IBM Security QRadar Vulnerability Manager
Version 7.2.1

User Guide

Note

Before using this information and the product that it supports, read the information in “Notices” on page 61.

Contents

Introduction to IBM Security QRadar Vulnerability Manager

This information is intended for use with IBM® Security QRadar® Vulnerability Manager. QRadar Vulnerability Manager is a scanning platform that is used to identify, manage, and prioritize the vulnerabilities on your network assets.

This guide contains instructions for configuring and using QRadar Vulnerability Manager on an IBM Security QRadar SIEM or IBM Security QRadar Log Manager console.

Intended audience

System administrators responsible for configuring IBM Security QRadar Vulnerability Manager must have administrative access to IBM Security QRadar SIEM and to your network devices and firewalls. The system administrator must have knowledge of your corporate network and networking technologies.

Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. QRadar Vulnerability Manager installations and deployments

You access IBM Security QRadar Vulnerability Manager by using the **Vulnerabilities** tab.

Access to the vulnerabilities tab

Depending on the product that you install and whether you upgrade QRadar or install a new system, the **Vulnerabilities** tab might not be displayed.

- If you install QRadar SIEM, the **Vulnerabilities** tab is enabled by default with a temporary license key.
- If you install QRadar Log Manager, the **Vulnerabilities** tab is not enabled.
- Depending on how you upgrade QRadar, the **Vulnerabilities** tab might not be enabled.

To use QRadar Vulnerability Manager after an install or upgrade you must upload and allocate a valid license key. For more information, see the *Administration Guide* for your product.

For more information about upgrading, see the *IBM Security QRadar Upgrade Guide*.

Vulnerability processing and scanning deployments

When you install and license QRadar Vulnerability Manager, a vulnerability processor is automatically deployed on your QRadar console. A processor is not automatically deployed if you use a software activation key on your QRadar console.

The vulnerability processor provides a scanning component by default. If required, you can deploy more scanners, either on dedicated QRadar Vulnerability Manager managed host scanner appliances or QRadar managed hosts. For example, you can deploy a vulnerability scanner on an Event Collector or QRadar QFlow Collector. You cannot deploy a vulnerability scanner on a high availability managed host.

If required, you can move the vulnerability processor to a different managed host in your deployment. You might move the processor to preserve disk space on your QRadar console.

Restriction: You can have only one vulnerability processor in your deployment and you can move the processor only to a dedicated QRadar Vulnerability Manager managed host processor appliance. When you move the vulnerability processor between the console and a managed host, the system enforces validation checks in the deployment editor.

Important: After you change your vulnerability processor deployment, you must wait for your deployment to fully configure. In the Scan Profiles page, the following message is displayed: **QVM is in the process of being deployed.**

To configure your vulnerability processing and scanning components, you must use the QRadar deployment editor, which is on the **Admin** tab.

Ensure that following applications are installed on all desktop systems that you use to access the QRadar product user interface:

- Java™ Runtime Environment (JRE) version 1.7
- Adobe Flash version 10.x

For more information about the deployment editor, see the *Administration Guide* for your product.

Vulnerability processor and scanner appliance activation keys

You can scan and process your vulnerabilities by using dedicated QRadar Vulnerability Manager managed host appliances.

When you install a processor or scanner managed host appliance, you must type a valid activation key.

For more information about installing a managed host appliance, see the *Installation Guide* for your product.

The activation key is a 24-digit, four part, alphanumeric string that you receive from IBM. The activation key specifies which software modules apply for each appliance type:

- The QRadar Vulnerability Manager processor appliance includes vulnerability processing and scanning components.
- The QRadar Vulnerability Manager scanner appliance includes only a vulnerability scanning component.

You can obtain the activation key from the following locations:

- If you purchased a QRadar Vulnerability Manager software or virtual appliance download, a list of activation keys are included in the *Getting Started* document that is attached in a confirmation email. You can use this document to cross-reference the part number for the appliance that you are supplied with.
- If you purchased an appliance that is preinstalled with QRadar Vulnerability Manager software, the activation key is included in your shipping box or CD.

Options for moving the vulnerability processor in your QRadar Vulnerability Manager deployment

If required, you can move the vulnerability processor from your QRadar console to a dedicated QRadar Vulnerability Manager managed host appliance.

For example, you might move your vulnerability processing capability to a managed host to minimize disk space impact on your QRadar console.

Restriction: You can have only one vulnerability processor in your deployment. Also, you must deploy the vulnerability processor only on a QRadar console or QRadar Vulnerability Manager managed host processor appliance.

To move the vulnerability processor, choose one of the following options:

Option 1 Deploy a dedicated QRadar Vulnerability Manager processor appliance

To deploy a processor appliance you must complete the followings tasks:

1. Install a dedicated QRadar Vulnerability Manager managed host processor appliance. For more information, see the *Installation Guide* for your product.
2. Add the managed host processor appliance to your deployment by using the deployment editor.

   When you select the managed host option in the deployment editor, the processor is automatically removed from the QRadar console.

Option 2 Move the vulnerability processor from your console to your managed host

If the vulnerability processor is on your QRadar console, then later you can move your vulnerability processor to a previously installed QRadar Vulnerability Manager managed host processor appliance.

At any time, you can move the vulnerability processor back to your QRadar console.

Deploying a dedicated QRadar Vulnerability Manager processor appliance

You can deploy a dedicated QRadar Vulnerability Manager managed host processor appliance.

When you deploy your vulnerability processor to a managed host, all vulnerabilities are processed on the managed host.

Restriction: After you deploy processing to a dedicated QRadar Vulnerability Manager managed host, any scan profiles or scan results that are associated with a QRadar console processor are not displayed. You can continue to search and view vulnerability data on the **Manage Vulnerabilities** pages.

Before you begin

Ensure that a dedicated QRadar Vulnerability Manager managed host is installed and a valid processor appliance activation key is applied.

Procedure

1. Click the **Admin** tab.
2. On toolbar, click **Deployment Editor**.
3. From the menu, select **Actions** > **Add a Managed Host**.

   In the managed host wizard, ensure that you select the IP address of the QRadar Vulnerability Manager managed host processor appliance.

   You must wait several minutes while the managed host is added.
4. In the Validation Error window, select the QRadar Vulnerability Manager managed host processor and click **OK**.
5. Click **Yes**.
6. In the deployment editor menu, select **File** > **Save and close**.
7. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
8. Click **OK**.

What to do next

Verify that the QRadar Vulnerability Manager processor is deployed on the managed host.

Related concepts:

"Vulnerability processor and scanner appliance activation keys" on page 2
You can scan and process your vulnerabilities by using dedicated QRadar Vulnerability Manager managed host appliances.

Related tasks:

"Verifying that a vulnerability processor is deployed"
In IBM Security QRadar Vulnerability Manager, you can verify that your vulnerability processor is deployed on a QRadar console or QRadar Vulnerability Manager managed host.

Moving your vulnerability processor to a managed host or console

If required, you can move your vulnerability processor between a QRadar Vulnerability Manager managed host appliance and your QRadar console.

Before you begin

Ensure that a dedicated QRadar Vulnerability Manager managed host is installed and a valid processor appliance activation key is applied.

Procedure

1. Click the **Admin** tab.
2. On the toolbar, click **Deployment Editor**.
3. Click the **Vulnerability View** tab.
4. In the Vulnerability Components pane click **QVM Processor**.
5. Type a memorable name for the **QVM Processor** that you want to add, then follow the instructions in the user interface and click **Next**.
6. In the Adding a new component window, ensure that you select the host for the console or managed host appliance.

   If your processor is on the managed host, you can select only the QRadar console.
7. Click **Finish** and **Yes**.
8. In the deployment editor menu, select **File** > **Save and close**.
9. In the Validation Error window, select the processor on the console or managed host.

   If you select the processor on the console, then the vulnerability processor on the managed host is automatically removed during the deployment.

   You must wait several minutes while the deployment completes.
10. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
11. Click **OK**.

Verifying that a vulnerability processor is deployed

In IBM Security QRadar Vulnerability Manager, you can verify that your vulnerability processor is deployed on a QRadar console or QRadar Vulnerability Manager managed host.

Procedure

1. Log in to the QRadar console.
2. On the **Admin** tab, click the **Deployment Editor**.
3. Select the **Vulnerability View** tab.
4. Verify that the **QVM Processor** is displayed in the Vulnerability View pane.

What to do next

If the **QVM Processor** is not deployed, then you must deploy the processor. "Moving your vulnerability processor to a managed host or console" on page 4.

Removing a vulnerability processor from your console or managed host

If required, you can remove the vulnerability processor from a QRadar console or QRadar Vulnerability Manager managed host.

Procedure

1. Log in to the QRadar console.
2. On the **Admin** tab, click **Deployment Editor**.
3. Select the **Vulnerability View** tab.
4. Select the **QVM Processor** on the Vulnerability View pane.
5. In the Warning window, click **Yes**.
6. From the **Deployment Editor** menu, select **Edit** > **Delete**.
7. From the **Deployment Editor** menu, select **File** > **Save and close**.
8. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
9. Click **OK**.

