélectionnez cette option pour supprimer une exclusion d'analyse. Pour plus d'informations, voir **Suppression des exclusions d'analyse**
Print	Sélectionnez cette option pour imprimer une exclusion d'analyse. Pour plus d'informations, voir **Impression des exclusions d'analyse**.

Affichage des exclusions d'analyse

Vous pouvez afficher des exclusions d'analyse qui indiquent les actifs de votre réseau à ne jamais analyser.

Avant de commencer

La page de liste Scan Exclusions affiche une liste d'exclusions d'analyse. Si la liste est vide, il n'existe alors aucune exclusion d'analyse. Pour plus d'informations sur la création d'une exclusion d'analyse, voir **Création d'exclusions d'analyse**.

A propos de cette tâche

la page Scan Exclusions affiche les informations suivantes :

Tableau 3-11 Paramètres d'exclusion Scan

Paramètre	Description
Adresse IP	L'adresse IP ou la plage d'adresses IP exclue de toute analyse.
Description	Description de l'exclusion Scan.
Date de mise à jour	Date à laquelle l'exclusion Scan a été créée ou mise à jour. Pour plus d'informations sur la mise à jour d'une exclusion Scan, voir **Modification des exclusions d'analyse**.
Mis à jour par	Nom de l'utilisateur QRadar ayant effectué la dernière mise à jour de l'exclusion Scan.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Exclusions**.

Création d'exclusions d'analyse

Vous pouvez créer une exclusion d'analyse pour indiquer les actifs de votre réseau qui ne doivent jamais être analysés par un profil d'analyse.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Exclusions**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Add**.

Etape 4 Dans la zone **IP Address,** entrez l'adresse IP ou la plage d'adresses IP que vous souhaitez exclure de toutes les analyses.

Etape 5 Dans la zone **Description**, entrez une description de l'exclusion d'analyse.

Remarque : Fournissez une description identifiable à l'avenir. la description doit contenir plus de 5 caractères.

Etape 6 Cliquez sur **Save.**

Modification des exclusions d'analyse

Vous pouvez mettre à jour les actifs de votre réseau qui doivent être exclus de toutes les analyses.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Exclusions**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Edit**.

Etape 4 Cliquez sur **Save**.

Suppression des exclusions d'analyse

Vous pouvez retirer les restrictions d'actifs de votre réseau qui doivent être exclues de toutes les analyses.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Exclusions**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Delete**.

Etape 4 Cliquez sur **OK**.

Impression des exclusions d'analyse

Vous pouvez imprimer une liste d'exclusions d'analyse

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Exclusions**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Print**.

Etape 4 Sur la page Print, cliquez sur **Print**.

Création des profils d'analyse

Vous pouvez personnaliser l'analyse d'actifs de votre réseau pour les vulnérabilités en configurant plusieurs profils d'analyse.

Avant de commencer

Vous devez consulter les différentes options de configuration du profil d'analyse. Pour plus d'informations, voir **Configuration du profil d'analyse**.

Un profil d'analyse fournit plusieurs options de configuration. Les options que vous choisissez dépendent des données de vulnérabilité que vous souhaitez afficher et de la configuration des actifs de votre réseau.

Utilisez les informations suivantes afin de cerner le processus de configuration des profils d'analyse :

- Analyse élémentaire. Voir **Configuration d'une analyse manuelle d'actif**.
- Analyses planifiées d'actifs. Voir **Planification d'analyses de nouveaux actifs**.

- Analyse planifiée à l'aide d'une fenêtre opérationnelle. Voir **Analyse pendant les heures autorisées**.
- Analyse authentifiée Linux ou UNIX. Voir **Configuration d'une analyse authentifiée Linux/UNIX**.
- Analyse corrective Windows. Voir **Configuration d'une analyse de correctif Windows**.
- Analyse complète de la plage de ports. Voir **Analyse d'une plage de port complète**.
- Analyse d'actifs à l'aide de ports ouverts. Voir **Analyse d'actifs avec des ports ouverts**.
- Analyse de domaines. Voir **Analyse des domaines sur une base mensuelle**.

Configuration d'une analyse manuelle d'actif

Vous pouvez configurer un profil d'analyse élémentaire pouvant être exécuté manuellement.

A propos de cette tâche

Cette procédure décrit les étapes nécessaires à la configuration d'une analyse manuelle d'actif élémentaire. Pour consulter la liste complète des options de configuration du profil d'analyse, voir **Configuration du profil d'analyse**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **What To Scan**

Etape 7 Dans la zone **CIDR Range/IP/IP Range**, entrez l'adresse IP de l'actif que vous souhaitez analyser.

Etape 8 Cliquez sur **Save**.

Etape suivante

Exécuter les étapes dans la procédure, **Exécution manuelle d'un profil d'analyse**.

Planification d'analyses de nouveaux actifs

Vous pouvez configurer un profil d'analyse pour planifier des analyses hebdomadaires des nouveaux actifs réseaux découverts, non analysés.

Avant de commencer

A l'aide de l'onglet **Assets**, vous devez créer et sauvegarder une nouvelle recherche d'actif au moyen des options suivantes :

Paramètre	Modifier	Option
Days Since Asset Found	inférieur à	Deux jours
Days Since Asset Scanned	Supérieur à	Deux jours

Pour plus d'informations sur l'utilisation de l'onglet **Assets** et la sauvegarde des recherches d'actifs, voir le Guide d'utilisation *IBM Security QRadar SIEM* ou le Guide d'utilisation *IBM Security QRadar Log Manager.*

A propos de cette tâche

Utilisez l'onglet QRadar **Assets** pour afficher et rechercher les actifs de votre réseau. Lorsque vous recherchez vos actifs réseaux et que vous sauvegardez les critères de recherche, ces critères de recherche s'affichent dans le panneau **Include Saved Searches**.

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

Pour passer en revue la liste complète des options de profil d'analyse que pouvez configurer, voir **Configuration du profil d'analyse**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **When To Scan**

Etape 7 Dans la zone de liste **Run Schedule**, sélectionnez **Weekly**.

Etape 8 Dans la zone **Start Time**, entrez la date et l'heure à laquelle vous souhaitez exécuter votre analyse dans les jours de la semaine.

Etape 9 Sélectionnez les cases à cocher pour **Tuesday** et **Thursday**.

Etape 10 Cliquez sur le panneau extensible **What To Scan**

Etape 11 Dans le volet **Include Saved Searches**, identifiez votre recherche d'actif sauvegardée dans la zone **Available Saved Searches** et cliquez sur **Add**.

Etape 12 Cliquez sur **Save**.

Etape suivante

Au cours et à la fin de l'analyse planifiée, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse planifiée. Pour plus d'informations, voir **Affichage des profils d'analyse**.
- Consultez les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Analyse pendant les heures autorisées

Vous pouvez planifier une analyse des actifs réseaux aux heures indiquées, à l'aide d'une fenêtre opérationnelle.

Pour plus d'informations sur la fenêtre opérationnelle, voir **Operational windows**.

Avant de commencer

Pour associer un profil d'analyse à une fenêtre opérationnelle, vous devez créer une fenêtre opérationnelle. Pour plus d'informations, voir **Création d'une fenêtre opérationnelle**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **When To Scan**

Etape 7 Dans la zone de liste **Run Schedule**, sélectionnez **Daily**.

Etape 8 Dans la zone **Start Time**, entrez ou sélectionnez la date et l'heure d'exécution de votre analyse chaque jour.

Etape 9 Dans le volet **Operational Windows**, sélectionnez une fenêtre opérationnelle à partir de la zone de liste et cliquez sur **Add**.

Etape 10 Cliquez sur le panneau extensible **What To Scan**

Etape 11 Dans le panneau **Include Network Nodes,** entrez une plage d'adresses IP dans le champ, puis cliquez sur **Add**.

Etape 12 Cliquez sur **Save**.

Etape suivante

Au cours et à la fin de l'analyse planifiée, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse planifiée. Pour plus d'informations, voir **Affichage des profils d'analyse**.
- Consultez les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Configuration d'une analyse authentifiée Linux/UNIX

Vous pouvez configurer une analyse d'authentification des systèmes d'exploitation Linux ou UNIX qui se trouvent sur votre réseau.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **When To Scan**

Etape 7 Dans la zone de liste **Run Schedule**, sélectionnez, **Manual**.

Etape 8 Cliquez sur le panneau extensible **What To Scan**

Etape 9 Dans le panneau **Include Network Nodes,** entrez une plage d'adresses IP dans le champ, puis cliquez sur **Add**.

Etape 10 Cliquez sur le panneau extensible **Scan Setup**.

Etape 11 Dans le panneau **Linux/Unix Patch Scanning**, entrez le **Nom d'utilisateur** et le **Mot de passe** pour les hôtes Linux ou UNIX que vous voulez analyser.

Etape 12 Cliquez sur **Save**.

Etape suivante

Exécuter les étapes dans la procédure, **Exécution manuelle d'un profil d'analyse**.

Facultatif. Au cours et à la fin de l'analyse planifiée, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse. Pour plus d'informations, voir **Affichage des profils d'analyse**.
- Consultez les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Configuration d'une analyse de correctif Windows

Vous pouvez configurer une analyse de correctif des systèmes d'exploitation Windows installés sur votre réseau.

Before you being

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

Si les résultats de votre analyse de correctif Windows renvoient une vulnérabilité d'erreur de vérification locale, dont les détails indiquent les anomalies de connectivité d'Interface de Gestion Windows (WMI), vous devez configurer vos systèmes Windows. Pour plus d'informations, voir **Connectivité d'analyse de correctif Windows.**.

A propos de cette tâche

Si l'analyse de correctif Windows est effectuée sans privilèges d'administration, le Gestionnaire de Vulnérabilité Qradar analyse le registre distant pour chaque installation Windows.

ATTENTION : *Lorsqu'on exécute une analyse sans disposer de privilèges d'administration, cette analyse est incomplète, susceptible de donner lieu à des faux positifs et ne couvrira pas plusieurs applications tierces.*

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **When To Scan**

Etape 7 Dans la zone de liste **Run Schedule**, sélectionnez, **Manual**.

Etape 8 Cliquez sur le panneau extensible **What To Scan**

Etape 9 Dans le panneau **Include Network Nodes,** entrez une plage d'adresses IP dans le champ, puis cliquez sur **Add**.

Etape 10 Cliquez sur le panneau extensible **Scan Setup**.

Etape 11 **Dans le panneau Windows Patch Scanning**, entrez le **Nom d'utilisateur** et le **Mot de passe** pour les hôtes Windows ou UNIX que vous voulez analyser.

Etape 12 Cliquez sur **Save**.

Etape suivante

Exécuter les étapes dans la procédure, **Exécution manuelle d'un profil d'analyse**.

Facultatif. Au cours et à la fin de l'analyse planifiée, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse. Pour plus d'informations, voir **Affichage des profils d'analyse**.
- Passer en revue les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Analyse d'une plage de port complète

Vous pouvez analyser l'intégralité de la plage de ports sur l'actif que vous indiquez.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **What To Scan**

Etape 7 Dans le champ **CIDR Range/IP/IP Range**, entrez la plage CIDR des actifs que vous voulez analyser.

Etape 8 Cliquez sur le panneau extensible **How To Scan**

Etape 9 Dans le champ **Protocol**, acceptez les valeurs par défaut de **TCP & UDP**.

Etape 10 Dans **Range field**, tapez **1-65535**.

Etape 11 Dans le champ **Max Hosts**, entrez un nombre maximal d'hôtes que vous voulez analyser simultanément. Vous pouvez entrer n'importe quelle valeur dans la plage 1 - 255.

Etape 12 Dans le champ **Timeout (m)**, entrez le délai d'expiration (en minutes) après lequel vous voulez que l'analyse expire. La valeur par défaut est 30 minutes.

Remarque : Vous pouvez entrer n'importe quelle valeur dans la plage 1 - 500. Veillez à ne pas entrer un temps trop court, sinon l'analyse peut expirer sans détecter de port.

Etape 13 Cliquez sur **Save**.

Etape suivante

Exécuter les étapes dans la procédure, **Exécution manuelle d'un profil d'analyse**.

Facultatif. Au cours et à la fin de l'analyse planifiée, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse. Pour plus d'informations, voir **Affichage des profils d'analyse**.

- Passer en revue les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Analyse d'actifs avec des ports ouverts

Vous pouvez configurer un profil d'analyse de façon à pouvoir analyser des actifs avec des ports ouverts.

Avant de commencer

A l'aide de l'onglet QRadar **Assets**, vous pouvez visualiser et rechercher vos actifs réseau. Lorsque vous recherchez vos actifs réseaux et que vous sauvegardez les critères de recherche, ces critères de recherche s'affichent dans le panneau **Include Saved Searches**.

Pour plus d'informations sur la sauvegarde d'une recherche d'actif, voir le Guide d'utilisation *IBM Security QRadar SIEM* ou le Guide d'utilisation *IBM Security QRadar Log Manager*

A l'aide de l'onglet **Assets**, vous devez créer et sauvegarder une nouvelle recherche d'actif au moyen des options suivantes :

Tableau 3-12 Options de recherche sauvegardée d'actif

Paramètre	Modifier	Option
Actifs avec port ouvert	Egal à	80
Actifs avec port ouvert	Egal à	8080

Pour plus d'informations sur l'utilisation de l'onglet **Assets** et la sauvegarde de recherches d'actif, voir le Guide d'utilisation *IBM Security QRadar SIEM* ou le Guide d'utilisation *IBM Security QRadar Log Manager*

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

Pour passer en revue la liste complète des options de profil d'analyse que vous pouvez configurer, voir **Configuration du profil d'analyse**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **When To Scan**

Etape 7 Dans la zone de liste **Run Schedule**, sélectionnez, **Manual**.

Etape 8 Cliquez sur le panneau extensible **What To Scan**

Etape 9 Dans le panneau **Include Saved Searches**, identifiez votre recherche d'actif sauvegardée dans le champ **Available Saved Searches**, puis cliquez sur **Add**.

Etape 10 Cliquez sur **Save**.

Etape suivante

Exécuter les étapes dans la procédure, **Exécution manuelle d'un profil d'analyse**.

Facultatif. Au cours et à la fin de l'analyse planifiée, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse. Pour plus d'informations, voir **Affichage des profils d'analyse**.
- Passer en revue les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Analyse des domaines sur une base mensuelle

Vous pouvez configurer un profil d'analyse de sorte qu'il analyse chaque mois les domaines figurant sur votre réseau.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Create**.

Etape 4 Dans le panneau extensible **Scan Profile**, entrez un nom pour votre profil d'analyse dans le champ **Profile Name**.

Remarque : Le nombre de caractères qui composent le nom du profil doit être supérieur à 4.

Etape 5 Facultatif. Entrez une description de profil d'analyse dans le champ **Profile Description**.

Etape 6 Cliquez sur le panneau extensible **When To Scan**

Etape 7 Dans la zone de liste **Run Schedule**, sélectionnez **Monthly**.

Etape 8 Dans le champ **Start Time**, sélectionnez l'heure de début et de fin de votre analyse.

Etape 9 Dans le champ **Day of the month**, sélectionnez un jour pour chaque mois au cours duquel votre analyse s'exécute.

Etape 10 Cliquez sur le panneau extensible **What To Scan**

Etape 11 Dans le champ **Domains**, entrez l'URL de l'actif que vous voulez analyser.

Etape 12 Cliquez sur **Add**.

Etape 13 Facultatif. Répétez **Etape 11** et **Etape 12**, pour chaque domaine que vous voulez analyser.

Etape 14 Cliquez sur **Save**.

Etape suivante

Facultatif. Au cours et à la fin de l'analyse planifiée, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse planifiée. Pour plus d'informations, voir **Affichage des profils d'analyse**.
- Passer en revue les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Modification d'un profil d'analyse

Vous pouvez modifier les paramètres d'un profil d'analyse existant.

A propos de cette tâche

Si vous modifiez un profil d'analyse, vous ne pouvez pas changer le **Type d'analyse** que vous avez sélectionné lors de la création du profil d'analyse d'origine.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Sélectionnez le profil d'analyse que vous voulez modifier.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Edit**.

Etape 5 Modifiez les paramètres décrits dans **Configuration du profil d'analyse**.

Etape 6 Cliquez sur **Save**.

Suppression d'un profil d'analyse

Vous pouvez supprimer un profil d'analyse.

ATTENTION : *Aucun message d'avertissement ne s'affiche lorsque vous supprimez un profil d'analyse. Votre profil d'analyse est immédiatement supprimé.*

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Sélectionnez le profil d'analyse que vous voulez supprimer.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Delete**.

Impression de profils d'analyse

Vous pouvez imprimer des exclusions globales.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 **Dans le menu de navigation, sélectionnez Administrative >** Scan Profiles.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Print**.

Etape 4 Sur la page Print, cliquez sur **Print**.

Export de profils d'analyse

Vous pouvez exporter des profils d'analyse au format XML (Entensible Markup Language) ou au format CSV (comma-separated values).

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Choisissez l'une des options suivantes :

- Dans la barre d'outils, sélectionnez **Actions > Export to XML**.
- Dans la barre d'outils, sélectionnez **Actions > Export to CSV**.

Etape 4 Choisissez l'une des options suivantes dans la fenêtre de dialogue **Waiting for export to commence** :

- Facultatif. Pour générer un courriel de confirmation, sélectionnez **Notify When Done**.
- Facultatif. Pour annuler l'exportation, sélectionnez **Cancel Export**.

Exécution manuelle d'un profil d'analyse

Vous pouvez exécuter manuellement un profil d'analyse.

A propos de cette tâche

Les analyses peuvent également être planifiées. Pour plus d'informations, voir **Configuration du profil d'analyse**.

Avant de commencer

Si vous tentez d'exécuter une analyse et que le processeur QRadar Vulnerability Manager n'est pas déployé, un message d'erreur s'affiche.

Pour déployer un processeur QRadar Vulnerability Manager, voir **Déploiement d'un processeur**.

Avant de pouvoir exécuter manuellement un profil d'analyse, vous devez en créer et le sauvegarder puis définir **Run Schedule** dans le panneau **When To Scan** sur **Manual**. Pour plus d'informations, voir **Configuration du profil d'analyse**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Administrative > Scan Profiles**.

Etape 3 Sélectionnez le profil d'analyse que vous voulez exécuter.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Run Now**.

Etape suivante

Au cours et à la fin de l'analyse, vous pouvez effectuer les tâches suivantes :

- Contrôler l'avancement de votre analyse. Pour plus d'informations, voir **Affichage des profils d'analyse**.

- Passer en revue les résultats de l'analyse terminée. Pour plus d'informations, voir **Affichage des résultats d'analyse**.

Connectivité d'analyse de correctif Windows.

Pour analyser un correctif des systèmes Windows sur votre réseau, vous devez activer les services Windows.

Les administrateurs doivent effectuer dans l'ordre les actions suivantes :

1. Activation de l'accès au registre distant.
   Voir **Activation de l'accès au registre distant**.
2. Activation de l'Interface de Gestion Windows (Windows Management Interface).
   Voir **Activation de l'interface de gestion Windows**.

Pare-feux et WMI Windows

Si vous devez lire des données WMI sur un serveur distant, il vous faut activer les connexions entre votre console QRadar et le serveur que vous contrôlez. Si le serveur utilise un pare-feu Windows, vous devez configurer le système pour activer les requêtes de l'Interface de Gestion Windows (WMI) distant.

Le modèle DCOM appelle un ordinateur distant

Si le compte que vous utilisez pour contrôler le serveur Windows n'est pas un administrateur sur ce dernier, vous devez l'autoriser à interagir avec le modèle DCOM.

Activation de l'accès au registre distant

Vous pouvez configurer votre registre Windows pour activer l'analyse de correctif Windows.

Procédure

Etape 1 Connectez-vous à votre système Windows.

Etape 2 Cliquez sur le bouton **Start**.

Etape 3 Dans le champ **Search programs and files**, entrez **services** puis appuyez sur **Enter**.

Etape 4 Dans la fenêtre Services, localisez le service **Remote Registry.**

Etape 5 Faites un clic droit sur le service **Remote Registry**, puis cliquez sur **Start**.

Etape 6 Fermez la fenêtre **Services**.

Etape suivante

Exécuter les étapes dans la procédure, **Activation de l'interface de gestion Windows**.

Activation de l'interface de gestion Windows

Vous pouvez activer votre interface de gestion Windows pour activer l'analyse du correctif Windows.

Avant de commencer

Exécuter les étapes dans la procédure, **Activation de l'accès au registre distant**.

Procédure

Etape 1 Connectez-vous à votre système Windows.

Etape 2 Cliquez sur le bouton **Start**.

Etape 3 Dans le champ **Search programs and files**, entrez, **computer management** puis appuyez sur **Enter**.

Etape 4 Déployez le menu de navigation **Services and Applications**

Etape 5 Dans le menu de navigation, cliquez avec le bouton droit de la souris sur **WMI Control** puis sélectionnez **Properties**.

Etape 6 Cliquez sur l'onglet **Security**.

Etape 7 Cliquez sur **Security**.