Options for adding scanners to your QRadar Vulnerability Manager deployment

If you have a large network and require flexible scanning options, you can add more scanners to your QRadar Vulnerability Manager deployment.

Your QRadar Vulnerability Manager processor is automatically deployed with a scanning component. By deploying more scanners you can increase the flexibility of your scanning operations. For example, you can scan specific areas of your network with different scanners and at different scheduled times.

To add more vulnerability scanners, choose any of the following options:

Option 1 Deploy a dedicated QRadar Vulnerability Manager managed host scanner appliance

You can scan for vulnerabilities by using a dedicated QRadar Vulnerability Manager managed host scanner appliance.

To deploy a scanner appliance, you must complete the followings tasks:

1. Install a dedicated QRadar Vulnerability Manager managed host scanner appliance.
2. Add the managed host scanner appliance to your deployment by using the deployment editor.

Option 2 Deploy a QRadar Vulnerability Manager scanner on your QRadar console

If you move your vulnerability processor from your QRadar console to a QRadar Vulnerability Manager managed host, you can add a scanner to your console.

Option 3 Deploy a scanner to a QRadar managed host

You can add a vulnerability scanner to any preexisting QRadar managed hosts in your deployment. For example, you can add a scanner to an event collector, flow collector, or event processor.

Restriction: You cannot add a vulnerability scanner to a high availability managed host.

Option 4 Configure access to an IBM hosted scanner and scan your DMZ

You can configure access to an IBM hosted scanner and scan the assets in your DMZ.

Deploying a dedicated QRadar Vulnerability Manager scanner appliance

You can deploy a dedicated QRadar Vulnerability Manager managed host scanner appliance.

Before you begin

Ensure that a dedicated QRadar Vulnerability Manager managed host scanner appliance is installed and a valid appliance activation key is applied.

Procedure

1. Click the **Admin** tab.
2. On the toolbar, click **Deployment Editor**.
3. From the menu, select **Actions** > **Add a managed host**.

   In the managed host wizard, ensure that you select the IP address of the QRadar Vulnerability Manager managed host scanner appliance.

   You must wait several minutes while the deployment saves.
4. At the Adding Managed Host dialog box, click **OK**.
5. From the deployment editor menu, select **File** > **Save and close**.
6. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration.**.
7. Click **OK**.

Related concepts:

"Vulnerability processor and scanner appliance activation keys" on page 2
You can scan and process your vulnerabilities by using dedicated QRadar Vulnerability Manager managed host appliances.

Deploying a vulnerability scanner to a QRadar console or managed host

You can deploy a QRadar Vulnerability Manager scanner to a QRadar console or managed host. For example, you can deploy a scanner to a flow collector, flow processor, event collector, or event processor.

Before you begin

To deploy a scanner on your QRadar console, ensure that the vulnerability processor is moved to a dedicated QRadar Vulnerability Manager managed host appliance.

To deploy scanners on QRadar managed hosts, ensure that you have existing managed hosts in your deployment. For more information, see the *Installation Guide* for your product.

Procedure

1. On the **Admin** tab, click **Deployment Editor**.
2. Select the **Vulnerability View** tab.
3. On the Vulnerability Components pane, click **QVM Scanner**.
4. Type a unique name for the **QVM Scanner** that you want to add.

   Restriction: The name can be up to 20 characters in length and can include underscores or hyphens.
5. Click **Next**.
6. From the **Select a host** list box, select the **IP address** of the QRadar managed host or console.

   Restriction: You cannot add a scanner to a QRadar console when the vulnerability processor is on the console. You must move the vulnerability processor to a QRadar Vulnerability Manager managed host.
7. Click **Next**.
8. Click **Finish**.
9. From the deployment editor menu, select **File** > **Save and close**.
10. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration.**.
11. Click **OK**.

What to do next

Verify that the external scanner is listed in the **Scan Server** list box in the **Scan Profile Details** expandable pane.

Related concepts:

"Scan profile details" on page 20
In IBM Security QRadar Vulnerability Manager you can describe your scan, select the scanner that you want to use, and choose from a number of scan type options.

Related tasks:

"Moving your vulnerability processor to a managed host or console" on page 4
If required, you can move your vulnerability processor between a QRadar Vulnerability Manager managed host appliance and your QRadar console.

Scanning the assets in your DMZ

In IBM Security QRadar Vulnerability Manager, you can connect to an external scanner and scan the assets in your DMZ for vulnerabilities.

If you want to scan the assets in the DMZ for vulnerabilities, you do not need to deploy a scanner in your DMZ. You must configure QRadar Vulnerability Manager with a hosted IBM scanner that is located outside your network.

Detected vulnerabilities are processed by the processor on either your QRadar console or QRadar Vulnerability Manager managed host.

Procedure

1. Configure your network and assets for external scans.
2. Configure QRadar Vulnerability Manager to scan your external assets.

Configuring your network and assets for external scans

To scan the assets in your DMZ, you must configure your network and inform IBM of the assets that you want to scan.

Procedure

1. Configure outbound internet access on port 443.
2. Send the following information to `QRadar-QVM-Hosted-Scanner@hursley.ibm.com`:
   - Your organization's external IP address.

     Restriction: The IP address must be configured before you can run external scans.
   - The IP address range of the assets in your DMZ.

Configuring QRadar Vulnerability Manager to scan your external assets

To scan the assets in your DMZ you must configure QRadar Vulnerability Manager, by using the deployment editor.

Procedure

1. On the **Admin** tab, click **Deployment Editor**.
2. Click the **Vulnerability View** tab.
3. In the Vulnerability Components pane, click **External Scanner**.
4. Type a unique name for the External Scanner that you want to add.
5. Click **Next**.
6. Type your external IP address and click **Next**.

   Restriction: You cannot scan external assets until your external IP address is configured. Ensure that you email details of your external IP address to IBM.
7. Optional: If your network is configured to use a proxy server, then type the details of your server, then click **Next**.
8. Click **Finish**.
9. From the deployment editor menu, select **File** > **Save and close**.
10. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
11. Click **OK**.

What to do next

Verify that the external scanner is listed in the **Scan Server** list box in the **Scan Profile Details** expandable pane.

For more information, see “Scan profile details” on page 20.

Supported web browsers

For the features in IBM Security QRadar products to work properly, you must use a supported web browser.

When you access the QRadar system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following tables list the supported versions of web browsers.

Table 1. Supported web browsers for QRadar products

Web browser	Supported version
Mozilla Firefox	• 10.0 Extended Support Release (ESR) • 10.0 Extended Support Release (ESR)
Microsoft Internet Explorer, with document mode and browser mode enabled	• 8.0 • 9.0
Google Chrome	• Latest version

Enabling document mode and browser mode in Internet Explorer

If you use Microsoft Internet Explorer to access IBM Security QRadar products, you must enable browser mode and document mode.

Procedure

1. In your Internet Explorer web browser, press F12 to open the Developer Tools window.
2. Click **Browser Mode** and select the version of your web browser.
3. Click **Document Mode** and select **Internet Explorer 7.0 Standards**.

Vulnerability backup and recovery

You can back up and recover your vulnerability data including vulnerability configurations. For example, you can back up scan profiles.

QRadar Vulnerability Manager back up and recovery is managed by using the **Admin** tab.

For more information about vulnerability backup and recovery, see the *Administration Guide* for your product.

Chapter 2. IBM Security QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager is a network scanning platform that detects vulnerabilities within the applications, systems, and devices on your network or within your DMZ.

QRadar Vulnerability Manager uses security intelligence to help you manage and prioritize your network vulnerabilities. For example, you can use QRadar Vulnerability Manager to continuously monitor vulnerabilities, improve resource configuration, and identify software patches. You can also, prioritize security gaps by correlating vulnerability data with network flows, log data, firewall, and intrusion prevention system (IPS) data.

You can maintain real-time visibility of the vulnerabilities that are detected by the built-in QRadar Vulnerability Manager scanner and other third-party scanners. Third-party scanners are integrated with QRadar and include IBM Security EndPoint Manager, Guardium®, AppScan®, Nessus, nCircle, and Rapid 7.

Unless otherwise noted, all references to QRadar Vulnerability Manager refer to IBM Security QRadar Vulnerability Manager. All references to QRadar refer to IBM Security QRadar SIEM and IBM Security QRadar Log Manager and all references to SiteProtector™ refer to IBM Security SiteProtector.

Vulnerability scanning

In IBM Security QRadar Vulnerability Manager, vulnerability scanning is controlled by configuring scan profiles. Each scan profile specifies the assets that you want to scan and the scan schedule.

Vulnerability processor

When you license QRadar Vulnerability Manager, a vulnerability processor is automatically deployed on your QRadar console. The processor contains a QRadar Vulnerability Manager scanning component.

Deployment options

Vulnerability scanning can be deployed in different ways. For example, you can deploy your scanning capability to a QRadar Vulnerability Manager managed host scanner appliance or a QRadar managed host.

Configuration options

Administrators can configure scans in the following ways:

- Schedule scans to run at times convenient for your network assets.
- Specify the times during which scans are not allowed to run.
- Specify the assets that you want to exclude from scans, either globally or for each scan.
- Configure authenticated patch scans for Linux, UNIX, or Windows operating systems.

- Configure different scanning protocols or specify the port ranges that you want to scan.

Related concepts:

"Options for adding scanners to your QRadar Vulnerability Manager deployment" on page 5
If you have a large network and require flexible scanning options, you can add more scanners to your QRadar Vulnerability Manager deployment.

Vulnerability management dashboard

You can display vulnerability information on your QRadar dashboard.

IBM Security QRadar Vulnerability Manager is distributed with a default vulnerability dashboard so that you can quickly review the risk to your organization.

You can create a new dashboard, manage your existing dashboards, and modify the display settings of each vulnerability dashboard item.

For more information about dashboards, see the *Users Guide* for your product.

Reviewing vulnerability data on the default vulnerability management dashboard

You can display default vulnerability management information on the QRadar dashboard.

The default vulnerability management dashboard contains risk, vulnerability, and scanning information.

You can configure your own dashboard to contain different elements like saved searches.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, in the **Show Dashboard** list, select **Vulnerability Management**.

Creating a customized vulnerability management dashboard

In QRadar you can create a vulnerability management dashboard that is customized to your requirements.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, click **New Dashboard**.
3. Type a **Name** and **Description** for your vulnerability dashboard.
4. Click **OK**.
5. Optional: On the toolbar select **Add Item** > **Vulnerability Management** and choose from the following options:
   - If you want to show default saved searches on your dashboard, select **Vulnerability Searches**.
   - If you want to show website links to security and vulnerability information, select **Security News**, **Security Advisories**, or **Latest Published Vulnerabilities**.

- If you want show information that is about completed or running scans, select **Scans Completed** or **Scans In Progress**.

Related tasks:

"Saving your vulnerability search criteria" on page 41
In IBM Security QRadar Vulnerability Manager, you can save your vulnerability search criteria for future use.

Chapter 3. Security software integrations

IBM Security QRadar Vulnerability Manager integrates with other security products to help you manage and prioritize your security risks.

IBM Security QRadar Risk Manager and IBM Security QRadar Vulnerability Manager integration

IBM Security QRadar Vulnerability Manager integrates with QRadar Risk Manager to help you prioritize the risks and vulnerabilities in your network.

QRadar Risk Manager is installed as a managed host and added to your QRadar SIEM console by using the deployment editor.

For more information about installing QRadar Risk Manager, see the *IBM Security QRadar Risk Manager Installation Guide*.

Risk policies and vulnerability prioritization

You can integrate QRadar Vulnerability Manager with QRadar Risk Manager by defining and monitoring asset or vulnerability risk policies.

When the risk policies that you define in QRadar Risk Manager either pass or fail, then the vulnerability risk scores in QRadar Vulnerability Manager are adjusted. The adjustment levels depend on the risk policies in your organization.

When the vulnerability risk scores are adjusted in QRadar Vulnerability Manager, administrators can do the following tasks:

- Gain immediate visibility of the vulnerabilities that failed a risk policy.

  For example, new information might be displayed on the QRadar dashboard or sent by using email.
- Reprioritize the vulnerabilities that require immediate attention.

  For example, an administrator can use the **Risk Score** to quickly identify high risk vulnerabilities.

If you apply risk policies at an asset level in QRadar Risk Manager, then all the vulnerabilities on that asset have their risk scores adjusted.

For an example of how QRadar Vulnerability Manager integrates with QRadar Risk Manager, see “Prioritizing high risk vulnerabilities by applying risk policies” on page 46.

For more information about creating and monitoring risk policies, see the *IBM Security QRadar Risk Manager User Guide*.

IBM Endpoint Manager integration

IBM Security QRadar Vulnerability Manager integrates with IBM Endpoint Manager to help you filter and prioritize the vulnerabilities that can be fixed.

Integration components

A typical QRadar Vulnerability Manager IBM Endpoint Manager integration consists of the following components:

- An IBM Security QRadar console.
- A licensed installation of QRadar Vulnerability Manager.
- An IBM Endpoint Manager server installation.
- An IBM Endpoint Manager agent installation on each of the scan targets in your network.

Vulnerability remediation

Depending on whether you installed and integrated IBM Endpoint Manager, QRadar Vulnerability Manager provides different information to help you remediate your vulnerabilities.

- If IBM Endpoint Manager is not installed, then QRadar Vulnerability Manager provides information about vulnerabilities for which a fix is available.

  QRadar Vulnerability Manager maintains a list of vulnerability fix information. Fix information is correlated against the known vulnerability catalog.

  Using the QRadar Vulnerability Manager search feature, you can identify vulnerabilities that have an available fix.
- If IBM Endpoint Manager is installed, then QRadar Vulnerability Manager also provides specific details about the vulnerability fix process. For example, a fix might be scheduled or an asset might be already fixed.

  The IBM Endpoint Manager server gathers fix information from each of the IBM Endpoint Manager agents. Fix status information is transmitted to QRadar Vulnerability Manager at pre-configured time intervals.

  Using the QRadar Vulnerability Manager search feature, you can quickly identify those vulnerabilities that are scheduled to be fixed or are already fixed.

Related tasks:

"Identifying the patch status of your vulnerabilities" on page 48
In IBM Security QRadar Vulnerability Manager, you can identify the patch status of your vulnerabilities.

Configuring secure socket layer (SSL) for IBM Endpoint Manager integration

You can configure secure socket layer (SSL) encryption to integrate QRadar Vulnerability Manager with IBM Endpoint Manager.

Procedure

1. To download the public key certificate, open your web browser and type `https://`*`IP address`*`/webreports`.

   Remember: The *IP address* is the IP address of your IBM Endpoint Manager server.
2. Click **Add Exception**.
3. In the Add Security Exception window, click **View**.
4. Click the **Details** tab and click **Export**.
5. In the **File name:** field, type `iemserver_cert.der`
6. In the **Save as type:** field, select **X.509 Certificate (DER)**.

7. Click **Save**.
8. Copy the public key certificate to your QRadar console.
9. Optional: To create a QRadar Vulnerability Manager truststore.
   a. Using SSH, log in to the IBM Security QRadar SIEM console as the root user.
   b. Type the following command:
      ```
      keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias iem.
      ```
   c. At the prompts, type the appropriate information to create the truststore.
10. To import the public key certificate to your truststore, type the following command:
    ```
    keytool -importcert -file iemserver_cert.der -keystore truststore.jks
    -storepass <your truststore password> -alias iem_crt_der
    ```
11. At the **Trust this certificate?** prompt, type **Yes**.

Integrating IBM Security QRadar Vulnerability Manager with IBM Endpoint Manager

You can integrate IBM Security QRadar Vulnerability Manager, with IBM Endpoint Manager.

Before you begin

The following components must be installed on your network:

- An IBM Endpoint Manager server.
- An IBM Endpoint Manager agent on each asset in your network that you scan.

If you use secure socket layer (SSL) encryption, ensure that you configure secure socket layer (SSL) for IBM Endpoint Manager integration.

Procedure

1. Using SSH, log in to the IBM Security QRadar SIEM console as the root user.
2. Change directory to following location:
   ```
   /opt/qvm/iem
   ```
3. To configure the QRadar Vulnerability Manager IBM Endpoint Manager adapter, type the following commands:
   a. Type `./iem-setup-webreports.pl`
   b. Type the *IP address* of the IBM Endpoint Manager server.
   c. Type the *User name* of the IBM Endpoint Manager server.
   d. Type the *Password* of the IBM Endpoint Manager server.
4. Optional: At the **Use SSL encryption?** prompt, type the appropriate response.

   Important: If you type `Yes`, then ensure that the prerequisite conditions are met.
5. Type the location of your truststore.
6. Type your truststore password.

IBM Security SiteProtector integration

QRadar Vulnerability Manager integrates with IBM Security SiteProtector to help direct intrusion prevention system (IPS) policy.

When you configure SiteProtector, the vulnerabilities that are detected by scans are automatically forwarded to SiteProtector.

SiteProtector receives vulnerability data from QRadar Vulnerability Manager scans that are performed only after the integration is configured.

Connecting to IBM Security SiteProtector

You can forward vulnerability data to IBM Security SiteProtector to help direct intrusion prevention system (IPS) policy.

Procedure

1. On the **Admin** tab, click **Deployment Editor**.
2. Select the **Vulnerability View** tab.
3. On the Vulnerability Components pane, click **SiteProtector Adapter**.
4. Type a unique name for the SiteProtector Adapter that you want to add and click **Next**.