Etape 8 Facultatif. Pour ajouter un utilisateur ou groupe d'analyse :

- **a** Cliquez sur **Add**.
- **b** Dans le champ **Enter the object names to select** entrez le nom de groupe d'utilisateurs ou d'utilisateur.
- **c** Cliquez sur **OK**.

Etape 9 Dans le panneau **Permissions for Administrators** sélectionnez **Allow** pour l'option **Remote Enable**.

Etape 10 Cliquez sur **OK**.

Etape suivante

Facultatif. Si WMI présente des anomalies, vous pouvez installer WMI Administrative Tools de Microsoft. Il comprend un navigateur WMI qui vous aide à vous connecter à un ordinateur distant et à parcourir les informations WMI. Ceci vous aidera à isoler tout problème de connectivité dans un environnement plus direct et plus simple.

4 ANALYSE DE RÉSULTATS

QRadar Vulnerability Manager fournit deux façons d'examiner vos données de vulnérabilité ; l'analyse des résultats et la gestion des vulnérabilités.

Vous pouvez utiliser Scan results pour étudier les hôtes, les vulnérabilités et les services ouverts découverts via l'exécution d'analyses. Pour plus d'informations sur les profils d'analyse, voir **Configuration du profil d'analyse**.

Manage Vulnerabilities fournit une vue de réseau de la posture de votre vulnérabilité actuelle et un moyen puissant de rechercher, de filtrer et de visualiser vos données de vulnérabilité. Pour plus d'informations, voir **Gérer les vulnérabilités**.

QRadar Vulnerability Manager vous permet d'afficher les résultats d'analyse pour chaque hôte et de créer des règles d'exception de vulnérabilité. Pour plus d'informations, voir **Gérer des règles d'exception**.

Vous pouvez étudier de manière détaillée les services ouverts et les vulnérabilités associés à des hôtes spécifiques et visualiser des informations sur le risque qu'une vulnérabilité pose à votre entreprise.

Utilisez Scan Results pour effectuer les tâches suivantes :

- Examiner les informations sur les résultats d'analyse existants. Pour plus d'informations, voir **Affichage des résultats d'analyse**.
- Rechercher vos résultats d'analyse. Pour plus d'informations, voir **Recherche de résultats d'analyse**.

Barre d'outils des résultats d'analyse

Une barre d'outils est disponible sur la page **Scan Results** de l'onglet **Vulnerabilities**.

Vous pouvez accéder aux options suivantes sur la barre d'outils Scan Results :

Tableau 4-1 Options de la barre d'outils des résultats de l'analyse

Option	Description
Search	**New Search** - Sélectionnez cette option pour rechercher les résultats d'analyse. Pour plus d'informations, voir **Recherche de résultats d'analyse**. **Edit Search** - Sélectionnez cette option pour modifier une recherche de vos résultats d'analyse.
Actions	**Run Now** - Sélectionnez cette option pour lancer une analyse ou pour réexécuter une analyse terminée. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**. **Cancel** - Sélectionnez cette option pour annuler une analyse en cours d'exécution. Pour plus d'informations, voir **Annulation d'analyse de vulnérabilité**. **Delete** - Sélectionnez cette option pour supprimer un ensemble de résultats d'analyse. Pour plus d'informations, voir **Suppression d'analyses de vulnérabilité**. **Pause** - Sélectionnez cette option pour mettre en pause une analyse en cours d'exécution. **Resume** - Sélectionnez cette option pour démarrer une analyse qui présente un état "mis en pause". **Print** - Sélectionnez cette option pour imprimer les résultats d'analyse. **Export to XML** - Sélectionnez cette option pour exporter les résultats d'analyse en format XML. Pour plus d'informations, voir **Export de résultats d'analyse de vulnérabilité**. **Export to CSV** - Sélectionnez cette option pour exporter les résultats d'analyse en format CSV. Pour plus d'informations, voir **Export de résultats d'analyse de vulnérabilité**.

Affichage des résultats d'analyse

La page Scan Results affiche une liste récapitulative des résultats générés en exécutant un profil d'analyse.

À propos de cette tâche

La page Scan Results fournit les informations suivantes :

Tableau 4-2 Paramètres de liste de résultats d'analyse

Paramètre	Description
Profil	Nom du profil d'analyse. Placez le curseur de votre souris sur le **Profil** pour que s'affichent les informations sur le profil d'analyse et l'état de l'analyse. Pour plus d'informations sur les Profils d'analyse, voir **Configuration du profil d'analyse**.

Tableau 4-2 Paramètres de liste de résultats d'analyse (suite)

Paramètre	Description
Schedule	Planning d'exécution appliqué au profil d'analyse. **Manual** s'affiche si vous lancez une analyse manuelle. Pour plus d'informations sur l'exécution d'un profil d'analyse, voir **Exécution manuelle d'un profil d'analyse**.
Score	Note standardisée du CVSS (Common Vulnerability Scoring System) pour l'analyse. Cette note vous aide à classer les vulnérabilités en ordre de priorité.
Hosts	Nombre d'hôtes identifiés et analysés lors de l'exécution du profil d'analyse. Cliquez sur le lien de colonne **Hôte** pour que s'affichent les données de vulnérabilité pour les hôtes analysés. Pour plus d'informations, voir **Affichage des résultats d'analyse relatifs aux hôtes**.
Vulnerabilities	Nombre de différents types de vulnérabilités trouvés via un processus d'analyse. Cliquez sur le lien de colonne **Vulnérabilités** pour que s'affichent toutes les vulnérabilités uniques. Pour plus d'informations, voir **Affichagedes vulnérabilités de résultats d'analyse**.
Vulnerability Instances	Nombre de vulnérabilités trouvées via le processus d'analyse.
Open Services	Nombre de services ouverts uniques trouvés via le processus d'analyse. Un service ouvert unique est comptabilisé comme tel. Cliquez sur le lien de colonne **Services ouverts** pour que s'affichent les vulnérabilités classées selon le service ouvert. Pour plus d'informations, voir **Affichage des services ouverts de résultats d'analyse**.
Status	Les options de l'état du profil d'analyse comprennent : • Stopped - Cet état s'affiche si l'analyse s'est terminée avec succès ou si elle a été annulée. • Running - L'analyse est en cours d'exécution • Paused - L'analyse est momentanément interrompue. • Not Started - L'analyse n'est pas encore lancée.
Progress	Indique l'état d'avancement de l'analyse. >Placez le curseur de votre souris sur la barre de progression, pendant l'exécution de l'analyse pour que s'affichent les informations relatives à l'état d'avancement de l'analyse.
Start Date/Time	Indique la date et l'heure auxquelles a commencé l'exécution du profil d'analyse.
Duration	Affiche le temps pris pour l'exécution complète de l'analyse.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilités**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Recherche de résultats d'analyse

Vous pouvez rechercher et filtrer des résultats d'analyse afin que seuls les résultats auxquels vous êtes intéressés s'affichent.

À propos de cette tâche

Utilisez les informations contenues dans le tableau suivant pour configurer la recherche de vos résultats d'analyse :

Tableau 4-3 Paramètres de recherche de résultats d'analyse

Paramètre	Description
Scan Profile	Sélectionnez le profil d'analyse que vous voulez rechercher.
Network Group	Dans la zone de liste, sélectionnez le Groupe de réseaux que voulez rechercher.
Scan Status	Sélectionnez l'état d'analyse actuelle de l'analyse que vous voulez rechercher. Choisissez parmi ces options : • Any • Stopped • Running • Paused
Contains Asset With Name	Entrez le nom de l'actif que vous voulez rechercher.
Exécution d'analyse au cours des derniers jours	Entrez le nombre de jours au cours desquels vous voulez rechercher les analyses terminées.
Contains IP	Entrez une adresse IP pour rechercher vos Résultats d'analyse pour une adresse IP spécifique.
Contains Vulnerability	Cliquez sur **Browse** pour sélectionner la vulnérabilité que vous voulez rechercher.
Most recent scan only	Cochez cette case à cocher pour afficher les résultats relatifs à l'analyse exécutée en dernier pour chaque profil d'analyse.
Exclude on demand scan	Sélectionnez cette case à cocher si vous ne voulez pas que les résultats des analyses que vous avez exécutées manuellement s'affichent.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilités**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Dans la barre d'outils, sélectionnez **Search > New Search**.

Etape 4 Configurez votre recherche sur la base des critères décrits dans **Tableau 4-3**.

Etape 5 Cliquez sur **Search**.

Annulation d'analyse de vulnérabilité

Vous pouvez annuler une vulnérabilité qui est **En cours d'exécution** ou **mise en pause**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilités**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Sélectionnez l'analyse que vous souhaitez annuler.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Cancel**.

Résultats

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

Remarque : Un état **Stopped** peut également indiquer qu'une analyse s'est terminée avec succès.

Suppression d'analyses de vulnérabilité

Vous pouvez supprimer une analyse de vulnérabilité dont l'état est **Paused** ou **Stopped**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Sélectionnez l'analyse que vous voulez supprimer.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Delete**.

Export de résultats d'analyse de vulnérabilité

Vous pouvez exporter des résultats d'analyse de vulnérabilité en format XML ou en format CSV.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Choisissez l'une des options suivantes :

- Dans la barre d'outils, sélectionnez **Actions > Export to XML**.
- Dans la barre d'outils, sélectionnez **Actions > Export to CSV**.

Etape 4 Facultatif. Dans la boîte de dialogue **Waiting for export to commence**, sélectionnez l'une des options suivantes :

- Cliquez sur **Notify When Done** pour être avisé par courriel de la fin de l'export.
- Cliquez sur **Cancel Export** pour annuler l'export.

Etape 5 Suivez les instructions qui apparaissent à l'écran pour sauvegarder ou ouvrir le fichier que vous avez exporté.

Affichage des résultats d'analyse relatifs aux hôtes

Vous pouvez afficher des informations sur l'hôte analysé et examiner le nombre de vulnérabilités classées selon le risque qu'elles posent.

À propos de cette tâche

La barre d'outils **Actions** sur la page Scan Results Host fournit les options suivantes :

Tableau 4-4 Barre d'outils des hôtes des résultats de l'analyse

Options	Description
Print	Sélectionnez cette option pour imprimer la liste récapitulative des données de vulnérabilité regroupées selon l'actif.
Export to XML	Sélectionnez cette option pour exporter la liste récapitulative des données de vulnérabilité en format XML.
Export to CSV	Sélectionnez cette option pour exporter la liste récapitulative des données de vulnérabilité en format CSV.

La page Scan Results Hosts fournit les informations suivantes :

Tableau 4-5 Paramètres de pages des hôtes des résultats d'analyse

Paramètre	Description
IP Address	L'adresse IP de l'actif analysé. Pour plus d'informations sur l'actif analysé, sélectionnez l'une des options suivantes : • Placez le curseur de votre souris sur le lien de colonne **Adresse IP**. • Cliquez sur le lien de colonne **Adresse IP** pour que s'affiche la fenêtre Détails de l'actif. • Faites un clic droit sur le lien de colonne **Adresse IP** pour accéder aux options suivantes : - Navigate - sélectionnez cette option pour accéder aux informations sur la violation associée à l'actif analysé. - Information - sélectionnez cette option pour rechercher des événements et des flux et afficher également des informations sur l'actif. - Run QVM Scan - sélectionnez cette option pour analyser de nouveau un actif. Pour plus d'informations sur Asset Details, les violations, et les options du menu contextuel de l'actif, voir le *IBM Security QRadar SIEM Guide d'utilisation* ou le *IBM Security QRadar Log Manager Guide d'utilisation.*
Nom d'hôte	Nom d'hôte de l'hôte analysé. Il s'agit d'identificateur spécifique au réseau associé à cet hôte.
OS	Le système d'exploitation qui s'exécute sur l'hôte analysé.
Note	La note du CVSS basée sur les vulnérabilités trouvées sur l'hôte.

Tableau 4-5 Paramètres de pages des hôtes des résultats d'analyse (suite)

Paramètre	Description
Instances de Services Ouverts	Nombre d'instances de services ouverts trouvés sur l'hôte. Cliquez sur le lien de colonne **Instances de Services Ouverts** pour que s'affichent toutes les instances de services ouverts trouvées sur l'hôte. Pour plus d'informations, voir **Affichage des instances de services ouverts**.
Instances de vulnérabilité	Nombre d'instances de vulnérabilité trouvées sur l'hôte. Cliquez sur le lien de colonne **Instances de vulnérabilité** pour visualiser toutes les instances de vulnérabilité trouvées sur l'hôte. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**
Élevé	Nombre de vulnérabilités à risque élevé trouvées sur l'hôte.
Moyen	Nombre de vulnérabilités à risque moyen trouvées sur l'hôte.
Faible	Nombre de vulnérabilités à faible risque trouvées sur l'hôte.
Avertissement	Le nombre de vulnérabilités à très faible risque mais potentiellement importantes trouvées sur l'hôte.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Cliquez sur le lien de colonne **Hosts** associé à l'hôte que vous voulez étudier.

Affichage des instances de vulnérabilité

Vous pouvez afficher des informations sur l'hôte analysé et les vulnérabilités trouvées sur ce dernier.

À propos de cette tâche

Vous pouvez accéder aux options suivantes sur la barre d'outils Vulnerability Instances Host Details :

Tableau 4-6 Options de la barre d'outils des détails sur l'hôte des instances de vulnérabilité.

Fonction	Description
Vulnerabilities	Cliquez sur **Vulnérabilités** pour actualiser la liste des vulnérabilités trouvées sur l'hôte.
Open Services	Cliquez sur **Services ouverts** pour visualiser les services ouverts trouvés sur l'hôte. Pour plus d'informations, voir **Affichage des instances de services ouverts**.
Host Details	Cliquez sur **Host Details** pour que s'affiche la fenêtre **Asset Details**. Pour plus d'informations, voir le guide d'utilisation *IBM Security QRadar SIEM* ou le guide d'utilisation *IBM Security QRadar Log Manager.*

Tableau 4-6 Options de la barre d'outils des détails sur l'hôte des instances de vulnérabilité. (suite)

Fonction	Description
Actions	**Exception** - Sélectionnez cette option pour créer une exception de vulnérabilité. Pour plus d'informations, voir **Création d'une exception de vulnérabilité**. **Print** - Sélectionnez cette option pour imprimer les vulnérabilités trouvées sur l'hôte. **History** - Sélectionnez cette option pour visualiser les détails sur l'historique de la vulnérabilité. Pour plus d'informations, voir **Affichage de l'historique de vulnérabilité**.

Les informations suivantes figurent en haut de la page Vulnerability Instances Host Details :

Tableau 4-7 Paramètres de pages des détails sur l'hôte des instances de vulnérabilité

Paramètre	Description
Adresse IP	Adresse IP de l'hôte analysé.
Scan Profile	Nom du profile d'analyse utilisé pour analyser l'hôte, notamment la date et l'heure auxquelles l'hôte a été analysé.
Host Name	Nom de l'hôte sur lequel les services ouverts et les vulnérabilités ont été trouvés.
OS	Le système d'exploitation qui s'exécute sur l'hôte analysé.
Vulnerability Instances	Nombre d'instances de vulnérabilité trouvées sur l'hôte. Cliquez sur le lien **Instances de vulnérabilité** pour actualiser la liste active des vulnérabilités.
Network Group	Le groupe de réseaux dans lequel réside l'hôte.
ID Method	La méthode utilisée par le scanner pour détecter l'hôte.
Open Services Instances	Nombre d'instances de services ouverts trouvés sur l'hôte. Cliquez sur le lien **Instances de services ouverts** pour que s'affichent tous les services ouverts trouvés sur l'hôte. Voir **Affichage des instances de services ouverts**.

Les données de vulnérabilité suivantes figurent au bas de la page Vulnerability Instances :

Tableau 4-8 Paramètres de vulnérabilités

Paramètre	Description
Risk	Le niveau de risque associé à la vulnérabilité.
Severity	Le niveau de gravité associé à la vulnérabilité.
Vulnerability	Description de la vulnérabilité. Cliquez sur le lien **Vulnérabilité** pour que s'affiche la fenêtre Détails de Vulnérabilité. Pour plus d'informations, voir **Affichage de l'historique de vulnérabilité**.

Tableau 4-8 Paramètres de vulnérabilités (suite)

Paramètre	Description
Score	Le risque associé à la vulnérabilité.
Details	Les produits et versions logiciels exposés à la vulnérabilité.
Services	Les services associés à la vulnérabilité trouvée sur l'hôte.
Date Found	La date et l'heure auxquelles la vulnérabilité a été trouvée sur l'hôte.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Cliquez sur le lien de colonne **Hôtes**.

Etape 4 Cliquez sur le lien de colonne **Instances de vulnérabilité**

Affichage des instances de services ouverts

Vous pouvez afficher des informations sur un hôte analysé et les services ouverts trouvés sur ce dernier.

À propos de cette tâche

Vous pouvez accéder aux options suivantes sur la barre d'outils Open Instances Host Details :

Tableau 4-9 Barre d'outils des détails sur l'hôte des instances de service ouvert

Fonction	Description
Vulnérabilités	Cliquez sur **Vulnérabilités** pour visualiser les vulnérabilités trouvées sur l'hôte. Voir **Affichage des instances de vulnérabilité**
Open Services	Cliquez sur **Open Services** pour actualiser la liste des services ouverts trouvés sur l'hôte.
Détails sur l'hôte	Cliquez sur **Détails sur l'hôte** pour que s'affiche la fenêtre **Détails sur l'actif**. Pour plus d'informations, voir le Guide d'utilisation *IBM Security QRadar SIEM* ou le Guide d'utilisation *IBM Security QRadar Log Manager.*
Actions	Cliquez sur **Print** pour imprimer les instances de services ouverts.

Les informations détaillées sur l'hôte s'affichent en haut de la page et fournissent les précisions suivantes :

Tableau 4-10 Paramètres des détails sur l'hôte

Paramètre	Description
Adresse IP	Adresse IP de l'hôte analysé.
Scan Profile	Le nom du profil d'analyse qui a été utilisé pour générer les données des Instances du Service ouvert ainsi que l'heure et la date d'exécution du profil d'analyse.

Tableau 4-10 Paramètres des détails sur l'hôte (suite)

Paramètre	Description
Host Name	Nom de l'hôte sur lequel les services ouverts et les vulnérabilités ont été trouvés.
OS	Le système d'exploitation de l'hôte analysé.
Vulnerability Instances	Nombre d'instances de vulnérabilité trouvées sur l'hôte. Cliquez sur le lien **Instances de vulnérabilité** pour visualiser toutes les vulnérabilités trouvées sur l'hôte. Voir **Affichage des instances de vulnérabilité**.
Network Group	Le groupe de réseaux dans lequel réside l'hôte analysé. Cela permet d'identifier le noeud dans la hiérarchie de réseaux QRadar.
ID Method	La méthode utilisée par le scanner pour détecter l'hôte.
Open Services Instances	Nombre d'instances de services ouverts trouvées sur l'hôte. Cliquez sur le lien **Instances de Services Ouverts** pour actualiser la liste des instances de services ouverts.

Les informations sur les services ouverts s'affichent au bas de la page et fournissent les précisions suivantes :

Tableau 4-11 Paramètres des instances de services ouverts

Paramètre	Description
Service	Nom du service ouvert trouvé sur l'hôte.
Port	Le port sur lequel le service ouvert a été détecté. Dans le cas où le service spécifique n'est pas connu, vous voyez s'afficher Port.
Protocol(s)	Le protocole sur lequel le service ouvert s'exécute.
Description	Brève description du service ouvert.
Détails	Détails importants sur le service ouvert trouvé sur l'hôte.
Port par défaut	Le port par défaut associé au service ouvert.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Cliquez sur le lien de colonne **Hôtes**.

Etape 4 Cliquez sur le lien de colonne **Instances de services ouverts**

Affichage des vulnérabilités de résultats d'analyse

Vous pouvez afficher les vulnérabilités trouvées par un profil d'analyse, quel que soit l'hôte ou le service ouvert.

À propos de cette tâche

La page Scan Result Vulnerabilities affiche les informations suivantes :

Tableau 4-12 Paramètres des vulnérabilités des résultats d'analyse

Paramètre	Description
Risque	Le niveau de risque associé à la vulnérabilité.
PCI Severity	Affiche la gravité du risque que la vulnérabilité pose à l'architecture PCI. L'intervalle de gravité de l'architecture PCI est : • Absolue • Critique • Élevée • Moyenne • Faible
Vulnérabilité	Description de la vulnérabilité. Cliquez sur une **Vulnérabilité** pour que s'affiche la fenêtre Détails de vulnérabilité. Pour plus d'informations, voir **Affichage de l'historique de vulnérabilité**.
Hosts	Le nombre d'hôtes sur lesquels une vulnérabilité spécifique a été trouvée. Cliquez sur le lien de colonne **Hôtes** pour que s'affichent les hôtes sur lesquels la vulnérabilité a été trouvée. Voir **Affichage des résultats d'analyse relatifs aux hôtes**
Instances	Le nombre d'instances de la vulnérabilité sur tous les hôtes.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Cliquez sur le lien de colonne **Vulnerabilities**

Affichage des services ouverts de résultats d'analyse

Vous pouvez afficher tous les services ouverts trouvés par un profil d'analyse.

À propos de cette tâche

La page Scan Result Open Services affiche les informations suivantes :

Tableau 4-13 Paramètres de services ouverts de résultats d'analyse

Paramètre	Description
Service	Le service ouvert sur lequel la vulnérabilité a été trouvée.
Port par défaut	Le port par défaut associé au service ouvert.
Protocole(s)	Le protocole sur lequel le service ouvert a été trouvé.
Description	Brève description du service ouvert.

Tableau 4-13 Paramètres de services ouverts de résultats d'analyse (suite)

Paramètre	Description
Détails	Des informations plus détaillées sur le service ouvert trouvées via l'analyse. S'il existe plusieurs instances de service ouvert, cette colonne affiche Multiple(N) où N représente le nombre de services ouverts distincts. Lorsque Multiple(N) s'affiche, placez votre souris sur la valeur pour visualiser des détails sur les multiples services ouverts. S'il n' y a qu'un seul service ouvert distinct trouvé, cette colonne affiche les détails le concernant.
Hosts	Indique le nombre d'hôtes uniques trouvés via l'analyse contenant ce service ouvert. Cliquez sur le lien de colonne **Hôtes** pour que s'affichent les hôtes sur lesquels le service ouvert a été trouvé. Pour plus d'informations, voir **Affichage des résultats d'analyse relatifs aux hôtes**.
Vulnerability Instances	Nombre de vulnérabilités trouvées sur le service ouvert.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Scan Results**.

Etape 3 Cliquez sur le lien de colonne **Open Services**

5 GÉRER LES VULNÉRABILITÉS

Manage vulnerabilities est utilisé pour gérer les vulnérabilités sur votre infrastructure de réseau. Vous pouvez afficher les informations de vulnérabilité à jour en fonction des analyses que vous avez exécutées et fournir des analyses rétrospectives historiques de chaque vulnérabilité. Vous pouvez également filtrer vos données de vulnérabilité en fonction de la découverte et de la publication d'une vulnérabilité.

Les données de vulnérabilités qui s'affichent sont basées sur les informations du statut de vulnérabilité conservées dans le modèle d'actifQRadar. Ces informations n'incluent pas uniquement des vulnérabilités trouvées par le scannerQRadar Vulnerability Manager, mais également les vulnérabilités qui sont importées depuis des produits de scannage externes.

Utilisez Manage Vulnerabilities pour créer de puissants critères de filtrage enregistrés. Avec ces informations, vous pouvez créer des tableaux de bord de gestion de vulnérabilité ou des rapports planifiés, vous permettant de vous concentrer sur les vulnérabilités qui constituent le risque le plus élevé pour votre organisation.

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. Pour plus d'informations, voir **Assigner manuellement des vulnérabilités.**
- 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. Pour plus d'informations, voir **Créer une exception de vulnérabilité**.
- Affichez les informations historiques sur les vulnérabilités se trouvant sur votre réseau. Pour plus d'informations, voir **Affichage de l'historique de vulnérabilité**.

- Affichez les données de vulnérabilité par réseau, actif, vulnérabilité, service ouvert ou par instance de vulnérabilité.

Effectuer une recherche de vulnérabilité

Vous pouvez rechercher vos données de vulnérabilité par réseau, actif, vulnérabilité, service ouvert et par instance de vulnérabilité.

Avant de commencer

Avant de pouvoir effectuer une recherche sur vos données de vulnérabilité, vous devez créer un profil d'analyse puis analyser vos actifs de réseau. Pour plus d'informations, voir :

- **Configuration d'un profil de scan**
- **Exécuter manuellement un profil de scan**

A propos de cette tâche

Les recherches sauvegardées par défaut fournissent une évaluation de risque rapide pour votre organisation. Les recherches sauvegardées s'affichent dans la zone **Available Saved Searches** sur la page Vulnerability Manager Search.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, cliquez sur l'une des options suivantes :

- **Manage Vulnerabilities**

Remarque : Sélectionnez cette option pour afficher Vulnerability Instances. Pour plus d'informations, voir **Options d'affichage des données de vulnérabilité**.

- **Manage Vulnerabilities > By Network**.
- **Manage Vulnerabilities > By Asset**.
- **Manage Vulnerabilities > By Vulnerability**.
- **Manage Vulnerabilities > By Open Service**.

Etape 3 Sur la barre d'outils, sélectionnez **Search > New Search**.

Etape 4 Si vous souhaitez charger une recherche sauvegardée, procédez comme suit :

a Facultatif. Sélectionnez un groupe à partir de la zone de liste **Group** pour afficher les recherches disponibles pour ce groupe dans la liste **Available Saved Searches**.

b Choisissez une des options suivantes :

- Facultatif. Dans la zone **Type Saved Search or Select from List**, entrez le nom de la recherche que vous voulez charger.
- Dans la liste **Available Saved Searches**, sélectionnez la recherche sauvegardée que vous voulez charger.

c Cliquez sur **Load.**

d Sur la fenêtre de la boîte de dialogue, cliquez sur le bouton **OK**.

Remarque : La fenêtre de la boîte de dialogue s'affiche uniquement lorsque vous avez déjà chargé une recherche sauvegardée.

e Cliquez sur **Search**.

Etape 5 Si vous souhaitez créer une nouvelle recherche, exécutez les étapes suivantes dans le panneau **Search Parameters(s)** :

a Dans la première zone de liste, sélectionnez le paramètre que vous souhaitez utiliser.

b Dans la seconde zone de liste, sélectionnez le modificateur que vous voulez utiliser pour la recherche. Les modificateurs qui sont disponibles dépendent du paramètre qui est sélectionné dans la première zone de liste.

c Dans la troisième zone de liste, entrez ou sélectionnez les informations spécifiques qui sont relatives à votre paramètre de recherche.

d Cliquez sur **Add Filter**.

e Répétez ces étapes **a** dans **d** pour chaque filtre que vous voulez ajouter.

f Le filtre s'affiche dans la zone de texte **Current Filters**.

Pour plus d'informations sur les paramètres de recherche de vulnérabilité, voir **Paramètres de recherche de vulnérabilité**.

Etape 6 Cliquez sur **Search**.

Etape suivante

Vous pouvez enregistrer les critères de recherche de vulnérabilité. Pour plus d'informations, voir **Enregistrement des critères de recherche de vulnérabilité**.

Vous pouvez exporter les résultats de recherche de vulnérabilité dans les formats Extensible Markup Language (XML) ou de valeurs séparées par une virgule (CSV). Pour plus d'informations, voir **Exportation des résultats de recherche de vulnérabilité**.

Paramètres de recherche de vulnérabilité

Vous pouvez effectuer et enregistrer les recherches personnalisées de vos données de vulnérabilité.

Pour plus d'informations sur la recherche de vos données de vulnérabilité, voir **Effectuer une recherche de vulnérabilité**.

Vous pouvez sélectionner n'importe quelle option dans le tableau suivant pour effectuer une recherche sur des données de vulnérabilité :

Tableau 5-1 Paramètres de recherche du gestionnaire de vulnérabilité

Option	Description
Access Complexity	Affiche les vulnérabilités en fonction de la complexité de l'attaque requise pour exploiter la vulnérabilité. Les options incluent : High, Medium et Low.

Tableau 5-1 Paramètres de recherche du gestionnaire de vulnérabilité (suite)

Option	Description
Access Vector	Affiche les vulnérabilités en fonction de l'emplacement dans lequel ils peuvent être exploités. Les options incluent : • Local - exige que l'attaquant dispose soit de l'accès physique au système vulnérabilité ou à un compte local (interpréteur de commandes). • Adjacent_Network - exige que l'attaquant dispose de l'accès au même sous réseau tel que le logiciel vulnérable. • Network - nécessite que l'attaquant soit capable de se connecter au réseau.
Asset saved search	Affiche les vulnérabilités pour l'hôte, l'adresse IP ou l'intervalle des adresses IP associées à la recherche sauvegardée d'actif. Pour plus d'informations sur les recherches sauvegardées d'actif, voir **Qu'est-ce qu'il faut analyser**.
Assets with open service	Affiche les vulnérabilités sur les actifs qui contiennent les services ouverts spécifiques. Par exemple http, ftp et smtp.
Assigned User	Affiche les vulnérabilités pour l'utilisateur QRadar qui est affecté à la correction des vulnérabilités.
Authentication	Affiche les vulnérabilités en fonction du nombre d'heures qu'un attaquant doit s'authentifier par rapport à une cible pour exploiter une vulnérabilité. Les options incluent : Multiple_Instances, Single_Instance et None. ***Remarque :*** *Les vulnérabilités qui s'affichent avec une valeur d'authentification de* ***None*** *sont considérées pour poser un risque très élevé pour votre organisation.*
Availability Impact	Affiche les vulnérabilités en fonction du niveau où la disponibilité de ressource peut être compromise lorsqu'une vulnérabilité est exploitée. Les options incluent : None, Partial et Complete.
Confidentiality Impact	Affiche les vulnérabilités en fonction le niveau d'information confidentielle qui peut être obtenu lorsqu'une vulnérabilité est exploitée. Les options incluent : None, Partial et Complete.
CVE ID	Affiche les vulnérabilités en fonction d'une valeur unique qui identifie la vulnérabilité publiée. Cette valeur est conservée par National Vulnerability Database. ***Remarque :*** *Une vulnérabilité peut contenir zéro, un ou plusieurs ID CVE.*
CVSS Base Score	Affiche les vulnérabilités en fonction de l'évaluation CVSS (Common Vulnerability Scoring System) qui est affectée à la vulnérabilité. L'intervalle est compris entre zéro et 10, dans lequel zéro indique un risque faible et 10, un risque élevé.

Tableau 5-1 Paramètres de recherche du gestionnaire de vulnérabilité (suite)

Option	Description
Access Vector	Affiche les vulnérabilités en fonction de l'emplacement dans lequel ils peuvent être exploités. Les options incluent : • Local - exige que l'attaquant dispose soit de l'accès physique au système vulnérabilité ou à un compte local (interpréteur de commandes). • Adjacent_Network - exige que l'attaquant dispose de l'accès au même sous réseau tel que le logiciel vulnérable. • Network - nécessite que l'attaquant soit capable de se connecter au réseau.
Asset saved search	Affiche les vulnérabilités pour l'hôte, l'adresse IP ou l'intervalle des adresses IP associées à la recherche sauvegardée d'actif. Pour plus d'informations sur les recherches sauvegardées d'actif, voir **Qu'est-ce qu'il faut analyser**.
Assets with open service	Affiche les vulnérabilités sur les actifs qui contiennent les services ouverts spécifiques. Par exemple http, ftp et smtp.
Assigned User	Affiche les vulnérabilités pour l'utilisateur QRadar qui est affecté à la correction des vulnérabilités.
Authentication	Affiche les vulnérabilités en fonction du nombre d'heures qu'un attaquant doit s'authentifier par rapport à une cible pour exploiter une vulnérabilité. Les options incluent : Multiple_Instances, Single_Instance et None. ***Remarque :*** *Les vulnérabilités qui s'affichent avec une valeur d'authentification de* ***None*** *sont considérées pour poser un risque très élevé pour votre organisation.*
Availability Impact	Affiche les vulnérabilités en fonction du niveau où la disponibilité de ressource peut être compromise lorsqu'une vulnérabilité est exploitée. Les options incluent : None, Partial et Complete.
Confidentiality Impact	Affiche les vulnérabilités en fonction le niveau d'information confidentielle qui peut être obtenu lorsqu'une vulnérabilité est exploitée. Les options incluent : None, Partial et Complete.
CVE ID	Affiche les vulnérabilités en fonction d'une valeur unique qui identifie la vulnérabilité publiée. Cette valeur est conservée par National Vulnerability Database. ***Remarque :*** *Une vulnérabilité peut contenir zéro, un ou plusieurs ID CVE.*
CVSS Base Score	Affiche les vulnérabilités en fonction de l'évaluation CVSS (Common Vulnerability Scoring System) qui est affectée à la vulnérabilité. L'intervalle est compris entre zéro et 10, dans lequel zéro indique un risque faible et 10, un risque élevé.

Tableau 5-1 Paramètres de recherche du gestionnaire de vulnérabilité (suite)

Option	Description
Days since asset found	Indique les vulnérabilités en fonction sur le nombre de jours écoulés depuis la reconnaissance de l'actif associé 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. Pour plus d'informations, voir le Guide d'utilisation de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
Days since associated vulnerability service traffic	Affiche les vulnérabilités dans lesquels figurait le trafic de la couche 7 vers ou depuis un actif, en fonction du nombre de jours écoulé depuis la détection du trafic.
Days since vulnerabilities discovered	Affiche les vulnérabilités en fonction sur le nombre de jours écoulé depuis la première reconnaissance des vulnérabilités sur vos actifs de réseau.
Days since vulnerabilities published	Affiche les vulnérabilités récemment publiées.
Found by scan profile	Affiche les vulnérabilités en fonction du profil d'analyse que vous avez utilisé pour générer les résultats d'analyse. Pour plus d'informations sur la création d'un profil d'analyse, voir **Configuration d'un profil de scan**. ***Remarque :*** *Le paramètre* ***Found by scan profile*** *affiche tous les profils d'analyse, contrairement de l'emplacement du déploiement du processeurQRadar Vulnerability Manager. Par conséquent, si vous déployez votre processeur vers un hôte géré, la liste des profils d'analyse qui apparaît sur la page* ***Scan Profile*** *ne correspond pas à la liste de profiles d'analyse s'affichant sur la zone de liste* ***Found by scan profile****. Pour plus d'informations, voir* **Déploiement d'une application QRadar Vulnerability Manager**.
Found by scanner	Affiche les vulnérabilités qui sont basées sur le scanner qui a été utilisé pour analyser vos actifs de réseau. Pour plus d'informations sur les scanners, voir **Exécuter et scanner une vulnérabilité**.
Hostname	Affiche les vulnérabilités en fonction du nom d'hôte.
Impact	Affiche les vulnérabilités en fonction du potentiel impact sur votre organisation. Par exemple : la perte du contrôle d'accès, le temps d'indisponibilité et la perte de réputation.
Include early warnings	Affiche les vulnérabilités qui sont classées comme les premières vulnérabilités d'avertissement. Pour plus d'informations, voir **Vulnérabilités**.
Include exceptioned vulnerabilities	Affiche les vulnérabilités exclues et non exclues. Pour plus d'informations sur les exceptions de vulnérabilités, voir **Gestion des règles d'exception**.

Tableau 5-1 Paramètres de recherche du gestionnaire de vulnérabilité (suite)

Option	Description
Integrity Impact	Affiche les vulnérabilités en fonction du niveau auquel l'intégrité du système doit être compromise en cas d'exploitation des vulnérabilités. Les options incluent : None, Partial et Complete.
IPv4 Address	Affiche les vulnérabilités pour une adresse IP spécifique ou pour une plage d'adresses IP.
Network	Affiche les vulnérabilités en fonction du réseau dans lequel les vulnérabilités ont été découvertes.
Only include assets with risk	Affiche les vulnérabilités en fonction des actifs qui ont échoué ou transmis certaines politiques de risque. Pour plus d'informations sur les politiques, voir le Guide d'utilisation d'*IBM Security QRadar Risk Manager*. ***Remarque :*** *Les fonctions de ce paramètre sont uniquement opérationnelles une fois que vous avez installé IBM Security QRadar Risk Manager.*
Only include early warnings	Affiche les premières vulnérabilités d'avertissement. Pour plus d'informations sur Early Warning Vulnerabilities, voir **Alerte précoce liée aux vulnérabilités**.
Only include exceptioned vulnerabilities	Affiche les vulnérabilités qui sont exclues. Pour plus d'informations sur les exceptions de vulnérabilités, voir **Gérer des règles d'exception**. ***Remarque :*** *Utilisez ce paramètre de recherche afin qu'il vous aide dans la production de rapports d'auditeur affichant les vulnérabilités exclues.*
Only include PCI Failures	Affiche les vulnérabilités avec une évaluation CVSS qui est supérieure à quatre et une gravité PCI qui est urgente, critique ou majeure.
Overdue by days	Affiche les vulnérabilités en fonction du nombre de jours pendant lesquels une vulnérabilité tarde à se résoudre. Pour plus d'informations sur la correction des vulnérabilités, voir **Gérer la résolution des vulnérabilités**.
PCI Severity	Affiche les vulnérabilités en fonction de la gravité du risque posé par la vulnérabilité à Payment Card Industry (PCI). Les options incluent : Urgent, Critical, High, Medium et Low.
Risk	Affichent les vulnérabilités en fonction de la gravité posée par la vulnérabilité. Les options incluent : High, medium, low et warning.
Status	Affichent les vulnérabilités en fonction de leur statut dans le processus de correction de la vulnérabilité.
Unassigned	Affiche les vulnérabilités en fonction de l'éventualité d'affectation à un utilisateur QRadar en vue d'une correction.

Tableau 5-1 Paramètres de recherche du gestionnaire de vulnérabilité (suite)

Option	Description
Vulnerability	Affiche les vulnérabilités en fonction d'une recherche de vulnérabilités publiées. Cliquez sur **Browse** pour afficher la fenêtre Vulnerabilities Search. Pour plus d'informations sur les paramètres de cette fenêtre, voir **Recherches de vulnérabilités publiée**.
Vulnerability external reference	Affiche les vulnérabilités en fonction d'une importation de liste d'ID de vulnérabilités, par exemple ID CVE. Pour plus d'informations sur Reference Sets, voir le Guide d'administration de *IBM Security QRadar SIEM ou de IBM Security QRadar Log Manager.*
La vulnérabilité contient un correctif virtuel provenant du fournisseur	Affiche les vulnérabilités pouvant être corrigées virtuellement par une unité Intrusion Prevention System (IPS).
Vulnerabilities on open port	Affiche les vulnérabilités sur un ou plusieurs ports ouverts.
Vulnerabilities on open service	Affiche les vulnérabilités sur un ou plusieurs services ouverts. Par exemple, http, ssh et ftp.
Vulnerability reference	Affiche les vulnérabilités qui sont basées sur les informations de référence aux vulnérabilités externes.
Vulnerability state	Affiche les vulnérabilités en fonction de l'état de la vulnérabilité depuis la dernière analyse de votre réseau ou d'actifs spécifiques. Par exemple, lorsque vous effectuez une analyse, les vulnérabilités qui sont découvertes sont soit Either New, Pre-existing, Fixed ou Existing.
Quick Search	Affiche les vulnérabilités en fonction d'une recherche de texte libre. Vous pouvez rechercher un titre de vulnérabilités, une description, une solution et un ID de référence externe. Dans la zone de texte, vous pouvez utiliser les opérateurs **and ou not** et les crochets.

Options d'affichage des données de vulnérabilité

Lorsque vous effectuez une recherche de vulnérabilité, vous pouvez changer la manière d'afficher les données de vulnérabilité à l'aide de la zone de liste **Display**.

Vous pouvez utiliser les options suivantes pour afficher les données de vulnérabilité :

Tableau 5-2 Afficher les options de la zone de liste

Options	Description
Networks	Affiche les données de vulnérabilité par réseau. Pour plus d'informations, voir **Affichage des vulnérabilités par réseau**
Assets	Affiche les données de vulnérabilité par actif. Pour plus d'informations, voir **Affichage des vulnérabilités par actif**.

Tableau 5-2 Afficher les options de la zone de liste (suite)

Options	Description
Vulnerabilities	Affiche les vulnérabilités trouvées lorsque vos actifs de réseau sont analysés. Pour plus d'informations, voir **Affichage des données de vulnérabilité**.
Open Services	Affiche les données de vulnérabilité par service ouvert. Pour plus d'informations, voir **Affichage des vulnérabilités par service ouvert**.
Instances	Affiche chaque occurrence d'une vulnérabilité pour tous les actifs dans votre organisation. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.

Filtrage des données de vulnérabilité

Vous pouvez filtrer vos données de vulnérabilité par risque, par gravité PCI ou par l'impact posé par la vulnérabilité sur votre entreprise.

Les options du filtre sont disponibles lorsque vous cliquez avec le bouton droit de la souris sur les valeurs des données de vulnérabilité sur les pages suivantes :

- Manage Vulnerabilities > By Vulnerability Instances
- Manage Vulnerabilities > By Network
- Manage Vulnerabilities > By Asset
- Manage Vulnerabilities > By Vulnerability
- Manage Vulnerabilities > By Open Service

Vous pouvez sélectionner chacune des options dans le tableau suivant pour filtrer vos données de vulnérabilité :

Tableau 5-3 Options de filtre de données de la vulnérabilité

Filter	Options
Filter By Risk	Sélectionnez cette option pour filtrer vos données de vulnérabilité en fonction du risque posé par les vulnérabilités. Les options incluent : • High • Medium • Low • Warning

Tableau 5-3 Options de filtre de données de la vulnérabilité (suite)

Filter	Options
Filter By PCI Severity	Sélectionnez cette option pour filtrer vos données de vulnérabilité en fonction du niveau de gravité posé par la vulnérabilité à Payment Card Industry (PCI). Les options incluent : • Urgent • Critical • High • Medium • Low
Filter By Impact	Sélectionnez cette option pour filtrer vos données de vulnérabilité en fonction de l'éventuel impact métier lorsqu'une vulnérabilité est exploitée. Les options incluent : • Access Control Loss • Data Loss • Disclosure • Downtime • Information Theft • Monitoring Failure • Reputation Loss • System Loss

Gérer la barre d'outils des vulnérabilités

Une barre d'outils est fournie sur la page **Manage Vulnerabilities** sur l'onglet **Vulnerabilities**.