   The name can be up to 20 characters in length and can include underscores or hyphens.
5. Type the IP address of the IBM Security SiteProtector agent manager server.
6. Click **Next**.
7. Click **Finish**.
8. From the deployment editor menu, select **File** > **Save and close**.
9. On the **Admin** tab toolbar, select **Advanced** > **Deploy Full Configuration**.
10. Click **OK**.

What to do next

Scan your network assets to determine if the vulnerability data is displayed in your SiteProtector installation.

Chapter 4. Vulnerability scanning

Using IBM Security QRadar Vulnerability Manager you can scan your network assets for known vulnerabilities. All network scanning is controlled by the scan profiles that you create.

Scan profiles

You can create multiple scan profiles and configure each differently to account for the specific requirements of your network.

You can run scans manually or schedule scans to run at convenient times for your network environment. You can also specify the network nodes, domains, or virtual domains that you want to scan. If required, you can include Windows, UNIX, or Linux authenticated patch scanning.

Using scan profiles, you can do the following tasks:

- Review information about existing scan profiles.
- Specify the network assets that you want to exclude from all scanning.
- Create operational windows, which define the times at which scans can run.
- Manually run scan profiles or schedule scan to run at a future date.

QRadar integration

QRadar Vulnerability Manager integrates with QRadar to provide the option to scan the assets that form part of a saved asset search.

Creating a scan profile

In IBM Security QRadar Vulnerability Manager, you configure scan profiles to specify how and when your network assets are scanned for vulnerabilities.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Actions** > **Create**.
4. In the **Scan Profile Details** pane of the Scan Profile Configuration page, enter text in the **Profile Name** field.

   To create a scan profile, the only mandatory field in the **Scan Profile Details** pane is the **Profile Name** field. All other parameters are optional.
5. Optional: If you added more scanners to your QRadar Vulnerability Manager deployment, you can select a different scanner from the **Scan Server** list.
6. Optional: To scan your network by using a predefined set of scanning criteria, select a scan from the **Type of Scan** list.
7. Click the **What To Scan** pane.
8. In the **Include Network Nodes** pane, enter an IP address, IP range, or CIDR range in the **CIDR Range/IP/IP Range** field.

   The only mandatory field in the **What To Scan** pane is the **CIDR Range/IP/IP Range** field. All other parameters are optional.

9. Click **Add**.
10. Click **Save**.

Related tasks:

"Running a scan profile manually" on page 32
In IBM Security QRadar Vulnerability Manager you can run a scan profile manually.

Viewing scan profiles

You can view existing scan profiles, monitor the status of scans, and identify the time that a scan takes to complete.

Procedure

1. Click the **Vulnerabilities** tab.
2. On the navigation menu, select **Administrative** > **Scan Profiles**.

   A scan profile can show a status of **Stopped**. A status of **Stopped** indicates that the scan completed successfully or was canceled.
3. Optional: To display more information about a scan profile, hover your mouse on the **Profile Name** field.

Monitoring scans in progress

In IBM Security QRadar Vulnerability Manager, you can monitor the progress of a scan that is running. You can also monitor the status of the scanning tools that are either queued or running.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. Optional: Select a scan and on the toolbar click **Actions** > **Run Now**.
4. Hover your mouse on the **Progress** field while the scan is running.

Scan profile details

In IBM Security QRadar Vulnerability Manager you can describe your scan, select the scanner that you want to use, and choose from a number of scan type options.

Scan profile details are specified in the **Scan Profile Details** pane, in the Scan Profile Configuration page.

You can configure the following options:

Table 2. Scan profile details configuration options

Options	**Description**
Active	Specifies whether you want to run the scan automatically at a scheduled time in the future. By default this check box is selected.
Update asset model	Specifies whether you want to send your scan results to the QRadar asset model. When you configure a scan profile, this check box is selected by default. For more information about Assets and the QRadar asset model, see the *Users Guide* for your product.

Table 2. Scan profile details configuration options (continued)

Options	Description
Scan Server	The scanner that is used to run the scan profile. The scanner that you select depends on your network configuration. For example, to scan DMZ assets, then select a scanner that has access to that area of your network. The **Controller** scan server corresponds to the scanner that is deployed with the vulnerability processor on your QRadar console or QRadar Vulnerability Manager managed host. **Restriction:** You can have only one vulnerability processor in your deployment. However, you can deploy multiple scanners either on dedicated QRadar Vulnerability Manager managed host scanner appliances or QRadar managed hosts.
Bandwidth Limit	The scanning bandwidth. The default setting is Medium. **Important:** If you select a value greater than 1000 kbps, you can affect network performance.
Type of scan	The pre-configured scanning criteria about ports and protocols. **Restriction:** Any selections that you make in the **How To Scan** pane supersede all scan types apart from **PCI Scan**.

Scan scheduling

In IBM Security QRadar Vulnerability Manager, you can schedule the dates and times that it is convenient to scan your network assets for known vulnerabilities.

Scan scheduling is controlled by using the **When To Scan** pane, in the Scan Profile Configuration page.

A scan profile that is configured with a manual setting must be run manually. However, scan profiles that are not configured as manual scans, can also be run manually.

When you select a scan schedule, you can further refine your schedule by configuring a permitted scan interval.

Related tasks:

"Configuring a permitted scan interval" on page 30
In IBM Security QRadar Vulnerability Manager, you can create an operational window to specify the times that a scan can run.

Scanning domains monthly

In IBM Security QRadar Vulnerability Manager, you can configure a scan profile to scan the domains on your network each month.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, select **Actions** > **Create**.
4. In the **Scan Profile Details** pane, type a name for your scan profile in the **Profile Name** field.

5. Click the **When To Scan** pane.
6. In the **Run Schedule** list, select **Monthly**.
7. In the **Start Time** field, select a start date and time for your scan.
8. In the **Day of the month** field, select a day each month that your scan runs.
9. Click the **What To Scan** pane.
10. In the **Domains** field, type the URL of the asset that you want to scan.
11. Click **Add**.
12. Click **Save**.
13. Optional: During and after the scan, you can monitor scan progress and review completed scans.

Scheduling scans of new unscanned assets

In IBM Security QRadar Vulnerability Manager, you can configure scheduled scans of newly discovered, unscanned network assets.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**, then on the toolbar click **Search** > **New Search**.
3. To specify your newly discovered, unscanned assets, complete the following steps in the **Search Parameters** pane:
   a. Select **Days Since Asset Found**, **Less than 2** then click **Add Filter**.
   b. Select **Days Since Asset Scanned Greater than 2** then click **Add Filter**.
   c. Click **Search**.
4. On the toolbar, click **Save Criteria** and complete the following steps:
   a. In the **Enter the name of this search** field, type the name of your asset search.
   b. Click **Include in my Quick Searches**.
   c. Click **Share with Everyone**.
   d. Click **OK**.
5. Click the **Vulnerabilities** tab.
6. In the navigation pane, select **Administrative** > **Scan Profiles**.
7. On the toolbar, select **Actions** > **Create**.
8. In the **Scan Profile Details** pane, type a name for your scan profile in the **Profile Name** field.

   Restriction: The profile name must be greater than 4 characters.
9. Click the **When To Scan** pane and in the **Run Schedule** list, select **Weekly**.
10. In the **Start Time** fields, type or select the date and time that you want your scan to run on each selected day of the week.
11. Select the check boxes for the days of the week that you want your scan to run.
12. Click the **What To Scan** pane.
13. In the Include Saved Searches pane, select your saved asset search from the **Available Saved Searches** list.
14. Click **Add** and **Save**.

    For more information about using the **Assets** tab and saving asset searches, see the *Users Guide* for your product.

Network scan targets and exclusions

In IBM Security QRadar Vulnerability Manager, you can provide information about the assets, domains, or virtual webs on your network that you want to scan.

Use the **What To Scan** pane on the Scan Profile Configuration page to specify the network assets that you want to scan.

You can exclude a specific host or range of hosts that must never be scanned. For example, you might restrict a scan from running on critical servers that are hosting your production applications. You might also want to configure your scan to target only specific areas of your network.

QRadar Vulnerability Manager integrates with QRadar by providing the option to scan the assets that form part of a saved asset search. For more information, see "Scheduling scans of new unscanned assets" on page 22.

Include network nodes

You can specify your scan targets by defining a CIDR range, IP address, IP address range, or a combination of all 3.

For more information about scanning assets, see "Configuring a basic asset scan" on page 32.

Domain scanning

You can add domains to your scan profile to test for DNS zone transfers on each of the domains that you specify.

A host can use the DNS zone transfer to request and receive a full zone transfer for a domain. Zone transfer is a security issue because DNS data is used to decipher the topology of your network. The data that is contained in a DNS zone transfer is sensitive and therefore any exposure of the data might be perceived as a vulnerability. The information that is obtained might be used for malicious exploitation such as DNS poisoning or spoofing.