Vous pouvez accéder aux options suivantes sur la barre d'outils Manage Vulnerabilities :

Tableau 5-4 Options de la barre d'outils sur la vulnérabilité

Option	Description
Search	**New Search** - Sélectionnez cette option pour rechercher vos données de vulnérabilité. Pour plus d'informations, voir **Effectuer une recherche de vulnérabilité**. **Edit Search** - Sélectionnez cette option pour modifier une recherche de vulnérabilité.
Save Search Criteria	Sélectionnez cette option pour enregistrer vos critères de recherche de vulnérabilité et enregistrer les recherches dans la zone de liste de la barre d'outils **Quick Searches.** Pour plus d'informations, voir **Enregistrement des critères de recherche de vulnérabilité**.

Tableau 5-4 Options de la barre d'outils sur la vulnérabilité (suite)

Option	Description
Quick Searches	Sélectionnez **Quick Searches** pour exécuter des recherches de vulnérabilité précédemment sauvegardées. Les recherches précédemment sauvegardées s'affichent lorsque vous enregistrez vos critères de recherche. Pour plus d'informations, voir **Enregistrement des critères de recherche de vulnérabilité**. ***Remarque :*** *QRadar Vulnerability Manager est réparti avec plusieurs recherches sauvegardées.*
Actions	**Print** - Sélectionnez cette option pour imprimer les résultats de recherche de vulnérabilité. **Export to XML** - Sélectionnez cette option pour exporter les résultats de recherche de vulnérabilité dans le format Extensible Markup Language (XML). Voir **Exportation des résultats de recherche de vulnérabilité**. **Export to CSV** - Sélectionnez cette option pour exporter les résultats de recherche de vulnérabilité dans le format des valeurs séparées par une virgule (CSV). Voir **Exportation des résultats de recherche de vulnérabilité**. **Exception** - Sélectionnez cette option pour créer une exception de vulnérabilité. Pour plus d'informations, voir **Modification d'une règle d'exception de vulnérabilité**. ***Remarque :*** *Cette option s'affiche uniquement lorsque vous accédez aux pages By Vulnerability Instances ou By Vulnerabilities. Pour plus d'informations, voir* **Affichage des instances de vulnérabilité** *et* **Affichage des données de vulnérabilité**. **Assign/Edit** - Sélectionnez cette option pour affecter manuellement une vulnérabilité à un utilisateur QRadar en vue d'une correction. Pour plus d'informations, voir **Affectation manuelle de vulnérabilités**. ***Remarque :*** *Cette option s'affiche uniquement lorsque vous accédez à la page By Vulnerability Instances. Pour plus d'informations, voir* **Affichage des instances de vulnérabilité**. **History** - Sélectionnez cette option pour afficher les informations de l'historique de la vulnérabilité. Pour plus d'informations, voir **Affichage de l'historique de vulnérabilité**. ***Remarque :*** *Cette option s'affiche uniquement lorsque vous accédez à la page Vulnerability Instances. Pour plus d'informations, voir* **Affichage des instances de vulnérabilité**.
Quick Filter	Entrez vos critères de recherche dans le champ **Quick Filter** puis cliquez sur l'icône **Quick Filter** ou appuyez sur la touche Entrée sur le clavier. ***Remarque :*** *Lorsque vous cliquez dans la zone* ***Quick Filter****, une infobulle s'affiche, fournissant des informations sur la syntaxe adéquate pour l'utilisation de vos critères de recherche.*

Affichage des vulnérabilités par réseau

Vous pouvez regrouper et afficher les données de vulnérabilité pour chacun de vos réseaux.

Les données fournissent les informations sur le nombre de vulnérabilités sur votre réseau sur votre réseau, les actifs qui sont affectés et le nombre de vulnérabilités qui ne sont pas affectées ou qui accusent du retard conformément à la correction.

Si vous configurez les scanners tiers Vulnerability Assessment (VA), à l'aide de l'onglet QRadar **Admin**, alors les vulnérabilités qui sont détectées s'affichent automatiquement sur les pages **Manage Vulnerabilities**. Pour plus d'informations sur les scanners VA, voir *IBM Security QRadar SIEM Guide d'utilisation* ou *IBM Security QRadar Log Manager Guide d'utilisation*.

Avant de commencer

Pour afficher les données de vulnérabilité qui sont regroupées par actif, vous devez exécuter les tâches suivantes avant cette procédure :

1. Configurez votre hiérarchie de réseau. Pour plus d'informations, voir le Guide d'administration de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
2. Configurez un profil d'analyse. Pour plus d'informations, voir **Configuration du profil d'analyse**.
3. Exécutez un profil d'analyse. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.

A propos de cette tâche

La page Manage Vulnerabilities By Network affiche les informations suivantes :

Tableau 5-5 Gérer les vulnérabilités par les paramètres de réseau.

Paramètre	Description
Network	Le nom du réseau auquel appartiennent vos actifs analysés.
Score	L'évaluation moyenne accumulée Common Vulnerability Scoring System (CVSS) pour les vulnérabilités. L'intervalle est compris entre zéro et 10, dans lequel zéro indique un risque faible et 10, un risque élevé.
Assets	Le nombre total d'actifs sur chaque réseau.
Assets with Vulnerabilities	Le nombre total d'actifs sur le réseau contenant des vulnérabilités. Cliquez sur le lien de la colonne **Assets with Vulnerabilities** pour afficher les données de vulnérabilité regroupées par actif. Pour plus d'informations, voir **Affichage des vulnérabilités par actif**.
Open Services	Le nombre total de services ouverts sur chaque réseau.

Tableau 5-5 Gérer les vulnérabilités par les paramètres de réseau. (suite)

Paramètre	Description
Open Services with Vulnerabilities	Le nombre total de services ouverts sur chaque réseau contenant des vulnérabilités. Cliquez sur le lien de la colonne **Open Services with Vulnerabilities** pour afficher les données de vulnérabilité qui sont regroupées par service ouvert. Pour plus d'informations, voir **Affichage des vulnérabilités par service ouvert**.
Vulnerabilities	Le nombre des différents types de vulnérabilités trouvées sur les actifs de réseau analysés. Cliquez sur le lien de la colonne **Vulnerabilities** pour afficher les vulnérabilités sur vos actifs de réseau analysés. Pour plus d'informations, voir **Affichage des données de vulnérabilité**.
Vulnerability Instances	Le nombre de vulnérabilités trouvées sur les actifs de réseau analysés. Cliquez sur le lien de la colonne **Vulnerability Instances** pour afficher les vulnérabilités trouvées sur chaque actif analysé. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.
Unassigned	Le nombre de vulnérabilités trouvées sur les actifs de réseau analysés n'étant pas affectés à un utilisateur QRadar en vue d'une correction. Cliquez sur le lien de la colonne **Unassigned** pour afficher les vulnérabilités non affectées. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.
Overdue	Le nombre de vulnérabilités affectées à un utilisateur QRadar et non corrigées avant la date d'échéance. Cliquez sur le lien de la colonne **Overdue** pour afficher les vulnérabilités dont la correction accuse du retard sur l'échéance. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, sélectionnez **Manage Vulnerabilities > By Network**.

Etape suivante

La barre d'outils Manage Vulnerabilities By Network fournit les options pour rechercher et gérer vos vulnérabilités. Pour plus d'informations, voir **Gérer la barre d'outils des vulnérabilités**.

Vous pouvez cliquer avec le bouton droit de la souris sur vos données de vulnérabilités puis filtrer les résultats en fonction de la description des options dans **Tableau 5-3**.

Enregistrement des critères de recherche de vulnérabilité

Vous pouvez enregistrer vos critères de recherche de vulnérabilité pour une utilisation ultérieure.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Facultatif. Effectuez une recherche de vulnérabilité. Pour plus d'informations, voir **Effectuer une recherche de vulnérabilité**.

Etape 3 Sur la barre d'outils, cliquez sur **Save Search Criteria**.

Etape 4 Configurez les paramètres suivants :

Tableau 5-6 Enregistrer les paramètres de critères de recherche de vulnérabilité

Option	Description
Entrez le nom de cette recherche	Entrez le nom de la recherche que vous souhaitez enregistrer.
Include in my Quick Searches	Cochez cette case pour inclure la recherche sauvegardée dans la zone de liste **Quick Searches** sur la barre d'outils Manage Vulnerabilities.
Share with Everyone	Cochez cette case pour partager les critères de recherche sauvegardée avec tous les utilisateurs QRadar.
Assign Search to Groups(s)	Sélectionnez les groupes auxquels vous souhaitez affecter la recherche sauvegardée. Si vous ne sélectionnez pas les critères de recherche qu'un groupe affecte au groupe Other par défaut. Pour plus d'informations sur la gestion des groupes de recherche, voir le Guide d'utilisation de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
Set As Default	Cochez cette case pour afficher vos recherches sauvegardées lorsque vous affichez toutes les pages Manage Vulnerabilities.

Cliquez sur **OK**.

Suppression des critères de recherche de vulnérabilité enregistrée

Vous devez supprimer les critères de recherche de vulnérabilité enregistrée.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, sélectionnez **Manage Vulnerabilities > By Network**.

Etape 3 Sur la barre d'outils, sélectionnez **Search > New Search**.

Etape 4 Sur la page **Vulnerability Manager Search**, dans la liste **Available Saved Searches**, sélectionnez la recherche sauvegardée que vous souhaitez supprimer**.**

Etape 5 Cliquez sur **Delete**.

Etape 6 Cliquez sur le bouton **OK**.

Exportation des résultats de recherche de vulnérabilité

Vous pouvez exporter les résultats de recherche de vulnérabilité en format XML ou CSV.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, sélectionnez **Manage Vulnerabilities > By Network**.

Etape 3 Choisissez une des options suivantes :

- Dans la barre d'outils, sélectionnez **Actions > Export to XML**.
- Dans la barre d'outils, sélectionnez **Actions > Export to CSV**.

Etape 4 Facultatif. Dans la boîte de dialogue **Waiting for export to commence**, sélectionnez l'une des options suivantes :

- Cliquez sur **Notify When Done** pour être averti par courrier électronique une fois l'exportation terminée.
- Cliquez sur **Cancel Export** pour annuler l'exportation.

Etape 5 Suivez les instructions qui s'affichent à l'écran pour enregistrer ou pour ouvrir le fichier que vous avez exporté.

Affichage des vulnérabilités par actif

Vous pouvez rassembler et afficher les données de vulnérabilités pour chacun de vos actifs de réseau analysés.

Les données qui s'affichent fournissent des informations sur les actifs analysés, les nombres de vulnérabilités sur vos actifs mais également ceux des vulnérabilités qui ne sont pas affectées ou qui accusent du retard conformément à la correction.

Lorsque vous configurez des scanners Vulnerability Assessment (VA) tiers à l'aide de l'onglet QRadar **Admin** alors les vulnérabilités qui sont détectées s'affichent automatiquement sur les pages **Manage Vulnerabilities**. Pour plus d'informations sur les scanners VA, voir *IBM Security QRadar SIEM Guide d'utilisation* ou *IBM Security QRadar Log Manager Guide d'utilisation*.

Avant de commencer

Pour afficher les données de vulnérabilité qui sont regroupées par actif, vous devez exécuter les tâches suivantes avant cette procédure :

1. Configurez votre hiérarchie de réseau. Pour plus d'informations, voir le Guide d'administration de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
2. Configurez un profil d'analyse. Pour plus d'informations, voir **Configuration du profil d'analyse**.
3. Exécutez un profil d'analyse. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.

A propos de cette tâche

La page Manage Vulnerabilities By Asset affiche les informations suivantes :

Tableau 5-7 Gérer les vulnérabilités par paramètres d'actif.

Paramètre	Description
IP Address	L'adresse IP de l'actif analysé. Pour obtenir plus d'informations sur l'actif analysé, sélectionnez l'une des options suivantes : • Placez votre curseur sur le lien de la colonne **IP Address**. • Cliquez sur le lien de la colonne **IP Address** pour afficher la fenêtre Asset Details. • Cliquez avec le bouton droit de votre souris sur le lien de la colonne **IP Address** pour accéder aux options suivantes : - Navigate - sélectionnez cette option pour accéder aux informations de violation relatives à l'actif analysé. - Information - sélectionnez cette option pour rechercher des événements et flux puis affichez les informations d'actif. - Run QVM Scan - sélectionnez cette option pour ré-analyser un actif. Pour plus d'informations sur Asset Details, les violations et l'actif puis cliquez avec le bouton droit de la souris sur les options, voir le Guide d'utilisation de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
Asset Name	Le nom qui est affecté à l'actif analysé.
Score	L'estimation moyenne accumulée Common Vulnerability Scoring System (CVSS) pour toutes les vulnérabilités trouvées sur l'actif.
Open Services with vulnerabilities	Le nombre total des vulnérabilités de service ouvert trouvées sur l'actif analysé. Cliquez sur le lien de la colonne **Open Services with vulnerabilities** pour afficher les données de vulnérabilités regroupées par service ouvert. Pour plus d'informations, voir **Affichage des vulnérabilités par service ouvert**.

Tableau 5-7 Gérer les vulnérabilités par paramètres d'actif. (suite)

Paramètre	Description
Vulnerability Instances	Le nombre de vulnérabilités trouvées sur l'actif analysé. Cliquez sur le lien de la colonne **Vulnerability Instances** pour afficher les vulnérabilités trouvées sur l'actif analysé. Pour plus d'informations, voir **Affichage des instances de vulnérabilité Procédure**.
Unassigned	Le nombre de vulnérabilités trouvées sur l'actif analysé et non affectées à un utilisateur QRadar en vue d'une correction. Cliquez sur le lien de la colonne **Unassigned** pour afficher les vulnérabilités non affectées. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.
Overdue	Le nombre de vulnérabilités affectées à un utilisateur QRadar et non corrigées avant la date d'échéance. Cliquez sur le lien de la colonne **Overdue** pour afficher les vulnérabilités dont la correction accuse du retard sur l'échéance. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, sélectionnez **Vulnerability Manager > By Asset**.

Etape suivante

La barre d'outils Manage Vulnerabilities By Asset fournit plus d'options pour la recherche et la gestion de vulnérabilités trouvées sur votre réseau. Pour plus d'informations, voir **Gérer la barre d'outils des vulnérabilités**.

Vous pouvez cliquer avec le bouton droit de votre souris sur les données de vulnérabilités puis filtrer les résultats en fonction des options décrites dans **Tableau 5-3**.

Affichage des données de vulnérabilité

Vous pouvez afficher les informations sur les types de vulnérabilité trouvés via l'analyse d'actifs sur vos réseaux.

Les données qui s'affichent fournissent des informations sur le risque et le niveau de gravité que pose chaque vulnérabilité à votre organisation.

Lorsque vous configurez des scanners Vulnerability Assessment (VA) tiers à l'aide de l'onglet QRadar **Admin** alors les vulnérabilités qui sont détectées s'affichent automatiquement sur les pages **Manage Vulnerabilities**. Pour plus d'informations sur les scanners VA, voir *IBM Security QRadar SIEM Guide d'utilisation* ou *IBM Security QRadar Log Manager Guide d'utilisation*.

Avant de commencer

Pour afficher les donnés de vulnérabilité, vous devez exécuter les tâches suivantes avant d'entamer cette procédure :

1. Configurez votre hiérarchie de réseau. Pour plus d'informations, voir le Guide d'administration de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
2. Configurez un profil d'analyse. Pour plus d'informations, voir **Configuration du profil d'analyse**.
3. Exécutez un profil d'analyse. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.

A propos de cette tâche

La page Manage Vulnerabilities By Vulnerability fournit les informations suivantes :

Tableau 5-8 Gérer les vulnérabilités par les paramètres de la page de vulnérabilité.

Paramètre	Description
Vulnerability	Le nom de la vulnérabilité trouvée sur l'actif du réseau analysé. Cliquez sur le lien de la colonne **Vulnerability** pour afficher la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilité**.
PCI Severity	Le niveau de gravité posé par la vulnérabilité à Payment Card Industry (PCI). L'intervalle de gravité PCI est : • Urgent • Critical • High • Medium • Low
Risk	Le risque lié à la vulnérabilité. Les options incluent : High, Medium, Low et Warning.
CVE Id	L'ID Common Vulnerability and Exposure (CVE) est lié à la vulnérabilité. Cliquez sur le lien de la colonne **CVE Id** pour parcourir la National Vulnerability Database et afficher plus d'informations détaillées sur la vulnérabilité.
CVSS Score	L'évaluation CVSS (Common Vulnerability Scoring System) qui est affectée à la vulnérabilité. L'intervalle est compris entre zéro et 10, dans lequel zéro indique un risque faible et 10, un risque élevé.
Assets	Le nombre d'actifs trouvés pour contenir la vulnérabilité. Cliquez sur le lien de la colonne **Assets** pour afficher les informations sur l'actif dans lequel la vulnérabilité a été trouvée. Pour plus d'informations, voir **Affichage des vulnérabilités par actif**.

Tableau 5-8 Gérer les vulnérabilités par les paramètres de la page de vulnérabilité. (suite)

Paramètre	Description
Vulnerability Instances	Le nombre de vulnérabilités trouvées sur l'actif analysé. Cliquez sur le lien de la colonne **Vulnerability Instances** pour afficher les vulnérabilités trouvées sur l'actif. Pour plus d'informations, voir **Affichage des instances de vulnérabilité Procédure**.
Open Services with vulnerabilities	Le nombre total de services ouverts sur chaque réseau contenant des vulnérabilités. Cliquez sur le lien de la colonne **Open Services with Vulnerabilities** pour afficher les données de vulnérabilités regroupées par service ouvert. Pour plus d'informations, voir **Affichage des vulnérabilités par service ouvert**.
Unassigned	Le nombre de vulnérabilités non affectées à un utilisateur QRadar en vue d'une correction. Cliquez sur le lien de la colonne **Unassigned** pour afficher les vulnérabilités non affectées. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**
Overdue	Le nombre de vulnérabilités affectées à un utilisateur QRadar et non affectées avant la date d'échéance. Cliquez sur le lien de la colonne **Overdue** pour afficher les vulnérabilités dont la correction accuse du retard sur l'échéance. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, sélectionnez **Vulnerability Manager > By Vulnerability**.

Etape suivante

La barre d'outils Manage Vulnerabilities By Vulnerability fournit plus d'options pour la recherche et la gestion de vulnérabilités trouvées sur vos actifs de réseau. Pour plus d'informations, voir **Gérer la barre d'outils des vulnérabilités**.

Vous pouvez cliquer avec le bouton droit de votre souris sur les données de vulnérabilités puis filtrer les résultats en fonction des options décrites dans **Tableau 5-3**.

Affichage des vulnérabilités par service ouvert

Vous pouvez regrouper et afficher les données de vulnérabilité pour chaque service ouvert sur vos actifs de réseau.

Les données qui s'affichent fournissent des informations cruciales sur les services ouverts, depuis que les vulnérabilités peuvent facilement être exploitées sur des attaquants distants.

Avant de commencer

Pour afficher les données de vulnérabilité qui sont regroupées par service ouvert, vous devez exécuter les tâches suivantes avant d'entamer cette procédure :

1. Configurez un profil d'analyse. Pour plus d'informations, voir **Configuration du profil d'analyse**.
2. Exécutez un profil d'analyse. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.

A propos de cette tâche

La page Manage Vulnerabilities By Open Service affiche les informations suivantes :

Tableau 5-9 Gérer les vulnérabilités via l'ouverture des paramètres de service

Paramètre	Description
Service	Le nom des services ouverts trouvés sur les actifs de réseau analysés.
Default Port	Les numéros de port pour les vulnérabilités de service ouvert.
Description	La description du service ouvert.
Assets With Open Service Vulnerabilities	Le nombre d'actifs associés aux vulnérabilités de service ouvert. Cliquez sur le lien de la colonne **Assets with Open Services Vulnerabilities** pour afficher les vulnérabilités regroupées par actif. Pour plus d'informations, voir **Affichage des vulnérabilités par actif**.
Vulnerabilities	Le nombre des différents types de vulnérabilités. Cliquez sur le lien de la colonne **Vulnerabilities** pour afficher toutes les vulnérabilités pour le service ouvert qui vous intéresse. Pour plus d'informations, voir **Affichage des données de vulnérabilité**.
Vulnerability Instances	Le nombre de vulnérabilités associées au service ouvert. Cliquez sur le lien de la colonne **Vulnerability Instances** pour afficher les services ouverts associés aux vulnérabilités. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.
Unassigned	Le nombre de vulnérabilités n'ayant pas été affectées à un utilisateur QRadar en vue d'une correction. Cliquez sur le lien de la colonne **Unassigned** pour afficher les vulnérabilités non affectées. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.
Overdue	Le nombre de vulnérabilités affectées à un utilisateur QRadar et non corrigées avant la date d'échéance. Cliquez sur le lien de la colonne **Overdue** pour afficher les vulnérabilités dont la correction accuse du retard sur l'échéance. Pour plus d'informations, voir **Affichage des instances de vulnérabilité**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, sélectionnez **Vulnerability Manager > By Open Service**.