For more information about configuring a Domain Scan, see "Scanning domains monthly" on page 21

Scans that used saved asset searches

You can scan the assets and IP addresses that are associated with a QRadar saved asset search.

Using the **Assets** tab, any saved searches are displayed in the **Include Saved Searches** section of the What To Scan pane.

For more information about configuring a scan profile with a saved asset search, see "Scheduling scans of new unscanned assets" on page 22

For more information about saving an asset search, see the *Users Guide* for your product.

Exclude network scan targets

In the Exclude network nodes pane, you can specify the assets that must not be scanned. For example, if you want to avoid scanning a highly loaded, unstable, or sensitive server, exclude these assets.

When you configure a scan exclusion in a scan profile configuration, the exclusion applies only to the scan profile.

For more information, see "Excluding assets from all scans."

Virtual webs

You can configure a scan profile to scan different URLs that are hosted on the same IP address.

When you scan a virtual web, QRadar Vulnerability Manager checks each web page for SQL injection and cross site scripting vulnerabilities.

Excluding assets from all scans

In IBM Security QRadar Vulnerability Manager, scan exclusions specify the assets in your network that are not scanned.

Scan exclusions apply to all scan profile configurations and might be used to exclude scanning activity from unstable or sensitive servers.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Exclusions**.
3. On the toolbar, select **Actions** > **Add**.
4. In the **IP/IP Range** field, type the IP address or range of IP addresses that you want to exclude from all scanning.

   Restriction: You cannot type the IP address of an asset that is already excluded from scanning
5. In the **Description** field, type information about the scan exclusion.

   Provide a description that it is identifiable in the future. The description must contain at least 5 characters.

Managing scan exclusions

In IBM Security QRadar Vulnerability Manager you can update, delete, or print scan exclusions.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Exclusions**.
3. From the list on the Scan Exclusions page, click the **Scan Exclusion** that you want to modify.
4. On the toolbar, select an option from the **Actions** menu.
5. Depending on your selection, follow the on-screen instructions to complete this task.

Scan protocols and ports

In IBM Security QRadar Vulnerability Manager, you can choose different scan protocols and scan various port ranges.

Use the **How To Scan** pane on the Scan Profile Configuration page to specify scanning protocols and the ports that you want to scan.

You can configure your scan profile port protocols by using the following options:

Table 3. scan protocol and port options

Protocol	Description
TCP and UDP	The default scan protocol and scans most ports in the range 1 - 1024.
TCP	The most common scanning protocol. When TCP scanning is combined with IP range scanning, you can locate a host that is running services that are prone to vulnerabilities. The default port range is 1 - 65535.
SYN	Sends a packet to all specified ports. If the target is listening, it responds with a SYN and Acknowledgement (ACK). If the target is not listening, it responds with an RST (reset). Normally, the destination port is closed and an RST is returned. The default port range is 1 - 65535.
ACK	Similar to SYN, but in this case an ACK flag is set. The ACK scan does not determine whether the port is open or closed, but tests if the port is filtered or unfiltered. Testing the port is useful when you probe for the existence of a firewall and its rule sets. Simple packet filtering enables established connections (packets with the ACK bit set), whereas a more sophisticated stateful firewall might not. The default port range is 1-65535.
FIN	A TCP packet that is used to terminate a connection, or it can be used as a method to identify open ports. FIN sends erroneous packets to a port and expects open listening ports to send back different error messages than closed ports. The scanner sends a FIN packet, which might close a connection that is open. Closed ports reply to a FIN packet with an RST. Open ports ignore the packet in question. The default port range is 1 - 65535.

Scanning a full port range

In IBM Security QRadar Vulnerability Manager, you can scan the full port range on the assets that you specify.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, select **Actions** > **Create**.
4. In the Scan Profile Details pane, type a name for your Scan Profile in the **Profile Name** field.

   Restriction: The profile name must be greater than 4 characters.
5. Click the **What To Scan** pane.
6. In the **CIDR Range/IP/IP Range** field, type the CIDR range of the assets that you want to scan.
7. Click the **How To Scan** pane.

8. In the **Protocol** field, accept the default values of **TCP & UDP**.
9. In the **Range field**, type **1-65535**.

   Restriction: Port ranges must be configured in dash-separated, comma-delimited, consecutive, ascending, and non-overlapping order. Multiple port ranges must be separated by a comma. For example, the following examples show the delimiters that are used to enter port ranges:(1-1024, 1055, 2000-65535).
10. In the **Max Hosts** field, type the maximum number of hosts that you want to scan concurrently.

    You can type any value in the range 1 - 255.
11. In the **Timeout (m)** field, type the timeout period in minutes after which you want the scan to timeout.

    Important: You can type any value in the range 1 - 500. Ensure that you do not enter a time that is too short, otherwise the scan can timeout without discovering any ports.
12. Click **Save**.
13. Optional: In the Scan Profiles page, on the toolbar select **Actions** > **Run Now**.

Scanning assets with open ports

In IBM Security QRadar Vulnerability Manager, you can configure a scan profile to scan assets with open ports.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles** then on the toolbar, click **Search** > **New Search**.
3. To specify assets with open ports, configure the following options in the **Search Parameters** pane:
   a. Select **Assets With Open Port**, **Equals any of 80** and click **Add Filter**.
   b. Select **Assets With Open Port**, **Equals any of 8080** and click **Add Filter**.
   c. Click **Search**.
4. On the toolbar, click **Save Criteria** and configure the following options:
   a. In the **Enter the name of this search** field, type the name of your asset search.
   b. Click **Include in my Quick Searches**.
   c. Click **Share with Everyone** and click **OK**.
5. Click the **Vulnerabilities** tab.
6. In the navigation pane, select **Administrative** > **Scan Profiles**.
7. On the toolbar, select **Actions** > **Create**.
8. In the **Scan Profile Details** pane, type a name for your scan profile in the **Profile Name** field.

   Restriction: The profile name must be greater than 4 characters.
9. Click the **When To Scan** pane and in the **Run Schedule** list, select **Manual**.
10. Click the **What To Scan** pane.
11. In the Include Saved Searches pane, select your saved asset search from the **Available Saved Searches** list.

When you include a saved asset search in your scan profile, the assets and IP addresses associated with the saved search are scanned.

12. Click **Add** and **Save**.

    For more information about saving an asset search, see the *Users Guide* for your product.

What to do next

Perform the steps in the procedure, “Running a scan profile manually” on page 32.

Authenticated patch scans

In IBM Security QRadar Vulnerability Manager, you can scan for community names and do authenticated patch scans for Windows, Linux, and UNIX operating systems.

Use the **Scan Setup** pane on the Scan Profile Configuration page to specify your patch scan setup.

SNMP community names

You can scan your network assets by using SNMP Community Names.

When you scan assets, QRadar Vulnerability Manager authenticates with the SNMP services that are found and completes a more detailed vulnerability scan.

Linux, UNIX, and Windows patch scans

You can patch scan any Linux, UNIX, or Windows operating system that is on your network.

To do Windows operating systems patch scanning, remote registry access and Windows management interface (WMI) must be enabled. If your windows patch scan returns WMI connectivity issues you must configure your windows systems.

To read WMI data on a remote server, you must enable the connections between your QRadar console and the server that you are monitoring. If the server is using a Windows firewall, then you must configure the system to enable remote WMI requests.

If the account that you are using to monitor the Windows server is not an administrator, then you must enable the non-administrator to interact with Distributed Component Object Model (DCOM).

Configuring an authenticated scan of the Linux or UNIX operating systems

In IBM Security QRadar Vulnerability Manager, you can configure an authentication scan of the Linux or UNIX operating systems that are on your network.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, select **Actions** > **Create**.

4. In the Scan Profile Details pane, type a name for your scan profile in the **Profile Name** field.

   Restriction: The profile name must be greater than 4 characters.
5. Click the **When To Scan** pane.
6. In the **Run Schedule** list, select **Manual**.
7. Click the **What To Scan** pane.
8. In the **Include Network Nodes** pane, type an IP range in the field and click **Add**.
9. Click the **Scan Setup** pane.
10. In the **Linux/Unix Patch Scanning** pane, type the **Username** and **Password** for the Linux or UNIX hosts that you want to scan.

    Restriction: The user name and password must be valid and you must have the appropriate asset permissions.
11. Click **Save**.
12. Optional: In the Scan Profiles page, on the toolbar select **Actions** > **Run Now**.

Configuring a scan of the Windows operating system

In IBM Security QRadar Vulnerability Manager, you can configure a scan of the Windows operating systems that are installed on your network.

If scanning is performed without administrative privileges, then QRadar Vulnerability Manager scans the remote registry for each installation on the Windows operating system.

Scanning without administrative privileges is incomplete, prone to false positives, and does not cover many third-party applications.

Before you begin

QRadar Vulnerability Manager uses standard Windows operating system remote access protocols that are enabled by default in most windows deployments.

If your Windows scan results return a local checks error vulnerability, that indicates Windows management interface (WMI) connectivity issues, then you must configure your Windows systems.