Etape suivante

La barre d'outils Manage Vulnerabilities By Open Service fournit plus d'options pour la recherche et la gestion de vulnérabilités trouvées sur vos actifs de réseau analysés. Pour plus d'informations, voir **Gérer la barre d'outils des vulnérabilités**.

Vous pouvez cliquer avec le bouton droit de votre souris sur les données de vulnérabilités puis filtrer les résultats en fonction des options décrites dans**Tableau 5-3**.

Affichage des instances de vulnérabilité

Vous pouvez afficher chaque vulnérabilité sur chaque actif de votre réseau.

Lorsque vous configurez des scanners Vulnerability Assessment (VA) tiers à l'aide de l'onglet QRadar **Admin** alors les vulnérabilités qui sont détectées s'affichent automatiquement sur les pages **Manage Vulnerabilities**. Pour plus d'informations sur les scanners VA, voir *IBM Security QRadar SIEM Guide d'utilisation* ou *IBM Security QRadar Log Manager Guide d'utilisation*.

Avant de commencer

Pour afficher les données de vulnérabilité, vous devez exécuter les tâches suivantes :

1. Configurez votre hiérarchie de réseau. Pour plus d'informations, voir le Guide d'administration de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
2. Configurez un profil d'analyse. Pour plus d'informations, voir **Configuration du profil d'analyse**.
3. Exécutez un profil d'analyse. Pour plus d'informations, voir **Exécution manuelle d'un profil d'analyse**.

A propos de cette tâche

La page Manage Vulnerabilities By Vulnerability Instances affiche les informations suivantes :

Tableau 5-10 Par paramètres d'instances de vulnérabilité

Paramètre	Description
IP Address	L'adresse IP de l'actif analysé. Pour obtenir plus d'informations sur l'actif analysé, sélectionnez l'une des options suivantes : • Placez votre curseur sur le lien de la colonne **IP Address**. • Cliquez sur le lien de la colonne **IP Address** pour afficher la fenêtre Asset Details. • Cliquez avec le bouton droit de votre souris sur le lien de la colonne **IP Address** pour accéder aux options suivantes : - Navigate - sélectionnez cette option pour accéder aux informations de violation relatives à l'actif analysé. - Information - sélectionnez cette option pour rechercher des événements et flux puis affichez les informations d'actif. - Run QVM Scan - sélectionnez cette option pour ré-analyser un actif. Pour plus d'informations sur Asset Details, les violations et l'actif puis cliquez avec le bouton droit de la souris sur les options, voir le Guide d'utilisation de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
Asset Name	Le nom de l'actif sur lequel la vulnérabilité a été trouvée.
Vulnerability	Le nom de la vulnérabilité trouvée sur l'actif du réseau analysé. Cliquez sur le lien de la colonne **Vulnerability** pour afficher la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilité**.
PCI Severity	Le niveau de gravité posé par la vulnérabilité à Payment Card Industry (PCI). L'intervalle de gravité PCI est : • Urgent • Critical • High • Medium • Low
Risk	Le risque lié à la vulnérabilité. Les options incluent : High, Medium, Low et Warning.
CVE Id	L'ID Common Vulnerability and Exposure (CVE) est lié à la vulnérabilité. Cliquez sur le lien de la colonne **CVE Id** pour parcourir la National Vulnerability Database et afficher plus d'informations détaillées sur la vulnérabilité.
CVSS Score	L'évaluation Common Vulnerability Scoring System (CVSS) qui est affectée à la vulnérabilité. L'intervalle est compris entre zéro et 10, dans lequel zéro indique un risque faible et 10, un risque élevé.

Tableau 5-10 Par paramètres d'instances de vulnérabilité (suite)

Paramètre	Description
Date Found	La date et l'heure pendant lesquelles la vulnérabilité a été trouvée sur l'actif.
Last Date Seen	La date à laquelle la vulnérabilité a été vue pour la dernière fois sur l'actif.
Assigned To	Le nom de l'utilisateur QRadar qui est affecté pour la correction de la vulnérabilité. Pour plus d'informations, voir **Affichage des vulnéranilités affectées**.
Status	L'état de la vulnérabilité affectée. Les options incluent : • **Opened** - Indique qu'une vulnérabilité est affectée pour la correction. Voir **Affectation manuelle de vulnérabilités**. • **Reopened** - Indique qu'une vulnérabilité n'est pas corrigée. ***Remarque :*** *Lorsque la correction automatique est activée et qu'une vulnérabilité précédemment corrigée et fermée est découverte par une nouvelle analyse, la vulnérabilité est rouverte. Pour plus d'informations, voir* **Configuration de la résolution automatique des vulnérabilités.** • **Fixed** - Indique qu'une vulnérabilité est corrigée. • **Manually Closed** - Indique qu'une vulnérabilité est corrigée. • **Auto Closed** - Ce statut indique une analyse ultérieure, utilisant le même profil d'analyse, ne trouve aucune vulnérabilité affectée sur l'actif dans lequel la vulnérabilité a précédemment été trouvée.
Due days	Le retard sur l'échéance en nombre de jours accusé par une vulnérabilité en vue d'une correction. Une valeur zéro s'affiche lorsqu'une vulnérabilité est affectée à un utilisateurQRadar. Le retard sur l'échéance de la période est réduite à la valeur d'un, pour une durée de vingt quatre heures de non correction d'une vulnérabilité.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, cliquez sur **Manage Vulnerabilities**.

Etape suivante

La barre d'outils Vulnerability Instances fournit plus d'options pour rechercher et gérer vos vulnérabilités. Pour plus d'informations, voir **Gérer la barre d'outils des vulnérabilités**.

Vous pouvez cliquer avec le bouton droit de votre souris sur vos données de vulnérabilité puis filtrer les résultats en fonction des options qui sont décrites dans **Tableau 5-3**.

Affichage de l'historique de vulnérabilité

Vous pouvez afficher l'historique d'une vulnérabilité. Par exemple, la date de détection de la vulnérabilité ou l'utilisateur affecté pour corriger la vulnérabilité.

La fenêtre Vulnerability History fournit les informations suivantes :

Tableau 5-11 Paramètres de l'historique de vulnérabilité

Paramètre	Description
Vulnerability History	
IP Address	Indique l'adresse IP de l'actif analysé. Pour obtenir plus d'informations sur l'actif analysé, sélectionnez l'une des options suivantes : • Placez votre curseur sur le lien **IP Address**. • Cliquez sur le lien **IP Address** pour afficher la fenêtre Asset Details. • Cliquez avec le bouton droit de votre souris sur le lien de la colonne **IP Address** pour accéder aux options suivantes : - Navigate - sélectionnez cette option pour accéder aux informations de violation relatives à l'actif analysé. - Information - sélectionnez cette option pour rechercher des événements et flux puis affichez les informations d'actif. - Run QVM Scan - sélectionnez cette option pour ré-analyser un actif. Pour plus d'informations sur Asset Details, les violations et l'actif puis cliquez avec le bouton droit de la souris sur les options, voir le Guide d'utilisation de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
Host Name	Le nom qui est affecté à l'actif analysé.
Vulnerability	Détails de la vulnérabilité trouvés sur l'actif analysé. Cliquez sur le lien **Vulnerability** pour afficher la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilité**.
Details	Indique les détails de l'application ou du logiciel qui est affecté par la vulnérabilité.
Vulnerability History Details	
Date	Indique la date à laquelle la vulnérabilité à été mise à jour. Par exemple, la date à laquelle une vulnérabilité a été affectée à un utilisateur en vue d'une correction.
User Name	Le nom de l'utilisateur ayant mis la vulnérabilité à jour.

Tableau 5-11 Paramètres de l'historique de vulnérabilité

Paramètre	Description
Comment	Lorsqu'une vulnérabilité est mise à jour, les commentaires qui s'affichent sont soit des commentaires du système automatiquement mis à jour soit des commentaires ajoutés par un utilisateur. Par exemple, lorsqu'une vulnérabilité est affectée pour la correction, l'utilisateur est invité à entrer les commentaires puis ces derniers s'affichent.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Sur le menu de navigation, sélectionnez **Vulnerability Manager > By Network**.

Etape 3 Sur la barre d'outils, sélectionnez **Actions > History**.

Barre d'outils sur l'historique de la vulnérabilité

Une barre d'outils est fournie sur la fenêtre Vulnerability History.

Vous pouvez accéder aux options suivantes sur la barre d'outils sur l'historique Vulnerability :

Tableau 5-12 Options de la barre d'outils sur l'historique de vulnérabilité

Option	Description
Print	Sélectionnez cette option pour imprimer les informations sur l'historique de vulnérabilité.
Details	Sélectionnez cette option pour afficher la fenêtre **Asset Details**. Pour plus d'informations, voir le Guide d'utilisation de *IBM Security QRadar SIEM* ou de *IBM Security QRadar Log Manager*.
Exception	Sélectionnez cette option pour créer une exception de vulnérabilité. Pour plus d'informations, voir **Création d'une execption de vulnérabilité**.
Assign/Edit	Sélectionnez cette option pour affecter manuellement une vulnérabilité à un utilisateur QRadar en vue d'une correction. Pour plus d'informations, voir **Affectation manuelle de vulnérabilités.**

6 GÉRER DES RÈGLES D'EXCEPTION

Si une vulnérabilité présente moins de risque à votre entreprise, vous pouvez empêcher cette dernière de s'afficher automatiquement lorsque vous recherchez des données de vulnérabilité.

Une règle d'exception retire le besoin d'affecter une vulnérabilité pour une résolution automatique ou manuelle. Pour plus d'informations sur la résolution de vulnérabilité, voir **Gestion de la vulnérabilité**.

Lorsque vous créez une exception de vulnérabilité, cette dernière n'est retirée de QRadar Vulnerability Manager. La vulnérabilité peut s'afficher en effectuant une recherche de vulnérabilité et en sélectionnant le filtre de recherche approprié. Pour plus d'informations, voir **Recherche d'exceptions de vulnérabilité**.

Barre d'outils des exceptions relatives aux vulnérabilités

Une barre d'outils est fournie sur la page **Vulnerability Exception** de l'onglet **Vulnerabilities**.

Vous pouvez accéder aux options sur la barre d'outils Exception Rules :

Tableau 6-1 La barre d'outils de la page des règles Exception

Option	Description
Edit	Sélectionnez cette option pour éditer une exception de vulnérabilité. Pour plus d'informations, voir **Modification d'une règle d'exception de vulnérabilité**.
Remove	Sélectionnez cette option pour supprimer une exception de vulnérabilité. Pour plus d'informations, voir **Suppression d'une règle d'exception de vulnérabilité**.
Export to XML	Sélectionnez cette option pour exporter la liste d'exceptions sous format Extensible Markup Language (XML). Pour plus d'informations, voir **Exportation d'une règle d'exception de vulnérabilité**.
Export to CSV	Sélectionnez cette option pour exporter la liste d'exceptions dans un langage de valeurs séparées par une virgule (CSV). Pour plus d'informations, voir **Exportation d'une règle d'exception de vulnérabilité**.

Afficher les exceptions relatives aux vulnérabilités

Vous pouvez afficher des informations sur les vulnérabilités qui sont considérées comme des exceptions, notamment le risque, la gravité et la raison de la règle d'exception.

Avant de commencer

Si vous n'avez pas créé une option Vulnerability Exception, aucune donnée ne s'affiche. Pour en savoir plus sur la création d'une option Vulnerability Exception, voir **Création d'une exception de vulnérabilité**.

A propos de cette tâche

La page Exception Rules fournit les informations suivantes :

Tableau 6-2 Les paramètres de la page de paramètres des règles d'exception

Paramètre	Description
Vulnerability	Le nom de la vulnérabilité auquel la règle d'exception est appliquée. Cliquez sur le lien de la colonne **Vulnerability** pour afficher la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilité**.
Risk Level	Le risque associé à la vulnérabilité mise en exception. Les options comprennent High, Medium, Low et Warning.
PCI Severity	Le niveau de gravité lié à la vulnérabilité mise en exception au PCI (Payment Card Industry). La plage de gravité PCI est : • Urgent • Critical • High • Medium • Low
IP Address	L'adresse IP de l'hôte dans lequel se trouve la vulnérabilité.
Expiry Date	La date à laquelle expire la règle d'exception.
Reason	La raison pour laquelle la règle d'exception a été créée. Les options incluent : • False Positive • Mitigated • Vendor Response • Temporarily Ignored • IPS Mitigated • Other
Last Date Updated	La date de la dernière mise à jour de la règle d'exception.
Last Update By	Le nom du dernier utilisateurQRadar ayant mis à jour la règle d'exception.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Vulnerability Exception**.

Créer une exception de vulnérabilité

Vous pouvez appliquer une règle d'exception à une vulnérabilité qui vous semble présenter moins de risque à votre entreprise.

Si vous créez une exception, la vulnérabilité ne s'affiche plus de façon automatique dans les résultats de la recherche QRadar Vulnerability Manager.

A propos de cette tâche

La fenêtre Maintain Exception Rule fournit les paramètres suivants :

Tableau 6-3 Conservationdes paramètres de la fenêtre de règles d'exception

Paramètre	Description
Exception Rule	
Vulnerability	Le nom de la vulnérabilité. Cliquez sur le nom **Vulnerability** pour afficher la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilités**.
Risk Level	Le risque associé à la vulnérabilité. Les options comprennent High, Medium, Low et Warning.
PCI Severity	Le niveau de gravité lié à la vulnérabilité au PCI (Payment Card Industry). La plage de gravité PCI est : • Urgent • Critical • High • Medium • Low
Reason	Sélectionnez une cause pour la création de l'exception de vulnérabilité. La valeur par défaut est False Positive. Choisissez l'une des options suivantes : • **False Positive** • **Mitigated** • **Vendor Response** • **Temporarily Ignored** • **IPS Mitigation** • **Other**

Tableau 6-3 Conservationdes paramètres de la fenêtre de règles d'exception (suite)

Paramètre	Description
Expiry Date	Entrez la date d'expiration de la règle d'exception qui correspond à votre localité ou sélectionnez une date à partir de la zone de liste. ***Remarque :*** *La zone Expiry Date peut être mise à jour si la case Never Expires est décochée.*
Never Expires	Cochez la case **Never Expires** si vous souhaitez que la règle d'exception de vulnérabilité n'expire jamais. Si vous cochez la case, alors vous ne pourrez pas entrer une date d'expiration future dans la zone **Expiry Date**.
Assets	
Vulnérabilité d'exception pour tous les actifs	Sélectionnez cette option pour appliquer la règle d'exception à tous les actifs qui ont des instances de la vulnérabilité.
Exception for specific asset with current IP	La zone **Exception for specific asset with current IP** est remplie par l'adresse IP de l'actif dans lequel se trouve la vulnérabilité.
and Asset Name	Par défaut, la zone **and Asset Name** contient le nom de l'actif dans lequel se trouve la vulnérabilité.
Exception for specific IP/CIDR/Network	Sélectionnez cette option pour créer une règle d'exception pour la vulnérabilité se trouvant sur un IP, CIDR, ou Réseau spécifique. Choisissez l'une des options suivantes : • Entrez une adresse IP ou une plage CIDR. Cliquez sur **Add.** • Cliquez sur **Browse** et sélectionnez un Réseau à partir de la zone de liste qui s'affiche.
Remarques	
Commentaires	Entrez des commentaires sur la raison pour laquelle la règle d'exception est en train d'être créée pour la vulnérabilité.
Previous Comments	Lorsque vous créez une règle d'exception, aucun commentaire précédent ne s'affiche. Si vous éditez une exception, la zone de texte affiche les commentaires ajoutés lorsque la règle d'exception est créée ou modifiée. Vous devez entrer des commentaires pour sauvegarder une exception.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Vulnerability > By Network**.

Etape 3 Facultatif. Pour rechercher des vulnérabilités par réseau, voir **Exécuter une recherche de vulnérabilité**.

Etape 4 Cliquez sur le lien de la colonne **Vulnerability Instances**.

Etape 5 Sélection la vulnérabilité pour laquelle vous souhaitez créer une règle d'exception.

Etape 6 Dans la barre d'outils, sélectionnez **Actions > Exception**.

Etape 7 Entrez les valeurs pour les paramètres indiqués dans **Tableau 6-3**.

Etape 8 Cliquez sur **Save**.

Modification d'une règle d'exception de vulnérabilité

Si vous recevez des informations concernant une vulnérabilité, vous pouvez modifier et mettre à jour une règle d'exception de vulnérabilité existante.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Vulnerability Exception**.

Etape 3 Cliquez sur la vulnérabilité que vous souhaitez modifier.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Edit**.

Etape 5 Mettez à jour les valeurs des paramètres indiqués dans **Tableau 6-3**.

Etape 6 Cliquez sur **Save**.

Suppression d'une règle d'exception de vulnérabilité

Si vous recevez des informations qu'une vulnérabilité présente un grand risque, vous pouvez supprimer une règle d'exception.

A propos de cette tâche

ATTENTION : *Lorsque vous supprimez une règle d'exception de vulnérabilité, aucun avertissement ne s'affiche. L'exception de vulnérabilité est immédiatement supprimée.*

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Vulnerability Exception**.

Etape 3 Sélectionnez la vulnérabilité dont vous souhaiter retirer la règle d'exception.

Etape 4 Dans la barre d'outils, sélectionnez **Actions > Remove**.

Exportation d'une règle d'exception de vulnérabilité

Vous pouvez exporter des exceptions de vulnérabilité sous format Extensible Markup Language (XML) ou sous format CVS (comma-separated values).

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Vulnerability Exceptions**.

Etape 3 Choisissez l'une des options suivantes :

- Dans la barre d'outils, sélectionnez **Actions > Export to XML**.
- Dans la barre d'outils, sélectionnez **Actions > Export to CSV**.

Etape 4 Facultatif. Dans la boîte de dialogue **Waiting for export to commence**, choisissez l'une des options suivantes :

- Cliquez sur **Notify When Done** pour être averti par courrier électronique lorsque l'exportation est achevée.
- Cliquez sur **Cancel Export** pour annuler l'exportation.

Etape 5 Suivez les instructions figurant à l'écran pour enregistrer ou ouvrir le fichier que vous avez exporté.

Recherche d'exceptions de vulnérabilité

Vous pouvez rechercher des vulnérabilités là où s'applique une règle d'exception.

A propos de cette tâche

Cette procédure fournit les méthodes permettant de rechercher vos vulnérabilités avec des règles d'exception :

1. Affichez toutes les vulnérabilités, y compris celles dont les règles d'exception sont appliquées.
2. Affichez uniquement les vulnérabilités qui appliquent des règles d'exception.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Manage Vulnerabilities > By Asset**.

Etape 3 Dans la barre d'outils, sélectionnez **Search > New Search**.

Etape 4 Dans la première zone de liste **Search Parameters**, sélectionnez les options suivantes :

Option	Description
Include exceptioned vulnerabilities	Sélectionnez cette option pour afficher toutes les vulnérabilités, en particulier ces règles d'exception que vous avez appliquées.
Only include exceptioned vulnerabilities	Sélectionnez cette option pour n'afficher que des vulnérabilités avec les règles d'exception appliquées.

Etape 5 Cliquez sur **Add Filter**.

Etape 6 Cliquez sur **Search**.

7 GÉRER LA RÉSOLUTION DES VULNÉRABILITÉS

Les vulnérabilités ayant été détectées par l'analyse de vos actifs réseau peuvent être manuellement ou automatiquement affectées aux utilisateurs QRadar pour être résolues.

Vous pouvez suivre le processus de résolution en examinant l'information sur les utilisateurs ayant été affectés pour corriger les vulnérabilités et sur les dates auxquelles les vulnérabilités doivent être résolues.

Vous pouvez également rechercher des informations détaillées sur l'actif contenant la vulnérabilité et utiliser diverses options actives du clic droit. Pour plus d'informations, consulter le guide d' utilisation*IBM Security QRadar SIEM* ou le guide d'utilisateur *IBM Security QRadar Log Manager.*

Barre d'outils des vulnérabilités affectées

Une barre d'outils est disponible sur la page **My Assigned Vulnerabilities** sur l'onglet **Vulnerabilities**.

Vous pouvez accéder aux options suivantes sur la barre d'outils My Assigned Vulnerabilities

Tableau 7-1 Mes options de barre d'outils assigned vulnerabilities

Fonction	Description
Search	Cliquez sur **Search** et sélectionnez une des options suivantes: • **New Search** - Sélectionnez cette option pour rechercher des vulnérabilités affectées. Pour plus d'informations, voir **Rechercher les vulnérabilités affectées**. • **Edit Search** - Sélectionnez cette option pour modifier la recherche Assigned Vulnerabilities.
Save Search Criteria	Sélectionnez cette option pour sauvegarder une recherche de vos vulnérabilités affectées. Voir **Enregistrer une recherche des vulnérabilités affectées**.
Quick Searches	Sélectionnez des recherches enregistrées à partir de la zone de liste **Quick Searches**. Pour plus d'informations, voir **Enregistrer une recherche des vulnérabilités affectées**. **Remarque:** QRadar Vulnerability Manager est distribué à l'aide de plusieurs recherches sauvegardées.

Tableau 7-1 Mes options de barre d'outils assigned vulnerabilities (suite)

Fonction	Description
Actions	**Print** - Sélectionnez cette option pour imprimer les vulnérabilités affectées. **Export to XML** - Sélectionnez cette option pour exporter les vulnérabilités affectées en format Extensible Markup Language (XML). Voir **Exporter les vulnérabilités affectées**. **Export to CSV** - Sélectionnez cette option pour exporter les vulnérabilités affectées en format CSV. Voir **Exporter les vulnérabilités affectées**. **Exception** - Sélectionnez cette option pour créer une Vulnerability Exception. Pour plus d'informations, voir **Création d'une execption de vulnérabilité** **Assign/Edit** - Sélectionnez cette option pour réaffecter ou modifier une vulnérabilité affectée. Voir **Affecter manuellement les vulnérabilités**. **History** - Sélectionnez cette option pour afficher l'historique d'une vulnérabilité. Par exemple, lorsqu'il a été découvert quel utilisateur a été affecté pour la résolution. Pour plus d'informations, voir **Affichage de l'historique de vulnérabilité**.
Quick Filter	Saisissez vos critères de recherche dans le champ **Quick Filter** et cliquez sur l'icône **Quick Filter** ou appuyez sur Enter sur le clavier. ***Remarque:*** *Lorsque vous cliquez sur le champ* ***Quick Filter,*** *une infobulle fournissant des informations sur la syntaxe appropriée à utiliser pour vos critères de recherche s'affiche.*

Affichage des vulnérabilités affectées

Vous pouvez afficher les informations sur la vulnérabilité affectée. Par exemple, l'utilisateur qui est affecté à la vulnérabilité et la date d'échéance de la résolution.

Avant de commencer

Pour plus d'informations relatives à l'affectation de vulnérabilités, consulter **Affecter manuellement les vulnérabilités** ou **Configuration de la résolution automatique de vulnérabilités**.

La page My Assigned Vulnerabilities permet d'afficher les paramètres suivants:

Tableau 7-2 Mes paramètres assigned vulnerabilities

Paramètre	Description
Adresse IP	L'adresse IP de l'actif analysé. Pour étudier davantage d'informations sur l'actif analysé, sélectionnez l'une des options suivantes: • Déplacez la souris vers le lien de la colonne **IP Address**. • Cliquez sur le lien de la colonne **IP Address** pour visualiser la fenêtre Asset Details. • Cliquez avec le bouton droit de la souris sur le lien de la colonne **IP Address** pour accéder aux options suivantes: - Navigate - sélectionnez cette option pour accéder aux informations sur la violation relative à l'actif analysé. - Information - sélectionnez cette option pour rechercher des événements et des flux et afficher les informations d'actifs. - Run QVM Scan - sélectionnez cette option pour analyser à nouveau un atout.. Pour de plus amples informations sur les Asset Details, les violations et options de menu contextuel d'actif, consulter le guide d'utilisation *IBM Security QRadar SIEM ou* le guide d'utilisation *IBM Security QRadar Log Manager.*
Nom d'actif	Le nom de l'actif où a été détectée la vulnérabilité.
Vulnerability	Le nom de la vulnérabilité trouvée sur l'actif. Cliquez sur le lien de colonne **Vulnerability** pour visualiser la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilité.**
PCI Severity	Affiche le niveau de risque que pose la vulnérabilité au Payment Card Industry (PCI). Les options incluent : • Urgent • Critical • High • Medium • Low
Risk	Affiche la gravité du risque posé par la vulnérabilité. Les options incluent : High, Medium, Low, et Warning.

Tableau 7-2 Mes paramètres assigned vulnerabilities (suite)

Paramètre	Description
CVE ID	L'ID du Common Vulnerabilities and Exposures (CVE) associé à la vulnérabilité. Cliquez sur le lien de la colonne **CVE Id** pour explorer le site National Vulnerability Database. ***Remarque:*** *Si la vulnérabilité a plus d'un ID CVE, Multiple (N) s'affiche. Déplacez la souris vers la valeur pour que s'affiche l'intégralité des ID CVE.*
CVSS Score	Le score Common Vulnerability Scoring System (CVSS) affecté à la vulnérabilité. Pour plus d'informations sur le CVSS, voir **Glossaire**.
Date Found	Date et Heure auxquelles la vulnérabilité a été trouvée sur l'actif.
Last Date Seen	La date à laquelle la vulnérabilité a été vue la dernière fois sur l'actif.
Assigned To	Le nom d'utilisateurQRadar affecté pour résoudre la vulnérabilité. Pour plus d'informations, voir **Affecter manuellement les vulnérabilités**.
Status	L'état de la vulnérabilité affectée. Les options incluent : • **Opened** - Indique qu'une vulnérabilité est affectée à la résolution. Voir **Affecter manuellement les vulnérabilités**. • **Reopened** -Indique qu'une vulnérabilité n'est pas résolue. ***Remarque:*** *Si la résolution automatique est activée et qu'une vulnérabilité précédemment fixée ou fermée est découverte après une nouvelle analyse, la vulnérabilité est rouverte. Pour plus d'informations, voir* **Configuration de la résolution automatique de vulnérabilités**. • **Fixed** - Indique que la vulnérabilité n'est pas résolue. • **Closed** - Indique qu'une vulnérabilité est résolue. • **Auto Closed** - Cet état s'affiche si une analyse ultérieure, qui utilise le même profil d'analyse, ne trouve aucune vulnérabilité affectée à l'actif où si la vulnérabilité a déjà été trouvée.
Due days	Le nombre de jours durant lesquels la vulnérabilité doit être résolue. Pour chaque tranche de 24 heures, lorsqu'une vulnérabilité n'est pas résolue, la valeur diminue d'une valeur de un. ***Remarque:*** *Si l'auto-résolution est activée, la valeur affichée correspond à la gravité et au risque PCI posés par une vulnérabilité. Par exemple, une vulnérabilité faible au risque à une cible de 20 jours pour la résolution. Une haute vulnérabilité au risque a une cible de 10 jours pour la résolution. Pour plus d'informations, voir* **Configuration de la résolution automatique de vulnérabilités**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **My Assigned Vulnerabilities**.

Rechercher les vulnérabilités affectées

Vous pouvez rechercher les vulnérabilités ayant été affectées aux utilisateurs QRadar pour être résolues.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **My Assigned Vulnerabilities**.

Etape 3 Sur la barre d'outils, sélectionnez **Search > New Search**.

Etape 4 Si vous voulez charger une recherche enregistrée, suivez les étapes suivantes:

a Facultatif. Sélectionnez un groupe dans la zone de liste du groupe pour afficher les recherches qui sont disponibles pour ce groupe dans la liste **Available Saved Searches**.

b Choisissez une des options suivantes :

- Facultatif. Dans le champ **Type Saved Search or Select from List**, saisissez le nom de la recherche que vous souhaitez charger.
- Dans la liste Available Saved Searches, sélectionnez la recherche enregistrée que vous souhaitez charger.

c Sélectionnez **Load > Search**.

Les résultats de recherche s'affichent. La partie supérieure du tableau affiche les détails des filtres appliqués aux résultats de la recherche.

Etape 5 Si vous souhaitez créer une nouvelle recherche, effectuez les étapes suivantes dans la sous-fenêtre **Search Parameter**.

a Dans la première zone de liste, sélectionnez le paramètre que vous souhaitez rechercher.

b Dans la deuxième zone de liste, sélectionnez le modificateur que vous souhaitez utiliser pour la recherche. Les modificateurs qui sont disponibles dépendent du paramètre sélectionné dans la première zone de liste.

c Dans la troisième zone de liste, tapez ou sélectionnez les informations spécifiques qui sont liées à votre paramètre de recherche.

d Cliquez sur **Add Filter**.

e Répéter les étapes **a** to **d** pour chaque filtre que vous souhaitez ajouter à vos critères de recherche.

f Le filtre s'affiche dans la zone de saisie **Current Filters**.

Etape 6 Cliquez sur **Search**.

Enregistrer une recherche des vulnérabilités affectées

Vous pouvez enregistrer vos critères de recherche de vulnérabilités affectées et accéder à la recherche à l'aide de la zone de liste **Quick Searches** sur la barre d'outils.

Procédure

Etape 1 Facultatif. Pour effectuer une recherche de vos vulnérabilités affectées, consulter **Rechercher les vulnérabilités affectées**.

Etape 2 Sur la barre d'outils, cliquez sur **Save Criteria**.

Etape 3 Entrez des valeurs pour les paramètres suivants:

Option	Description
Saisissez le nom de cette recherche	Tapez le nom de la recherche que vous souhaitez enregistrer pour une utilisation ultérieure.
Include in my Quick Searches	Cochez cette case si vous souhaitez inclure la recherche enregistrée dans votre zone de liste **Quick Searches** sur la barre d'outils.
Share with Everyone	Cochez cette case si vous souhaitez partager vos exigences de recherche avec l'ensemble des utilisateurs QRadar.
Assign Search to Group(s)	Sélectionnez les groupes auxquels vous souhaitez affecter la recherche enregistrée. Si aucun groupe n'est sélectionné, les critères de recherche sont affectés par défaut au groupe **Other**. Pour plus d'informations sur la gestion des groupes de recherche, consulter le guide d'utilisation *IBM Security QRadar SIEM* ou le guide d'utilisation *IBM Security QRadar Log Manager.*
Set As Default	Cochez cette case si vous souhaitez configurer la recherche enregistrée comme affichage par défaut lorsque vous sélectionnez **My Assigned Vulnerabilities** dans le menu de navigation.

Etape 4 Cliquez sur **OK**.

Exporter les vulnérabilités affectées

Vous pouvez exporter les vulnérabilités attribuées au format XML ou CSV.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **My Assigned Vulnerabilities**.

Etape 3 Sélectionnez l'une des options suivantes:

- Sur la barre d'outils, sélectionnez **Actions > Export to XML**.
- Sur la barre d'outils, sélectionnez **Actions > Export to CSV**.

Etape 4 Facultatif. Dans la fenêtre **Waiting for export to commence**, sélectionnez une des options suivantes:

- Cliquez sur **Notify When Done** pour être informé par e-mail une fois que le processus d'exportation prend fin.
- Cliquez sur **Cancel Export** pour interrompre le processus d'exportation.

Etape 5 Suivez les instructions à l'écran pour enregistrer ou ouvrir le fichier que vous avez exporté.

Affecter manuellement les vulnérabilités

Vous pouvez manuellement affecter des vulnérabilités à un utilisateurQRadar pour qu'elles soient résolues.

A propos de cette tâche

La fenêtre Assign/Edit Vulnerability permet d'afficher les informations suivantes:

Tableau 7-3 Paramètres fenêtre de vulnérabilité Assign/edit

Paramètre	Description
Vulnerability	Le nom de la vulnérabilité affectée à l'utilisateur QRadar pour la résolution. Cliquez sur le lien **Vulnerability** pour visualiser la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilité**.
Risk Level	Le niveau de risque associé à la vulnérabilité affectée. Les options incluent : High, Medium, Low, et Warning.
PCI Severity	Affiche le niveau de risque que pose la vulnérabilité au Payment Card Industry (PCI). Les options incluent : • Urgent • Critical • High • Medium • Low
Adresse IP	L'adresse IP de l'actif ou la vulnérabilité a été trouvée. Cliquez sur le lien de la colonne **IP Address** pour visualiser la fenêtre Asset Details. Pour plus d'informations, consulter le guide d'utilisation *IBM Security QRadar SIEM* ou le guide d'utilisation *IBM Security QRadar Log Manager.*
Nom d'hôte	Le nom de l'hôte où la vulnérabilité a été découverte.
Assignment Details	
Priority	Le niveau de priorité associé à la vulnérabilité affectée. Les options incluent : • Critical • Major • Minor • Warning • Informational
Status	L'état de la vulnérabilité affectée. Les options incluent : • Opened • Reopened • Fixed • Closed

Tableau 7-3 Paramètres fenêtre de vulnérabilité Assign/edit (suite)

Paramètre	Description
Assigned User	Le nom d'utilisateur QRadar auquel est affectée la vulnérabilité. Facultatif. Si vous souhaitez affecter des vulnérabilités à différents utilisateurs QRadar, vous pourriez être amené à créer de nouveaux utilisateurs ou modifier vos autorisations d'utilisation en cours. Pour plus d'informations, consulter le guide d'administration *IBM Security QRadar SIEM* ou le guide d'administration *IBM Security QRadar Log Manager.*
Due Date	La date à laquelle la vulnérabilité affectée doit être résolue. Saisissez une nouvelle date dans le champ date d'échéance ou cliquez sur la liste déroulante et sélectionnez une date à laquelle la vulnérabilité doit être résolue.
Remarques	
Commentaires	Entrez des commentaires sur l'état d'avancement du processus de résolution de la vulnérabilité. Ces commentaires sont stockés et affichés dans le champ **Comment** lorsque vous cliquez sur **Save**.
Comment	Les commentaires antérieurs de l'utilisateur QRadar affecté pour résoudre la vulnérabilité.
User Name	Le nom d'utilisateur QRadar qui a saisi les commentaires sur le processus d'avancement de résolution de la vulnérabilité.
Date	La date à laquelle les observations ont été saisies par l'utilisateur ayant affecté les vulnérabilités, ou par l'utilisateur ayant été affecté pour résoudre la vulnérabilité.

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Vulnerability Manager > By Network**.

Etape 3 Facultatif. Effectuez une recherche de vulnérabilités. Pour plus d'informations, voir **Réalisation d'une recherche de vulnérabilité**.

Etape 4 Cliquez sur le lien de la colonne **Vulnerability Instances**.

Etape 5 Sélectionnez la vulnérabilité que vous souhaitez affecter à la résolution.

Etape 6 Sur la barre d'outils, cliquez sur **Actions > Assign/Edit**.

Etape 7 Entrez des valeurs pour les paramètres suivants:

Option	Description
Priority	Indiquez le niveau de priorité associé à la vulnérabilité.
Status	Indiquez l'état de la vulnérabilité assignée.
Assign User	Indiquez l'utilisateurQRadar affecté pour résoudre la vulnérabilité.
Due Date	Indiquez la date à laquelle la vulnérabilité doit être résolue.
Commentaires	Entrez les commentaires associés à l'affectation de la vulnérabilité.

Etape 8 Cliquez sur **Save**.

Configuration de la résolution automatique de vulnérabilités

Vous pouvez configurer QRadar Vulnerability Manager pour procéder à l'affectation automatique de vulnérabilités à un utilisateur QRadar pour qu'elles soient résolues.

Avant de commencer

Pour affecter automatiquement des vulnérabilités, il vous faut affecter un utilisateur technique à vos actifs via l'onglet **Assets** QRadar. Vous pouvez être amené à créer un nouvel utilisateur ou une liste de nouveaux utilisateurs pour faire en sorte que les vulnérabilités puissent être affectées. Pour plus d'informations sur la Gestion des Utilisateurs et des Rôles, consulter le guide d'administration *IBM Security QRadar SIEM Administration Guide* ou le guide d'administration*IBM Security QRadar Log Manager.*

A propos de cette tâche

Lors de l'analyse d'un actif via un utilisateur technique affecté, les vulnérabilités sont automatiquement affectées à l'utilisateur et son état est défini à **Opened**.

Pour plus d'informations sur l'utilisation de l'onglet **Assets**, consulter le guide d'utilisation *IBM Security QRadar SIEM* ou le guide d'utilisation *IBM Security QRadar Log Manager.*

Procédure

Etape 1 Cliquez sur l'onglet **Assets**.

Etape 2 Dans le menu de navigation, cliquez sur **Asset Profiles**.

Etape 3 Sélectionnez l'actif que vous souhaitez configurer.

Etape 4 Sur la barre d'outils, cliquez sur **Edit Asset.**

Etape 5 Cliquez sur la sous-fenêtre extensible **Owners**.

Etape 6 Dans la zone de liste **Technical User**, sélectionnez l'utilisateur auquel vous souhaitez affecter les vulnérabilités.

Etape 7 Cliquez sur **Save**.

Etapes suivantes

Effectuer une analyse des actifs qui ont un utilisateur technique affecté. Veillez à ce que les vulnérabilités détectées s'affichent sur la page **My Assigned Vulnerabilities** avec un état défini à **Opened**.

8 RAPPORTS QRADAR VULNERABILITY MANAGER

Vous pouvez créer ou modifier un rapport existant ou utiliser l'assistant de rapport pour créer, planifier et distribuer un nouveau rapport.

QRadar Vulnerability Manager est réparti dans 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. L'assistant utilise les éléments clé principaux pour pouvoir créer un rapport :

- Scheduling - Définit la date de génération de votre rapport. Pour plus d'informations, voir **Configuration de planifications de rapport**.
- Layout - Position et taille de chaque conteneur.
- Content - Définit les données de rapport qui s'affichent dans chaque rapport. Pour plus d'informations, voir **Configuration de contenu de rapport**.
- Container - marque de réservation et emplacement pour le contenu dans votre rapport.

Pour plus d'informations sur la gestion, la planification et l'exécution de rapports, voir *IBM Security QRadar SIEM - Guide d'administration*.

Configuration de planifications de rapport

L'assistant de rapport permet de planifier les moments de génération d'un rapport. Ces informations sur le tableau suivant permettent de planifier vos rapports.

Tableau 8-1 Options de planification de rapport

Report Interval	Description
Manually	Génère un rapport une seule fois, sans planification récurrente.
Hourly	Planifie le rapport à générer par heure. Si vous choisissez l'option **Hourly**, une configuration supplémentaire est requise. Dans les zones de liste, vous devez sélectionner une période pour commencer et terminer le cycle de génération de rapports. Un rapport est généré par heure dans cette période de temps. ***Remarque :*** *L'exécution du rapport horaire par défaut est planifiée à 1h 00 du matin.*

Tableau 8-1 Options de planification de rapport (suite)

Report Interval	Description
Daily	Planifie le rapport à générer quotidiennement. Si vous choisissez l'option **Daily**, une configuration supplémentaire est requise. Vous pouvez sélectionner plusieurs jours de la semaine et spécifier une heure de début pour chaque jour. ***Remarque :*** *L'exécution du rapport quotidien par défaut est planifiée à 1h 00 du matin.*
Weekly	Planifie le rapport à générer chaque semaine. Si vous choisissez une option **Weekly**, une configuration supplémentaire est requise. Vous pouvez sélectionner un seul jour de la semaine et indiquer une heure de début pour le jour que tu choisis. ***Remarque :*** *Le rapport hebdomadaire par défaut est généré à 1h 00 du matin.*
Monthly	Planifie le rapport à générer mensuellement. Si vous choisissez l'option **Monthly**, une configuration supplémentaire est requise. Vous pouvez sélectionner un jour dans le mois et indiquer une heure de début pour le jour que tu choisis. ***Remarque :*** *Le rapport mensuel par défaut est généré à 1h 00 du matin.*
Allow this report to generate manually	Cette option ne s'affiche que lorsque vous sélectionnez une option de planification de rapport, autre que **Manually**. Si vous sélectionnez **Yes**, vous pouvez générer manuellement un rapport planifié. Pour plus d'informations, voir **Exécution manuelle d'un rapport de vulnérabilité**.

Configuration de contenu de rapport

L'assistant de rapport permet d'indiquer les données qui s'affichent lorsque votre rapport est généré.

Les informations qui se trouvent dans le tableau suivant permettent d'indiquer vos données de rapport :

Tableau 8-2 Paramètres du contenu du rapport

Paramètre	Description
Détails du conteneur - Gestion de la vulnérabilité	
Titre de graphique	Entrez un titre de graphique pouvant comporter jusqu'à 100 caractères.
Sous-titre de graphique	Décochez la case pour modifier le sous-titre de rapport qui a été créé automatiquement. Entrez un titre pouvant comporter jusqu'à 100 caractères.