For more information about Windows connectivity, see:
- "Enabling remote registry access to assets on the Windows operating system" on page 29.
- "Enabling the Windows management interface" on page 29.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, select **Actions** > **Create**.
4. In the Scan Profile Details pane, type a name for your scan profile in the **Profile Name** field.

   Restriction: The profile name must be greater than 4 characters.
5. Click the **When To Scan** pane.

6. In the **Run Schedule** list, select **Manual**.
7. Click the **What To Scan** pane.
8. In the **Include Network Nodes** pane, type an IP range in the field and click **Add**.
9. Click the **Scan Setup** pane.
10. In the **Windows Patch Scanning** pane, type the **Domain**, **Username**, and **Password** for the Windows hosts that you want to scan.
11. Click **Add**.
12. Click **Save**.
13. Optional: In the Scan Profiles page, on the toolbar select **Actions** > **Run Now**.

Enabling remote registry access to assets on the Windows operating system

To scan Windows-based systems, you must configure your registry.

Procedure

1. Log in to your Windows-based system.
2. Click **Start**.
3. In the **Search programs and files** field, type **services** and press Enter.
4. In the Services window, locate the **Remote Registry** service.
5. Right-click the **Remote Registry** service and click **Start**.
6. Close the Services window.

Enabling the Windows management interface

To enable patch scanning, you must enable your Windows management interface (WMI).

Before you begin

Ensure that remote registry access is enabled.

Procedure

1. Log in to your Windows-based system.
2. Click **Start**.
3. In the **Search programs and files** field, type **computer management** and press Enter.
4. Expand the **Services and Applications** navigation menu.
5. In the navigation pane, right-click **WMI Control** and click **Properties**.
6. Click the **Security** tab.
7. Click **Security**.
8. Optional: To add a monitoring user or group:
   a. Click **Add**.
   b. In the **Enter the object names to select** field, type the name of your group or user name.
   c. Click **OK**.
9. If you experience WMI issues, you can install the WMI Administrative tools from the Microsoft website.

The tools include a WMI browser that helps you connect to a remote machine and browse through the WMI information. These tools help you to isolate any connectivity issues in a more direct and simpler environment.

Configuring a permitted scan interval

In IBM Security QRadar Vulnerability Manager, you can create an operational window to specify the times that a scan can run.

If you assign two operational windows to a scan profile, the scan profile executes at the time intersection of the operational windows. If the operational windows are not configured with an overlapping time schedule, then the scans do not run.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Operational Window**.
3. On the toolbar, select **Actions** > **Add**.
4. Choose an operational window schedule from the **Schedule** list.
5. Optional: Select the times when scanning is permitted.
6. Optional: Select your timezone.
7. Optional: If you selected **Weekly** from the **Schedule** list, then click the days of the week in the **Weekly** pane.
8. Optional: If you selected **Monthly** from the **Schedule** list, then select a day from the **Day of the month** list.
9. Click **Save**.

Scanning during permitted times

In IBM Security QRadar Vulnerability Manager, you can schedule a scan of your network assets at permitted times, by using an operational window.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Operational Window**.
3. On the toolbar, select **Actions** > **Add**.
4. Type a name for your operational window, then configure a permitted time interval and click **Save**.
5. In the navigation pane, select **Administrative** > **Scan Profiles**.
6. On the toolbar, select **Actions** > **Create**.
7. In the Scan Profile Details pane, type a name for your scan profile in the **Profile Name** field.

   Restriction: The profile name must be greater than 4 characters.
8. Click the **When To Scan** pane.
9. In the **Run Schedule** list, select **Daily**.
10. In the **Start Time** fields, type or select the date and time that you want your scan to run each day.
11. In the **Operational Windows** pane, select your operational window from the list and click **Add**.
12. Click the **What To Scan** pane.

13. In the **Include Network Nodes** pane, type an **IP range** in the field and click **Add**.
14. Click **Save**.

Managing operational windows

In IBM Security QRadar Vulnerability Manager, you can edit, delete, and print operational windows.

Remember: You can edit an operational window while it is associated with a scan profile.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Operational Window**.
3. Select the operational window that you want to edit.
4. On the toolbar, select an option from the **Actions** menu.
5. Follow the instructions in the user interface.

   Restriction: You cannot delete an operational window that is associated with a scan profile. You must first disconnect the operational window from the scan profile.

Related tasks:

"Disconnecting an operational window"
If you want to delete an operational window that is associated with a scan profile, you must disconnect the operational window from the scan profile.

Disconnecting an operational window

If you want to delete an operational window that is associated with a scan profile, you must disconnect the operational window from the scan profile.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. Select the scan profile that you want to edit.
4. On the toolbar, select **Actions** > **Edit**.
5. Click the **When To Scan** pane.
6. In the **Operational Windows** pane, click the operational window that you want to disconnect.
7. Click **Remove Selected**.
8. Click **Save**.

Network scanning options

You can customize how your network assets are scanned for vulnerabilities by configuring multiple scan profiles.

A scan profile provides numerous configuration options. The options that you choose depend on the vulnerability data that you want to display and the configuration of your network assets.

Configuring a basic asset scan

In IBM Security QRadar Vulnerability Manager, you can configure a basic scan profile that can be run manually.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the toolbar, select **Actions** > **Create**.
4. In the Scan Profile Details expandable pane, type a name for your Scan Profile in the **Profile Name** field.

   Restriction: The profile name must be greater than four characters.
5. Click the **What To Scan** expandable pane.
6. In the **CIDR Range/IP/IP Range** field, type the IP address of the asset that you want to scan.
7. Click **Save**.

Running a scan profile manually

In IBM Security QRadar Vulnerability Manager you can run a scan profile manually.

Scans can also be scheduled to run at a future time and date.

Before you begin

Ensure that a vulnerability processor is deployed.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Administrative** > **Scan Profiles**.
3. On the Scan Profiles page, click the scan profile that you want to run.
4. On the toolbar, select **Actions** > **Run Now**.

   By default, scans complete a fast scan by using the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocol. A fast scan includes most ports in the range 1 - 1024.

   During and after the scan, you can complete the following tasks:
   - Monitor the progress of your scan.
   - Review the results of the completed scan.

Related tasks:

"Monitoring scans in progress" on page 20
In IBM Security QRadar Vulnerability Manager, you can monitor the progress of a scan that is running. You can also monitor the status of the scanning tools that are either queued or running.

Rescanning an asset by using the right-click function

In IBM Security QRadar Vulnerability Manager you can quickly rescan an asset by using the right-click option.

Fast path: By using the right-click scan you can avoid using the Scan Profiles page.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities** > **By Asset**.
3. On the By Asset page, identify the asset that you want to rescan.
4. Right-click the **IP Address** and select **Run QVM Scan**.
5. In the Run QVM Scan window, select the scan profile that you want use when the asset is rescanned.

   The scanning process requires a scan profile. The scan profile determines the scanning configuration options that are used when the scan runs.

   Important: The scan profile that you select might be associated with multiple scan targets or IP address ranges. However, when you use the right-click option, only the asset that you select is scanned.
6. Click **Scan Now**.
7. Click **Close Window**.

   You can review the progress of your right-click scan. In the navigation pane, click **Scan Results**.

   Right-click scans are identified with the prefix **RC:**.

Chapter 5. Vulnerability scan investigations

In IBM Security QRadar Vulnerability Manager, the Scan Results page provides summary asset and vulnerability data at a scan level. It shows the results of completed scan profiles and can also be used to monitor the progress of a scan that is running.

The Manage Vulnerabilities section provides a network view of your current vulnerability posture. Use the Manage Vulnerabilities pages to do the following tasks:

- Build and save complex vulnerability search criteria.
- Investigate exploitation risk levels at a network, asset, and vulnerability level.
- Prioritize your vulnerability remediation processes.

Scan results

You can use the Scan Results page to investigate the following information:

- The status of a scan. For example, a scan with a status of **Completed** indicates that the scan completed successfully or was canceled.
- The degree of risk that is associated with each completed scan profile. Risk is indicated by the **Score** column and shows the total Common Vulnerability Scoring System (CVSS) score for the completed scan profile.
- The total number of assets that were configured for scanning in the scan profile.
- The total number of vulnerabilities that were discovered by the completed scan profile.
- The total number of open services that were discovered by the completed scan profile.
- While a scan is in progress, you can monitor the progress of a scan and investigate scanning tools that are queued and running.

Vulnerability counts

The Scan Results page shows **Vulnerabilities** and **Vulnerabilities Instances**. You must understand the difference.

- The **Vulnerabilities** column shows the total number of unique vulnerabilities that were discovered on all the scanned assets.
- When you scan multiple assets, the same vulnerability might be present on different assets. Therefore, the **Vulnerability Instances** column shows the total number of vulnerabilities that were discovered on all the scanned assets.

Searching scan results

In IBM Security QRadar Vulnerability Manager, you can search and filter your scan results.