Tableau 8-2 Paramètres du contenu du rapport (suite)

Paramètre	Description
Type de graphique	Vous pouvez sélectionner le type de graphique à afficher sur le rapport généré. Les options comprennent : • **Bar** - Affiche les données dans un graphique à barres. Lorsque vous sélectionnez cette option, le rapport n'inclut pas les données du sous-rapport. Il s'agit de l'option par défaut. Ce type de graphique demande à la recherche sauvegardée d'être une recherche groupée. • **Line** - Affiche les données dans un graphique à courbes. • **Pie** - Affiche les données dans un graphique circulaire. Ce type de graphique demande à la recherche sauvegardée d'être une recherche groupée. • **Stacked Bar** - Affiche les données dans un graphique à barres empilées. • **Stacked Line** - Affiche les données dans un graphique à courbes empilées. • **Table** - Affiche les données sous forme de tableau. L'option **Table** est uniquement disponible pour le conteneur de la page entière.
Plage de dates pour le graphique	

Tableau 8-2 Paramètres du contenu du rapport (suite)

Paramètre	Description
Données à utiliser	Vous pouvez sélectionner une plage de dates à afficher sur le rapport généré. Les options comprennent : • **Current** - Affiche les données de vulnérabilité pour tous les résultats de la recherche accumulés par le système. • **Daily** - Affiche les données de vulnérabilité du nombre de jours que vous avez spécifiés. Cette option s'affiche par défaut si vous cochez **Hourly** ou **Daily** comme option de planification de rapport. Choisissez l'une des options suivantes : - **Recent -** Affiche toutes les données des dernières 24 heures. La zone **Last** permet d'augmenter ou de diminuer le nombre de jours. - **Specific Interval** - Indique une date de début et une date de fin de votre plage de temps de génération de rapports. • **Weekly** - Affiche les données de vulnérabilité du nombre de semaines que vous avez spécifiés. La zone **Last** permet d'augmenter ou de diminuer le nombre de semaines de données de rapport. ***Remarque :*** *Les données de vulnérabilité sont générées lorsque vous accumulez des données de vulnérabilité pendant plus d'une semaine.* • **Monthly** - Affiche les données de vulnérabilité pour le nombre de mois que vous avez indiqué. Choisissez l'une des options suivantes : - **Recent -** Affiche toutes les données des derniers mois. La zone **Last** permet d'augmenter ou de diminuer le nombre de mois. - **Specific Interval** - Indique un mois de début et un mois de fin de votre plage de temps de génération de rapports.
Options de données	
Search to use	Affiche les recherches sauvegardées que vous pouvez utiliser pour générer votre rapport.
Group By	Affiche les options pour regrouper les données sur votre rapport.

Tableau 8-2 Paramètres du contenu du rapport (suite)

Paramètre	Description
Graph Field	Affiche la valeur que vous affichez sur le rapport généré. Les options comprennent : • **Asset Count** - Affiche le nombre d'actifs accumulés qui sont basés sur la valeur que vous avez sélectionnée dans la zone **Group By**. • **CVSS Base Score** - Affiche le score CVSS accumulé et regroupe les données en fonction de l'option que vous avez sélectionnée dans la zone **Group By**. • **Vulnerability Count** - Affiche le nombre total de vulnérabilités trouvées sur l'actif pour la plage de dates spécifiée.
Sort Order	Dans les options, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats sur le rapport généré : Ascendant ou Descendant.
Limit to top	Si vous accumulez un grand volume de données de vulnérabilité en analysant plusieurs actifs de réseau, vous pouvez limiter le nombre d'actifs affichés sur le rapport généré. La valeur par défaut est 10.

Configuration de distribution de rapport

Vous pouvez indiquer des options de distribution de rapport de vulnérabilité.

Le tableau suivant indique les options de distribution de rapport :

Tableau 8-3 Options de distribution de rapports générés

Option	Description
Report Console	Cochez cette case pour envoyer le rapport généré vers l'onglet **Reports**. Il s'agit du canal de distribution par défaut.
Sélectionnez les utilisateurs dont vous devez être en mesure de voir leur rapport généré	Cette option ne s'affiche que lorsque vous cochez la case **Report Console**. Dans la liste des utilisateurs, sélectionnez les utilisateurs QRadar Vulnerability Manager que vous souhaitez accorder le droit d'afficher les rapports générés. ***Remarque :*** *Vous devez avoir les autorisations réseau nécessaires pour partager le rapport généré avec d'autres utilisateurs. Pour de plus amples informations sur les droits, voir votre guide d'administration.*

Tableau 8-3 Options de distribution de rapports générés (suite)

Option	Description
Select all users	Cette option s'affiche uniquement une fois que vous cochez la case **Report Console**. Cochez cette case pour accorder le droit à tous les utilisateurs QRadar Vulnerability Manager d'afficher les rapports générés. ***Remarque :*** *Vous devez avoir les autorisations réseau nécessaires pour partager le rapport généré avec d'autres utilisateurs. Pour plus d'informations sur les droits, voir le guide d'administration IBM Security QRadar SIEM ou le guide d'administration IBM Security QRadar Log Manager.*
Email	Cochez cette case si vous souhaitez distribuer le rapport généré par courrier électronique.
Enter the report destination email address(es)	Cette option ne s'affiche que lorsque vous cochez la case **Email**. Entrez l'adresse e-mail pour chaque destinataire de rapports générés ; séparez une liste d'adresses e-mails par des virgules. Le nombre de caractères maximum est 255. ***Remarque :*** *Les destinataires d'e-mail reçoivent ce courrier de no_reply_reports@qradar.*
Include Report as attachment (non-HTML only)	Cette option ne s'affiche que lorsque vous cochez la case **Email**. Cochez cette case pour envoyer le rapport généré en tant que pièce-jointe.
Include link to Report Console	Cette option ne s'affiche que lorsque vous cochez la case **Email**. Cochez cette case pour inclure un lien vers la console de rapport dans le courrier électronique.

Création d'un rapport

Vous pouvez créer un rapport de vulnérabilité.

Procédure

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Dans la barre d'outils, sélectionnez **Actions > Create**, puis cliquez sur **Next**.

Etape 3 Sélectionnez une option de planification indiquée dans **Tableau 8-1** puis cliquez sur **Next**.

Etape 4 Configurez votre présentation de rapport :

a Dans la zone de liste **Orientation**, sélectionnez l'orientation de la page : l'orientation par défaut est Paysage.

b Sélectionnez une des options de présentation puis cliquez sur **Next**.

Etape 5 Indiquez les valeurs pour les paramètres suivants :

Option	Description
Titre de rapport	Entrez un titre de rapport. Le titre peut comporter jusqu'à 100 caractères. N'utilisez pas de caractères spéciaux.
Logo	Dans la zone de liste, sélectionnez un logo. QRadar est le logo par défaut. Pour de plus amples informations sur l'image de marque de votre rapport, voir *IBM Security QRadar SIEM - Guide d'utilisation.*
Type de graphique	Dans la zone de liste, sélectionnez **Vulnerabilities**.

Etape 6 Configurez vos options de données de rapport comme indiqué dans**Tableau 8-2**.

Etape 7 Cliquez sur **Save Container Details** puis sur **Next**.

Etape 8 La page Layout Preview s'affiche. Cliquez sur **Next**.

Etape 9 Cochez les cases pour le format de sortie de rapport requis. Vous pouvez sélectionner plusieurs types de sortie. Les options comprennent :

- Format PDF (Portable Document Format) - Il s'agit du format par défaut.
- Hypertext Markup Language (HTML)
- Rich Text Format (RTF)
- Extensible Markup Language (XML)
- Excel Spreadsheet (XLS)

Etape 10 Cliquez sur **Next**.

Etape 11 Configurez les options de distribution de rapport dans **Tableau 8-3** puis cliquez sur **Next**.

Etape 12 Entrez des valeurs pour les options suivantes :

Option	Description
Description de rapport	Entrez une description de rapport. La description s'affiche sur la page Report Summary et dans le courrier électronique de distribution du rapport généré.
Groupes	Sélectionnez les groupes auxquels vous souhaitez affecter votre rapport. Pour de plus amples informations sur les groupes, consultez votre guide d'utilisation.
Would you like to run the report now?	Cochez cette case si vous souhaitez générer le rapport une fois que l'assistant a terminé. Par défaut, la case est cochée.

Etape 13 Cliquez sur **Next** pour afficher l'option **Report Summary**, puis sur **Finish**.

Etape suivante

En fonction des options de configuration que vous avez sélectionnées, vous pouvez exécuter manuellement un rapport. Pour plus d'informations, voir **Exécution manuelle d'un rapport de vulnérabilité**.

Modification d'un rapport

Vous pouvez modifier un rapport de vulnérabilité.

Procédure

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez le rapport que vous souhaitez modifier.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Edit**, puis cliquez sur **Next**.

Etape 4 Sélectionnez une option de planification de rapport indiquée dans **Tableau 8-1** puis cliquez sur **Next**.

Etape 5 Configurez votre présentation de rapport :

a Dans la zone de liste **Orientation**, sélectionnez l'orientation de la page : l'orientation par défaut est Paysage.

b Sélectionnez une des options de présentation puis cliquez sur **Next**.

Etape 6 Indiquez les valeurs pour les paramètres suivants :

Option	Description
Titre de rapport	Entrez un titre de rapport. Le titre peut comporter jusqu'à 100 caractères. N'utilisez pas de caractères spéciaux.
Logo	Dans la zone de liste, sélectionnez un logo. Le logo QRadar est le logo par défaut. Pour de plus amples informations sur l'image de marque de votre rapport, voir le guide d'utilisation *IBM Security QRadar SIEM Guide* ou le guide d'utilisation*IBM Security QRadar Log Manager.*
Type de graphique	Dans la zone de liste, sélectionnez **Vulnerabilities**.

Etape 7 Cliquez sur **Define**.

Etape 8 Configurez vos options de données de rapport comme indiqué dans**Tableau 8-2**.

Etape 9 Cliquez sur **Save Container Details** puis sur **Next**.

Etape 10 Cochez les cases pour le format de sortie de rapport requis. Vous pouvez sélectionner plusieurs types de sortie. Les options comprennent :

- Format PDF (Portable Document Format) - Il s'agit du format par défaut.
- Hypertext Markup Language (HTML)
- Rich Text Format (RTF)
- Extensible Markup Language (XML)
- Excel Spreadsheet (XLS)

Etape 11 Cliquez sur **Next**.

Etape 12 Configurez les options de distribution de rapport dans**Tableau 8-3** puis cliquez sur **Next**.

Etape 13 Entrez des valeurs pour les options suivantes :

Option	Description
Description de rapport	Entrez une description de rapport. La description s'affiche sur la page Report Summary et dans le courrier électronique de distribution du rapport généré.
Groupes	Sélectionnez les groupes auxquels vous souhaitez affecter votre rapport. Pour de plus amples informations sur les groupes, voir le guide d'utilisation *IBM Security QRadar SIEM* ou le guide d'utilisation *IBM Security QRadar Log Manager.*
Would you like to run the report now?	Cochez cette case si vous souhaitez générer le rapport une fois que l'assistant a terminé. Par défaut, la case est cochée.

Etape 14 Cliquez sur **Next** pour afficher l'option **Report Summary**, puis sur **Finish**.

Exécution manuelle d'un rapport de vulnérabilité

Vous pouvez générer manuellement un rapport de vulnérabilité.

Procédure

Etape 1 Cliquez sur l'onglet **Reports**.

Etape 2 Sélectionnez le rapport que vous souhaitez générer.

Etape 3 Dans la barre d'outils, sélectionnez **Actions > Run Report**.

Etape 4 Cliquez sur **OK**.

9 RECHERCHE DES VULNÉRABILITÉS, DES ACTUALITÉS ET DES RECOMMANDATIONS

Utilisez les outils dans QRadar Vulnerability Manager pour rester au fait du niveau de menace de vulnérabilité et gérer la sécurité de votre organisation.

Une bibliothèque de vulnérabilité comprend des vulnérabilités communes qui sont regroupées à partir d'une liste de sources externes. La ressource externe la plus importante est NVD (National Vulnerability Database). Vous pouvez rechercher des vulnérabilités spécifiques utilisant des critères tels que le fournisseur, le produit et la plage de date. Par exemple, vous pouvez être intéressé par des vulnérabilités spécifiques qui existent dans les produits ou services qui vous utilisez dans votre entreprise.

QRadar Vulnerability Manager offre également une liste d'articles d'actualités et de recommandations sur la sécurité, rassemblée à partir d'une liste externe de ressources et de fournisseurs. Il s'agit d'une source utile d'informations de sécurité du monde entier vous permettant de rester à jour sur les nouvelles de sécurité actuelles.

Barre d'outils de vulnérabilités de recherche

Une barre d'outils est fournie sur la page **Research Vulnerabilities** pour vous aider à examiner les informations de vulnérabilité.

Utilisez la barre d'outils de vulnérabilité de recherche pour accéder aux options suivantes :

Tableau 9-1 Options de barre d'outils de vulnérabilités de recherche

Fonction	Description
Recherche	**New Search** - Sélectionnez cette option pour rechercher la liste des vulnérabilités publiées. Pour plus d'informations, voir **Recherche des vulnérabilités publiées**. **Edit Search** - Sélectionnez cette option pour modifier une recherche des vulnérabilités publiées. Pour plus d'informations, voir **Modification d'une recherche de vulnérabilité publiée**

Tableau 9-1 Options de barre d'outils de vulnérabilités de recherche (suite)

Fonction	Description
Actions	**Print** - Sélectionnez cette option pour imprimer une liste de vulnérabilités publiées. **Export to XML** - Sélectionnez cette option pour exporter les vulnérabilités publiées en format XML. Pour plus d'informations, voir **Exportation de vulnérabilités publiées**. **Export to CSV** - Sélectionnez cette option pour exporter les vulnérabilités en format CSV. Pour plus d'informations, voir **Exportation de vulnérabilités publiées**.

Affichage des vulnérabilités publiées

Vous pouvez afficher une liste des vulnérabilités publiées sur la page **Research Vulnerabilities**.

Avant de commencer

Par défaut, toutes les vulnérabilités publiées pendant les dernières 24 heures sont affichées. Si aucune vulnérabilité n'est affichée, alors vous pouvez sélectionner une plage de temps alternative à partir de la zone de liste **Viewing vulnerabilities from**.

A propos de cette tâche

La page Research Vulnerabilities affiche les informations suivantes :

Tableau 9-2 Paramètres des vulnérabilités de recherche

Paramètre	Description
Date de publication	La date à laquelle la vulnérabilité a été publiée.
Niveau de risque	Le niveau de risque présenté par la vulnérabilité.
Gravité PCI	Le niveau de gravité que la vulnérabilité présente au PCI (Payment Card Industry).
Intitulé de la vulnérabilité	L'intitulé de la vulnérabilité publiée. Cliquez sur le lien de la colonne **Vulnerability Name** pour afficher la fenêtre Vulnerability Details. Pour plus d'informations, voir **Affichage des détails de vulnérabilité**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research > Vulnerabilities**.

Etape 3 Facultatif. Pour étendre vos résultats, sélectionnez une plage de temps alternative à partir de la zone de liste **Viewing vulnerabilities from**.

Affichage des détails de vulnérabilité

Vous pouvez afficher plus d'informations détaillées sur une vulnérabilité publiée.

A propos de cette tâche

La fenêtre Vulnerability Details offre les informations suivantes :

Tableau 9-3 Paramètres de la fenêtre des détails de vulnérabilité

Paramètre	Description
Vulnerability ID	Affiche l'identifiant de la vulnérabilité sélectionnée. Ceci est un identifiant unique qui est autogénéré par QRadar Vulnerability Manager.
Published Date	Affiche la date à laquelle la vulnérabilité a été initialement publiée.
Name	Affiche le nom complet de la vulnérabilité publiée.
Assets	Affiche le nombre d'actifs affectés par la vulnérabilité publiée.
Assets, including exceptions	Affiche les nombres d'actifs affectés par la vulnérabilité publiée où une exception a été créée pour la vulnérabilité. Pour plus d'informations, voir **Créer une exception de vulnérabilité**.
CVE	Affiche l'identifiant de CVE (Common Vulnerabilities and Exposures) qui est associé à la vulnérabilité sélectionnée. Cliquez sur le lien **CVE** pour afficher plus d'informations détaillées de vulnérabilité sur le site Web de National Vulnerability Database. ***Remarque :*** *Si la vulnérabilité n'est pas classifiée à un identificateur CVE, alors* ***CVE*** *peut être affiché comme N/A.*
xforce	Affiche l'identifiant xForce qui est associé à la vulnérabilité sélectionnée. Cliquez sur le lien **xforce** pour afficher plus d'informations détaillées de vulnérabilité sur le site Web d'IBM Internet Security Systems. ***Remarque :*** *Si la vulnérabilité n'est pas classifiée à un identificateur xforce, alors* ***xforce*** *peut être affiché comme N/A.*
OSVDB	Affiche l'identifiant OSVDB (Open Source Vulnerability Database) qui est associé à la vulnérabilité sélectionnée. Cliquez sur le lien **OSVDB** pour afficher plus d'informations détaillées de vulnérabilité sur le site Web d'Open Source Vulnerability Database. ***Remarque :*** *Si la vulnérabilité n'est pas classifiée à un identificateur OSVDB, alors* ***OSVDB*** *peut être affiché comme N/A.*

Tableau 9-3 Paramètres de la fenêtre des détails de vulnérabilité (suite)

Paramètre	Description
CVSS Base Score	Affiche la notation de base CVSS (Common Vulnerability Scoring System) qui est affectée à la vulnérabilité. La plage est de zéro à 10, où zéro correspond à un faible risque et 10 correspond à un haut risque. ***Remarque :*** *Si la vulnérabilité n'est pas affectée à une notation CVSS, alors* ***CVSS Base Score*** *peut être affichée comme N/A.*
CVSS Temporal Score	Affiche la notation temporelle de CVSS (Common Vulnerability Scoring System) qui est affectée à la vulnérabilité.
CVSS Base Metrics	Affiche le vecteur métrique de base pour les paramètres qui sont utilisés pour calculer la notation CVSS. Par exemple, le vecteur d'accès pour une vulnérabilité peut être local, adjacent ou en réseau selon l'endroit à partir duquel il peut être exploité.
CVSS Temporal Metrics	Affiche le vecteur métrique temporel pour les paramètres qui sont utilisés pour calculer la notation CVSS. Par exemple, les détails techniques de la vulnérabilité, l'état de restauration de la vulnérabilité et la disponibilité de code d'exploitation ou les techniques.
Impact	Affiche l'impact le plus probable que la vulnérabilité pourrait avoir sur vos opérations commerciales. Par exemple, l'accès non autorisé et le vol d'informations sensibles, le plantage du système ou la perte de réputation commerciale ***Remarque :*** *Si la vulnérabilité n'est pas affectée à une notation d'impact de vulnérabilité, alors* ***Vulnerability Impact*** *peut être affiché comme N/A.*
Description	Affiche une description détaillée de la vulnérabilité sélectionnée.
Concern	Affiche plus d'informations détaillées sur la vulnérabilité, y compris les principales préoccupations que vous pourriez avoir sur cette vulnérabilité en particulier.
Solution	Affiche une solution de contournement suggérée par le fournisseur du produit incriminé.
Associated Service	Affiche le nom de tout produit associé à cette vulnérabilité. Ceci peut inclure les produits par nom de fournisseur identique.
Virtual Patching	Affiche les signatures d'exploitation qui cartographie la vulnérabilité publiée.
Reference	Affiche les liens vers les sites Web contenant plus d'informations qui sont pertinentes à la vulnérabilité publiée. ***Remarque :*** *S'il n'y a pas d'informations supplémentaires sur une vulnérabilité, alors* ***Reference*** *peut être affiché comme N/A.*
Products	Affiche le nom de tout produit associé à cette vulnérabilité. Ceci peut inclure les produits par nom de fournisseur identique.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> Vulnerabilities**.

Etape 3 Cliquez sur le lien de colonne **Vulnerability Name** pour la vulnérabilité que vous souhaitez examiner.

Recherche des vulnérabilités publiées

Vous pouvez rechercher des vulnérabilités publiées en utilisant une plage de critères.

A propos de cette tâche

Utilisez les options suivantes pour définir vos critères de recherche de vulnérabilité :

Tableau 9-4 Paramètres de recherche de vulnérabilité

Paramètre	Description
Phrase	Entrez une expression dans le champ **Phrase** pour rechercher une vulnérabilité contenant ce texte.
Recent	Cliquez sur **Recent** pour activer la zone de liste d'intervalle de temps. Tout est sélectionné par défaut mais vous pouvez choisir une option d'intervalle de temps pour affiner vos critères de recherche.
Specific Interval	Cliquez sur **Specific Interval** pour activer les champs **From Date** et **To Date.** Ceci vous permet de rechercher les vulnérabilités en utilisant un intervalle de dates plus précis.
From Date	Entrez une date de début au format de date qui correspond à votre pays ou sélectionnez une date dans la zone de liste.
To Date	Entrez une date de fin au format de date qui correspond à votre pays ou sélectionnez une date dans la zone de liste.
Vendor	Sélectionnez un fournisseur pour afficher les vulnérabilités associées à ce fournisseur.
Product	Sélectionnez un produit pour le fournisseur que vous sélectionnez.
Version	A partir de la zone de liste Version, sélectionnez une version pour le fournisseur et le produit que vous avez sélectionné.
CVE ID	Entrez un identifiant CVE pour rechercher les vulnérabilités avec un identifiant CVE en particulier.
Vulnerability ID	Entrez un identifiant de vulnérabilité pour rechercher les vulnérabilités avec un identifiant de vulnérabilité en particulier. Cet identifiant est un identifiant interne affecté à chaque vulnérabilité et stocké parQRadar.
OSVDB ID	Entrez un identifiant OSVDB pour rechercher les vulnérabilités avec un identifiant OSVDB en particulier.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, cliquez sur **Research > Vulnerabilities**.