For example, you might want to identify recent scans, scans on a specific IP address, or scans that identified a specific vulnerability.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.
3. On the toolbar, select **Search** > **New Search**.

   To search your scan results, there are no mandatory fields. All parameters are optional.
4. Optional: To show scan results for scans that completed within a recent number of days, type a value in the **Scan Run in the last days** field.
5. Optional: To show scan results for a specific vulnerability, click **Browse** in the **Contains Vulnerability** field.
6. Optional: To show scan results for scans that were only scheduled, click **Exclude on demand scan**.
7. Click **Search**.

Results

Related concepts:

"Scan scheduling" on page 21
In IBM Security QRadar Vulnerability Manager, you can schedule the dates and times that it is convenient to scan your network assets for known vulnerabilities.

Managing scan results

In IBM Security QRadar Vulnerability Manager, on the Scan Results page, you can manage your scan results and manage the scans that are running.

Depending on whether a scan is complete or running, the options that you can select from the **Actions** menu are different.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.
3. Optional: If you want to rerun a completed scan, select **Actions** > **Run Now**.

   A completed scan has a status of **Stopped**.
4. Optional: To delete a set of completed scan results:
   a. On the Scan Results page, select a set of completed scan results.
   b. On the toolbar, select **Actions** > **Delete**.

      Important: If you delete a set of scan results, no warning is displayed. The scan results are immediately deleted.

      When you delete a set of scan results, the associated scan profile is not deleted.
5. Optional: To cancel a scan that is running:
   a. On the Scan Results page, select a scan that is running.
   b. On the toolbar, select **Actions** > **Cancel**.

      You can cancel a scan that has a status of **Running** or **Paused**. After you cancel a scan, the status of the scan is **Stopped**.

Asset risk levels and vulnerability categories

In IBM Security QRadar Vulnerability Manager, you can investigate the exploitation risk level of your scanned assets on the Scan Results Hosts page.

The Scan Results Hosts page provides a risk and vulnerability summary for each of the assets that you scanned by running a scan profile.

Security administrators can investigate the following asset risk information:

Risk score

Each vulnerability that is detected on your network has a risk score that is calculated by using the Common Vulnerability Scoring System (CVSS) base score. A high risk score provides an indication of the potential for a vulnerability exploitation.

On the Scan Results Hosts page the **Score** column is an accumulation of the risk score for each vulnerability on an asset. The accumulated value provides an indication of the level of risk that is associated with each asset.

To quickly identify the assets that are most at risk to vulnerability exploitation, click the **Score** column heading to order your assets according to the risk level.

Vulnerability counts and categories

The Scan Results Hosts page shows the total number of vulnerabilities and open services that were discovered on every scanned asset.

To identify the assets with the highest number of vulnerabilities, click the **Vulnerability Instances** column heading to order your assets.

The **High**, **Medium**, **Low**, and **Warning** columns group all vulnerabilities according to their risk.

Asset, vulnerability, and open services data

In IBM Security QRadar Vulnerability Manager, the Hosts Details page shows asset, vulnerability, and open services data.

By using the options on the toolbar, you can switch between viewing vulnerabilities and open services.

The Host Details page provides the following information:

- Summary information about the asset that you scanned, including the operating system and network group.
- A list of the vulnerabilities or open services that were discovered on the scanned asset.
- Various ways of categorizing and ordering your list of vulnerabilities or open services for example, **Risk**, **Severity**, and **Score**.
- A quick way to view open service or vulnerability information. On the toolbar, click **Vulnerabilities** or **Open Services**.
- An easy way to view detailed information about the asset that you scanned. On the toolbar, click the **Host Details**.

- An alternative method of creating a vulnerability exception. On the toolbar, click **Actions** > **Exception**.

For more information about the Asset Details window, see the *Users Guide* for your product.

Related concepts:

Chapter 7, “Vulnerability exception rules,” on page 51
In IBM Security QRadar Vulnerability Manager, you can configure exception rules to minimize the number of false positive vulnerabilities.

Vulnerability risk and PCI severity

In IBM Security QRadar Vulnerability Manager, you can review the risk and payment card industry (PCI) severity for each vulnerability that is found by a scan.

You can review the following information:

- The risk level that is associated with each vulnerability.
- The number of assets in your network on which the specific vulnerability was found.

To investigate a vulnerability, you can click a vulnerability link in the **Vulnerability** column.

Chapter 6. Management of your vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can manage, search, and filter your vulnerability data to help you focus on the vulnerabilities that pose the greatest risk to your organization.

The vulnerability data that is displayed is based on the vulnerability status information that is maintained in the QRadar asset model. This information includes vulnerabilities that are found by the QRadar Vulnerability Manager scanner and the vulnerabilities that are imported from external scanning products.

Manage your vulnerabilities to provide the following information:

- A network view of your current vulnerability posture.
- Identify vulnerabilities that pose the greatest risk to your organization and assign vulnerabilities to QRadar users for remediation.
- Establish how widely your network is impacted by vulnerabilities and display detailed information about the network assets that contain vulnerabilities.
- Decide which vulnerabilities pose less risk to your organization and create vulnerability exceptions.
- Display historical information about the vulnerabilities on your network.
- Display vulnerability data by network, asset, vulnerability, open service, or vulnerability instance.

Investigating vulnerability risk scores

In IBM Security QRadar Vulnerability Manager, you can investigate vulnerability risk scores and understand how each score is calculated.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. Optional: Click the **Risk Score** column to sort your vulnerabilities by risk.
4. To investigate the risk score, hover you mouse on a vulnerability risk score.

Risk score details

In IBM Security QRadar Vulnerability Manager, vulnerability risk scores provide an indication of the risk that a vulnerability poses to your organization.

Using IBM Security QRadar Risk Manager, you can configure policies that adjust vulnerability risk scores and draw attention to important remediation tasks.

Risk Score

The **Risk Score** provides specific network context by using the Common Vulnerability Scoring System (CVSS) base, temporal, and environmental metrics.

When QRadar Risk Manager is not licensed the **Risk Score** column shows the CVSS environmental metric score with a maximum value of 10.

Exploitability subscore

Exploitability is calculated as a subset of the CVSS base score by using the following elements:

- Access Vector provides an indication of risk that is based on the remoteness for example, local, adjacent network, or network, of an attacker.
- Access Complexity provides an indication of risk that is based on attack complexity. The lower the complexity the higher the risk.
- Authentication provides an indication of risk that is based on authentication attempts. The fewer the attempts the higher the risk.

Risk adjustments

If IBM Security QRadar Risk Manager is installed and you configured vulnerability risk policies, then the risk adjustments are listed. The adjustments either increase or decrease the overall risk that is associated with a vulnerability.

Related concepts:

"IBM Security QRadar Risk Manager and IBM Security QRadar Vulnerability Manager integration" on page 15
IBM Security QRadar Vulnerability Manager integrates with QRadar Risk Manager to help you prioritize the risks and vulnerabilities in your network.

Related tasks:

"Prioritizing high risk vulnerabilities by applying risk policies" on page 46
In IBM Security QRadar Vulnerability Manager, you can alert administrators to higher risk vulnerabilities by applying risk policies to your vulnerabilities.

Searching vulnerability data

In IBM Security QRadar Vulnerability Manager, you can identify important vulnerabilities by searching your vulnerability data.

QRadar Vulnerability Manager provides various methods to search your data. You can search by network, by asset, by open service, or by vulnerability.

Default saved searches provide a fast method of identifying the risk to your organization. Saved searches are displayed in the **Available Saved Searches** field on the Vulnerability Manager Search page.

Before you begin

You must create a scan profile and scan your network assets before you search your vulnerability data.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search**.
4. If you want to load a saved search, do the following steps:
   a. Optional: Select a group from the **Group** list.
   b. Optional: In the **Type Saved Search** field, type the saved search that you want to load.

   c. From the **Available Saved Searches** list, select a saved search, and then click **Load**.
   d. Click **Search**.
5. If you want to create a new search, do the following steps in the Search Parameters pane:
   a. In the **first list**, select the parameter that you want to use.
   b. In the **second list**, select a search modifier. The modifiers that are available depend on the search parameter that you select.
   c. In the **third list**, type or select the specific information that is related to your search parameter.
   d. Click **Add Filter**.
6. Click **Search**.

Related concepts:

"Vulnerability search parameters" on page 43
In IBM Security QRadar Vulnerability Manager, you can search your vulnerability data and save the searches for later use.

Saving your vulnerability search criteria

In IBM Security QRadar Vulnerability Manager, you can save your vulnerability search criteria for future use.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search** and complete the search of your data.
4. On the toolbar, click **Save Search Criteria**.
5. In the Save Search Criteria window, type a recognizable name for your saved search.
6. Optional: To include your saved search in the **Quick Searches** list on the toolbar, then click **Include in my Quick Searches**.
7. Optional: To share your saved search criteria with all QRadar users, then click **Share with Everyone**.
8. Optional: To place your saved search is a group, then click a group or click **Manage Groups** to create a new group.