Etape 3 Dans la barre d'outils, sélectionnez **Search > New Search**.

Etape 4 Définissez vos critères de recherche en utilisant les paramètres décrits dans **Tableau 9-4**.

Etape 5 Cliquez sur **Search**.

Modification d'une recherche de vulnérabilité publiée

Vous pouvez modifier les critères d'une recherche de vulnérabilité publiée.

Avant de commencer

Cette procédure suppose que vous avez effectué une recherche des vulnérabilités publiées. Pour plus d'informations, voir **Recherche des vulnérabilités publiées**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> Vulnerabilities**.

Etape 3 Dans la barre d'outils, sélectionnez **Search > Edit Search**.

Etape 4 Modifiez votre recherche en utilisant les paramètres décrits dans**Tableau 9-4**.

Etape 5 Cliquez sur **Search**.

Exportation de vulnérabilités publiées

Vous pouvez exporter des vulnérabilités en format XML (Extensible Markup Language) ou CSV (Comma Separated Values).

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> Vulnerabilities**.

Etape 3 Choisissez une des options suivantes :

- Dans la barre d'outils, sélectionnez **Actions > Export to XML**.
- Dans la barre d'outils, sélectionnez **Actions > Export to CSV**.

Etape 4 La boîte de dialogue **Waiting For Export To Commence** s'affiche avec les options suivantes :

- Facultatif. Cliquez sur **Notify When Done** pour être notifié par e-mail lorsque l'exportation se termine.
- Facultatif. Cliquez sur **Cancel Export** pour annuler l'exportation.

Affichage des nouveaux articles de vulnérabilité

Vous pouvez afficher des actualités de sécurité du monde entier pour vous aider à maintenir à jour sur les développements en sécurité actuels.

Avant de commencer

Par défaut, tous les articles d'actualités publiés pendant les dernières 24 heures sont affichés. Si aucun article d'actualités ne s'affiche, sélectionnez une plage de durée alternative à partir de la zone de liste **Viewing news from**.

A propos de cette tâche

La barre d'outils Research News offre les options suivantes :

Tableau 9-5 Recherche d'options de barre d'outils d'actualités

Fonction	Description
Recherche	Cliquez sur **Search** et sélectionnez une des options suivantes : • **New Search** - Sélectionnez cette option pour rechercher la liste des articles d'actualités. Voir **Recherche d'articles d'actualités de vulnérabilités**. • **Edit Search** - Sélectionnez cette option pour modifier une recherche dans la liste des articles d'actualités. Voir **Modification d'une recherche d'article d'actualités de vulnérabilité**.
Actions	Cliquez sur **Actions** et sélectionnez une des options suivantes : • **Print** - Sélectionnez cette option pour imprimer la liste des articles d'actualités. • **Export to XML** - Sélectionnez cette option pour exporter une liste d'articles d'actualités en format XML. Voir **Exportation d'articles d'actualités de vulnérabilité**. • **Export to CSV** - Sélectionnez cette option pour exporter une liste d'articles d'actualités en format CSV. Voir **Exportation d'articles d'actualités de vulnérabilité**.

La page Research News affiche les informations suivantes :

Tableau 9-6 Recherche de paramètres de page d'actualités

Paramètre	Description
Published Date	La date à laquelle l'article d'actualités a été publié.
Source	La source de l'article d'actualités comme un lien. Cliquez sur le lien de la colonne **Source** pour afficher la page d'accueil du site Web qui publie l'article d'actualités.
Titre de l'article	Le titre de l'article d'actualités. Pour afficher le site Web de l'article d'actualités, sélectionnez une des options suivantes : • Cliquez sur le lien de la colonne **Article Title** pour l'article d'actualités que vous souhaitez examiner. • Cliquez deux fois sur une ligne de données sur la page Research News pour l'article d'actualités que vous souhaitez examiner.
Abstract	Un court résumé du début de l'article d'actualités.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research > News**.

Etape 3 Facultatif. Pour étendre vos résultats et afficher les articles d'actualités précédemment publiés, sélectionnez une plage de temps alternative à partir de la zone de liste **Viewing news from**.

Recherche d'articles d'actualités de vulnérabilités

Vous pouvez rechercher la liste des articles d'actualités de vulnérabilité.

A propos de cette tâche

Utilisez les options suivantes pour définir vos critères de recherche d'actualités de vulnérabilités :

Tableau 9-7 Vulnérabilité des options de paramètre de recherche d'actualités

Options	Description
Phrase	Entrez les mots-clés ou phrase pour l'article d'actualités que vous souhaitez rechercher. Vous devez entrer plus de 2 caractères.
Source	Dans la zone de liste **Source**, sélectionnez la source de l'article d'actualités que vous souhaitez rechercher.
Recent	Cliquez sur **Recent** pour activer la zone de liste. **All** est sélectionné par défaut mais vous pouvez choisir une option de plage de temps pour affiner vos critères de recherche.
Specific Interval	Cliquez sur **Specific Interval** pour activer les champs **From Date** et **To Date.** Ceci vous permet de rechercher les vulnérabilités en utilisant un intervalle de dates spécifique.
From Date	Entrez une date de début au format de date qui correspond à votre pays ou sélectionnez une date dans la zone de liste.
To Date	Entrez une date de fin au format de date qui correspond à votre pays ou sélectionnez une date dans la zone de liste.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> News**.

Etape 3 Dans le menu principal, sélectionnez **Search > New Search**.

Etape 4 Entrez vos critères de recherche grâce aux paramètres décrits dans **Tableau 9-7**.

Etape 5 Cliquez sur **Search**.

Modification d'une recherche d'article d'actualités de vulnérabilité

Vous pouvez modifier les critères d'une recherche actuelle d'article d'actualités.

Avant de commencer

Cette procédure suppose que vous avez effectué une recherche d'article d'actualités de vulnérabilité. Pour plus d'informations, voir **Recherche d'articles d'actualités de vulnérabilités**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> News**.

Etape 3 Dans la barre d'outils, sélectionnez **Search > Edit Search**.

Etape 4 Modifiez votre recherche comme exigé grâce aux paramètres décrits dans **Tableau 9-7**.

Etape 5 Cliquez sur **Search**.

Exportation d'articles d'actualités de vulnérabilité

Vous pouvez exporter des articles d'actualités de vulnérabilité en format XML (Extensible Markup Language) ou CVS (comma-separated values).

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research > News**.

Etape 3 Choisissez une des options suivantes :

- Dans la barre d'outils, sélectionnez **Export to XML**.
- Dans la barre d'outils, sélectionnez **Export to CSV**.

Etape 4 La boîte de dialogue **Waiting For Export To Commence** s'affiche avec les options suivantes :

- Facultatif. Cliquez sur **Notify When Done** pour être notifié par e-mail lorsque l'exportation se termine.
- Facultatif. Cliquez sur **Cancel Export** pour annuler l'exportation.

Affichage des recommandations aux vulnérabilités

Vous pouvez afficher les recommandations relatives aux vulnérabilités qui sont publiées par les fournisseurs de logiciel, identifiez les risques de sécurité de votre technologie et comprenez les implications des risques.

A propos de cette tâche

Par défaut, toutes les recommandations publiées pendant les dernières 24 heures sont affichées. Si aucune recommandation n'est affichée, alors sélectionnez une plage de temps alternative à partir de la zone de liste **Viewing advisories from**.

La barre d'outils Research Advisories offre les fonctions suivantes :

Tableau 9-8 Recherche d'options de barre d'outils de recommandation

Fonction	Description
Recherche	**New Search** - Sélectionnez cette option pour rechercher la liste des vulnérabilités. Voir **Recherche de recommandations aux vulnérabilités**.
	Edit Search - Sélectionnez cette option pour modifier une recherche dans la liste de vulnérabilités. Voir **Modification d'une recherche de recommandations aux vulnérabilités**.
Actions	**Print** - Sélectionnez cette option pour imprimer la liste des recommandations.
	Export to XML - Sélectionnez cette option pour exporter une liste de recommandations en format XML. Voir **Exportation des recommandations aux vulnérabilités**.
	Export to CSV - Sélectionnez cette option pour exporter une liste de recommandations en format CSV. Voir **Exportation des recommandations aux vulnérabilités**.

La page Research Advisories offre les informations suivantes :

Tableau 9-9 Paramètres de la page de conseils de recherche

Paramètre	Description
Date de publication	Affiche la date à laquelle la recommandation a été publiée pour la première fois.
Date de la dernière mise à jour	Affiche la date à laquelle la recommandation a été mise à jour pour la dernière fois.
Publisher	Afficher le nom de l'éditeur qui a publié la recommandation.
Advisory	Affiche le nom de la recommandation, y compris tout code de référence y étant associé. Cliquez sur le lien de colonne **Advisory** pour afficher plus de détails sur la recommandation.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research > Advisories**.

Etape 3 Facultatif. Pour étendre vos résultats et afficher les recommandations précédemment publiées, sélectionnez une plage de temps alternative à partir de la zone de liste **Viewing advisories from**.

Affichage des détails de recommandations

Vous pouvez examiner les recommandations et revoir les informations détaillées sur les possibles menaces sur votre entreprise.

A propos de cette tâche

La page Advisory Details offre les informations suivantes :

Tableau 9-10 Paramètres de la page de détails relatifs aux recommandations

Paramètre	Description
Détails relatifs aux recommandations	Détails relatifs aux recommandations.
Publisher	L'intitulé de l'éditeur qui a publié la recommandation.
Published Date	La date à laquelle la recommandation a été publiée.
Last Updated Date	La date à laquelle la recommandation a été mise à jour pour la dernière fois.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> Advisories**.

Etape 3 Facultatif. Pour étendre vos résultats et afficher les recommandations précédemment publiées, sélectionnez une plage de temps alternative à partir de la zone de liste **Viewing advisories from**.

Etape 4 Facultatif. Effectuez une recherche des recommandations aux vulnérabilités. Pour plus d'informations, voir **Recherche de recommandations aux vulnérabilités**.

Etape 5 Choisissez une des options suivantes :

- Cliquez sur le lien de colonne **Advisory**.
- Cliquez deux fois sur une ligne de données pour la recommandation que vous souhaitez examiner.

Recherche de recommandations aux vulnérabilités

Vous pouvez rechercher une recommandation aux vulnérabilités.

A propos de cette tâche

Utilisez les options suivantes pour définir vos critères de recherche de recommandations aux vulnérabilités :

Tableau 9-11 Paramètres de recherche de recommandations aux vulnérabilités

Paramètre	Description
Phrase	Entrez les mots-clés ou phrase pour l'article d'actualités que vous souhaitez rechercher. Vous devez entrer plus de 2 caractères.
Recent	Cliquez sur **Recent** pour activer la zone de liste. **All** est sélectionné par défaut mais vous pouvez choisir une option de plage de temps pour affiner vos critères de recherche.
Specific Interval	Cliquez sur **Specific Interval** pour activer les champs **From Date** et **To Date**. Ceci vous permet de rechercher les vulnérabilités en utilisant un intervalle de dates spécifique.
From Date	Entrez une date de début au format de date qui correspond à votre pays ou sélectionnez une date dans la zone de liste.

Tableau 9-11 Paramètres de recherche de recommandations aux vulnérabilités (suite)

Paramètre	Description
To Date	Entrez une date de fin au format de date qui correspond à votre pays ou sélectionnez une date dans la zone de liste.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> Advisories**.

Etape 3 Dans la barre d'outils, sélectionnez **Search > New Search**.

Etape 4 Entrez vos critères de recherche grâce aux paramètres décrits dans**Tableau 9-11**.

Etape 5 Cliquez sur **Search**.

Modification d'une recherche de recommandations aux vulnérabilités

Vous pouvez modifier les critères d'une recherche de recommandations aux vulnérabilités.

Avant de commencer

Cette procédure suppose que vous avez effectué une recherche d'article d'actualités de vulnérabilité. Pour plus d'informations, voir **Recherche de recommandations aux vulnérabilités**.

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> Advisories**.

Etape 3 Dans la barre d'outils, sélectionnez **Search > Edit Search**.

Etape 4 Modifiez votre recherche comme exigé grâce aux paramètres décrits dans **Tableau 9-11**.

Etape 5 Cliquez sur **Search**.

Exportation des recommandations aux vulnérabilités

Vous pouvez exporter les recommandations aux vulnérabilités en format XML (Extensible Markup Language) ou CSV (Comma Separated Values).

Procédure

Etape 1 Cliquez sur l'onglet **Vulnerabilities**.

Etape 2 Dans le menu de navigation, sélectionnez **Research> Advisories**.

Etape 3 Choisissez une des options suivantes :

- Dans la barre d'outils, sélectionnez **Export to XML**.
- Dans la barre d'outils, sélectionnez **Export to CSV**.

Etape 4 La boîte de dialogue **Waiting For Export To Commence** s'affiche avec les options suivantes :

- Facultatif. Cliquez sur **Notify When Done** pour être notifié par e-mail lorsque l'exportation se termine.
- Facultatif. Cliquez sur **Cancel Export** pour annuler l'exportation.

A GLOSSAIRE

CDP	Voir Collateral Damage Potential.
Chiffrement	Le chiffrement fournit plus de sécurité à tout le trafic QRadar entre les hôtes gérés. Lorsque le chiffrement est activé pour un hôte géré, des tunnels de chiffrement sont créés pour toutes les applications client sur un hôte géré pour fournir un accès protégé aux serveurs respectifs.
CIDR	Voir Classless Inter-Domain Routing.
Classless Inter-Domain Routing	Un plan d'adressage pour Internet, qu'utilisaient les adresses Internet espèce et allouées dans le routage inter-domaine. Avec CIDR, vous ne pouvez utiliser qu'une seule adresse IP pour désigner plusieurs adresses IP.
Client	L'hôte qui est à l'origine de la communication.
Collateral Damage Potential	FIRST (Forum of Incident Response and Security Teams) utilise un indicateur pour mesurer le potentiel de perte de vie ou d'actifs physiques par le biais de l'endommagement ou du vol de propriété ou d'équipement.
Common Vulnerability Scoring System	Dérivé des métriques et des formules, le modèle CVSS fournit aux utilisateurs finaux un indice composite global représentant la gravité et le risque d'une vulnérabilité. Les métriques sont répartis dans trois catégories différentes qui peuvent être mesurées de façon qualitative ou quantitative. Les métriques de base décrivent les qualités de toute vulnérabilité donnée qui ne se modifie pas au fil du temps ou dans plusieurs environnements. Les indicateurs temporels contiennent des caractéristiques d'une vulnérabilité qui évoluent au cours de son cycle de vie. Les indicateurs environnementaux contiennent ces caractères de vulnérabilité qui sont liés à une implémentation dans un environnement utilisateur spécifique. Ce canevas permet de communiquer avec précision les impacts potentiels et les caractéristiques de vulnérabilités. utilisation d'une échelle de 0 à 10.
CVSS	Voir Common Vulnerability Scoring System.
Exclusion local	Empêcher une analyse individuelle d'analyser les actifs certains.
HA	Voir High Availability.

High Availability	La fonction High Availability (HA) assure la disponibilité des données QRadar en cas de défaillance du matériel ou du réseau. Un cluster HA se compose d'un hôte primaire et d'un hôte secondaire qui sert de secours au cluster principal. L'hôte secondaire conserve les mêmes données que l'hôte primaire via l'une des deux méthodes : réplication de données ou mémoire externe partagée. A intervalles réguliers, toutes les 10 secondes par défaut, l'hôte secondaire envoie une commande PING de pulsation à l'hôte primaire pour détecter le matériel et la défaillance du réseau. Si l'hôte secondaire détecte une défaillance, l'hôte secondaire assume automatiquement toutes les responsabilités de l'hôte primaire.
IP	Voir Internet Protocol.
National Vulnerability Database	Un référentiel de données de vulnérabilité du gouvernement des Etats-Unis qui aide les entreprises dans la gestion de la vulnérabilité, la mesure de la sécurité et la conformité.
On Demand Scan	Une analyse exécutée manuellement lorsque vous l'exigez par opposition à une analyse automatique.
Operational Window	Vous permet de définir une plage de temps au cours de laquelle l'exécution d'un profil d'analyse ne doit jamais être autorisée.
PCI Severity	Lors de l'utilisation de CVSS (Common Vulnerability Scoring System), l'option PCI Severity est utilisée pour catégoriser les vulnérabilités avec un niveau de gravité élevé, moyen ou faible et aide ainsi les entreprises dans leur façon de donner la priorité au processus de correction des vulnérabilités.
Processus de résolution	Puisque les vulnérabilités sont détectées sur des hôtes, elles peuvent être manuellement, et dans certains cas, automatiquement affectées aux utilisateurs du système pour résolution ou pour correction.
Protocole IP	La méthode ou le protocole par lequel les données sont envoyées d'un ordinateur vers un autre sur Internet. Chaque ordinateur (connu sous le nom d'hôte) sur Internet dispose au moins d'une adresse IP qui l'identifie uniquement de tous les autres systèmes sur Internet. Une adresse IP comprend une adresse réseau et une adresse hôte. Une adresse IP peut également être divisée à l'aide d'un adressage ou d'un masquage de sous-réseau sans classe.
Scan Exclusion	Restriction de l'analyse de certains actifs, groupes de réseau ou plages CIDR.
Scan Profile	Une série de configuration et de paramètres qui détermine exactement comment et quand les actifs sur réseau sont analysés pour les vulnérabilités.
Simple Network Management Protocol	Un protocole de gestion de réseau utilisé pour superviser les routeurs IP, les autres périphériques réseau et les réseaux auxquels ils sont reliés.
SNMP	Voir Simple Network Management Protocol.

TCP	Voir Transmission Control Protocol.
Transfert de zone DNS	Est un type de transaction DNS généralement utilisé pour les bases de données que fournissent les packs de serveur DNS modernes.
Transmission Control Protocol	Un service de transmission fiable qui opère sur le protocole IP de la couche transport, qui garantit une livraison de bout en bout de paquets de données sans erreur.
UDP	Voir User Datagram Protocol.
User Datagram Protocol	Un protocole couche transport sans connexion qui fournit un seul service de messagerie aux services orientés vers la transaction.
Violation	Un message envoyé ou généré en réponse à une condition surveillée. Par exemple, une violation vous informe de la violation d'une règle ou d'une attaque du réseau.
vulnérabilité	Un bogue, un défaut, une faiblesse ou une exposition d'une application, d'un système, d'un périphérique ou d'un service qui peut mener vers un manquement à la protection de la confidentialité, l'intégrité ou la disponibilité.

B AVIS ET MARQUES

Dans cette annexe :

Cette section décrit quelques avis et marques importants et fournit des informations sur la conformité.

Avis

Ces informations sont destinées aux produits et services offerts aux Etats-Unis.

IBM peut ne pas offrir les produits, les services ou les fonctions décrits dans ce document dans d'autres pays. Contactez votre interlocuteur IBM habituel pour obtenir des informations sur les produits et services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre produit, programme ou service fonctionnellement équivalent peut être utilisé, s'il n'enfreint pas les droits de propriété intellectuelle d'IBM. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier le fonctionnement de tout produit, programme ou service non IBM.

IBM peut détenir des brevets ou des demandes de brevet en instance couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Vous pouvez soumettre des demandes de licences par écrit à l'adresse suivante :

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

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues auprès du service IBM Intellectual Property Department de votre pays/région ou 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, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays/région dans lequel il serait contraire aux lois locales : INTERNATIONAL BUSINESS MACHINES CORPORATION LIVRE LE PRESENT DOCUMENT «EN L'ETAT» SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER, 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 explicites ou implicites pour certaines transactions, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Ces informations peuvent contenir des inexactitudes techniques ou des erreurs typographiques. 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/ou 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 dispositions 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 d'IBM Customer Agreement, d'IBM International Program License Agreement 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 prix IBM indiqués sont des prix de détail suggérés par IBM, sont à jour et peuvent être modifiés sans préavis. Les prix distributeurs peuvent donc varier.

Ces informations contiennent des exemples de données et de rapports utilisés dans les opérations métier habituelles. Pour les illustrer aussi complètement que possible, les exemples incluent les noms des personnes, des sociétés, des marques et des produits. Tous ces noms sont fictifs et toute ressemblance avec des noms et adresses utilisés par une société réelle serait purement fortuite.

Si vous visualisez la copie électronique de ces informations, les photographies et illustrations en couleur peuvent ne pas apparaître.

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM est disponible sur la page Web “Copyright and trademark information” à l'adresse *http:\\www.ibm.com/legal/copytrade.shtml*.

Les noms suivants sont des marques ou des marques déposées d'autres sociétés :

Java et toutes les marques et tous les logos Java sont des marques ou des marques déposées d'Oracle et/ou de ses filiales.

Linux est une marque de Linus Torvalds aux Etats-Unis, dans d'autres pays ou les deux.

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

UNIX est une marque de The Open Group aux Etats-Unis et dans d'autres pays.

INDEX

P

Q

R

S

T

U

V

W