   For more information about managing search groups, see the *Administration Guide* for your product.
9. Optional: If you want to show the results of your saved search when you click any of the Manage Vulnerabilities pages in the navigation pane, then click **Set As Default**.
10. Click **OK**.

Deleting saved vulnerability search criteria

In IBM Security QRadar Vulnerability Manager, you can delete your saved vulnerability search criteria.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities** > **By Network**
3. On the toolbar, select **Search** > **New Search**.
4. On the Vulnerability Manager Search page, in the **Available Saved Searches** list, select the saved search that you want to delete.
5. Click **Delete**.
6. Click **OK**.

Vulnerability instances

In IBM Security QRadar Vulnerability Manager, you can display each vulnerability on every asset in your network.

If you configure third-party vulnerability assessment (VA) scanners, by using the QRadar **Admin** tab, then the vulnerabilities that are detected are automatically displayed in the By Vulnerability Instances page.

For more information about VA scanners, see the *Administration Guide* for your product.

The By Vulnerability Instances page provides the following information:

- A view of every vulnerability that was been detected by scanning your network assets.
- The risk that each vulnerability poses to the Payment Card Industry (PCI).
- The risk that a vulnerability poses to your organization. Click the **Risk Score** column to identify the highest risk vulnerabilities.
- The name of the QRadar user that is assigned to remediate the vulnerability.
- The numbers of days in which a vulnerability must be remediated.

Related concepts:

"Risk score details" on page 39
In IBM Security QRadar Vulnerability Manager, vulnerability risk scores provide an indication of the risk that a vulnerability poses to your organization.

Network vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can display vulnerability data that is grouped at a network level.

The By Network page provides a summary of all your vulnerability data that is grouped at a network level.

The **Risk Score** provides an accumulated network risk score for every vulnerability on your network.

Asset vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can display summary vulnerability data that is grouped at an asset level.

You can use the By Asset page to prioritize the assets in your organization that pose the greatest risk. Click the **Risk Score** column to order your assets by their risk.

The **Risk Score** provides an accumulated asset risk score for all the vulnerabilities on each asset.

Open service vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can display vulnerability data that is grouped by open service.

The By Open Service page provides a summary of all your vulnerability data that is grouped by open service.

Vulnerability search parameters

In IBM Security QRadar Vulnerability Manager, you can search your vulnerability data and save the searches for later use.

The following table is not a complete list of vulnerability search parameters, but a subset of the available options.

Select any of the parameters to search and display vulnerability data.

Table 4. Vulnerability search parameters

Option	Description
Access Complexity	The complexity of the attack that is required to exploit a vulnerability.
Access Vector	The network location from where a vulnerability can be exploited.
Asset saved search	The host, IP address, or range of IP addresses associated with a saved asset search. For more information about saving asset searches, see the *Users Guide* for your product.
Assets with open service	Assets that have specific open services. For example, http, FTP, and smtp.
Authentication	The number of times an attacker must authenticate against a target to exploit a vulnerability.
Availability Impact	The level that resource availability can be compromised if a vulnerability is exploited.
Confidentiality Impact	The level of confidential information that can be obtained if a vulnerability is exploited.
Days since asset found	The elapsed number of days since the asset with the vulnerability was discovered on your network. Assets can be discovered either by an active scan or passively by using log or flow analysis.

Table 4. Vulnerability search parameters (continued)

Option	Description
Days since associated vulnerability service traffic	Displays vulnerabilities on assets with associated layer 7 traffic to or from an asset, based on the elapsed number of days since the traffic was detected.
Days since vulnerabilities discovered	The elapsed number of days since the vulnerabilities were first discovered on your network assets.
External Reference of type	Vulnerabilities that have an associated Endpoint Manager fixlet. By using this parameter you can show only those vulnerabilities without an available patch.
Impact	The potential impact to your organization. For example, access control loss, downtime, and reputation loss.
Include early warnings	Newly published vulnerabilities that are detected on your network without performing additional scanning.
Include vulnerability exceptions	Those vulnerabilities with an exception rule applied.
Integrity Impact	The level to which system integrity might be compromised if a vulnerability is exploited.
Only include assets with risk	Vulnerabilities that pass or fail specific risk policies that are defined and monitored in IBM Security QRadar Risk Manager.
Vulnerability external reference	Vulnerabilities that are based on an imported list of vulnerability IDs, for example CVE ID. For more information about Reference Sets, see the *Administration Guide* for your product.
Vulnerability has a virtual patch from vendor	Vulnerabilities that can be patched by an intrusion prevention system.
Vulnerability reference	Vulnerabilities that are based on external vulnerability reference information.
Vulnerability state	The status of the vulnerability since the last scan of your network or specific network assets. For example, when you scan assets, the vulnerabilities that are discovered are either New, Pre-existing, Fixed, or Existing.
Quick Search	You can search for a vulnerabilities title, description, solution, and external reference ID. In the **Quick Search** field, you can use and, or, and not operators, and brackets.

Investigating the history of a vulnerability

In IBM Security QRadar Vulnerability Manager, you can display useful information about the history of a vulnerability.

For example, you can investigate information about how the risk score of a vulnerability was calculated. You can also review information about when a vulnerability was first discovered and the scan that was used to discover the vulnerability.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. Optional: Search your vulnerability data.
4. Click the vulnerability that you want to investigate.
5. On the toolbar, select **Actions** > **History**.

Related tasks:

"Searching vulnerability data" on page 40
In IBM Security QRadar Vulnerability Manager, you can identify important vulnerabilities by searching your vulnerability data.

Reducing the number of false positive vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can automatically create exception rules for vulnerabilities that are associated with a specific type of server.

When you configure server types, QRadar Vulnerability Manager creates exception rules and automatically reduces the vulnerabilities that are returned by searching your data.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, select **Server Discovery**.
3. To automatically create false positive exception rules for vulnerabilities on specific server types, from the **Server Type** list, select one of the following options:
   - FTP Servers
   - DNS Servers
   - Mail Servers
   - Web Servers

   It might take a few minutes for the **Ports** field to refresh.
4. Optional: From the **Network** list, select the network for your servers.
5. Click **Discover Servers**.
6. In the Matching Servers pane, select the servers where the vulnerability exception rules are created.
7. Click **Approve Selected Servers**.

Results

Depending on your server type selection the following vulnerabilities are automatically set as false positive exception rules:

Table 5. Server type vulnerabilities

Server Type	**Vulnerability**
FTP Servers	**FTP Server Present**

Table 5. Server type vulnerabilities (continued)

Server Type	Vulnerability
DNS Servers	**DNS Server is Running**
Mail Servers	**SMTP Server Detected**
Web Servers	**Web Service is Running**

Investigating high risk assets and vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can investigate high risk vulnerabilities that might be more susceptible to exploitation.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the By Vulnerability Instances page, click the **Risk Score** column heading to sort the vulnerabilities by risk score.
4. Optional: Hover your mouse on the **Risk Score** field to investigate the CVSS metrics that are used to derive the risk score.
5. Identify the vulnerability that has the highest score and click the **Vulnerability** link.
6. In the Vulnerability Details window, you can do the following to investigate the vulnerability:
   a. Optional: Click the **X-Force** link to view the IBM Security Systems website.
   b. Optional: Click the **CVE** link to view the National Vulnerability Database website.

      The IBM Security Systems website and National Vulnerability Database provide remediation information and details on how a vulnerability might impact your organization.
   c. Optional: In the **Solution** text box, you can review detailed information about how to remediate a vulnerability.

Related concepts:

"Risk score details" on page 39
In IBM Security QRadar Vulnerability Manager, vulnerability risk scores provide an indication of the risk that a vulnerability poses to your organization.

Prioritizing high risk vulnerabilities by applying risk policies

In IBM Security QRadar Vulnerability Manager, you can alert administrators to higher risk vulnerabilities by applying risk policies to your vulnerabilities.

When you apply a risk policy, the risk score of a vulnerability is adjusted, allowing administrators to prioritize more accurately the vulnerabilities that require immediate attention.

In this example, the vulnerability risk score is automatically increased by a percentage factor for any vulnerability that remains active on your network after 40 days.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar click **Search** > **New Search**.
4. In the Search Parameters pane, configure the following filters:
   a. **Risk Equals High**
   b. **Days since vulnerabilities discovered Greater than or equal to 40**
5. Click **Search** and then on the toolbar click **Save Search Criteria**.

   Type a saved search name that is identifiable in QRadar Risk Manager.
6. Click the **Risks** tab.
7. In the navigation pane, click **Policy Monitor**.
8. On the toolbar click **Actions** > **New**.
9. In the **What do you want to name this question** field, type a name.
10. In the **Which tests do you want to include in your question** field, click **are susceptible to vulnerabilities contained in vulnerability saved searches**.
11. In the **Find Assets that** field, click the underlined parameter on the **are susceptible to vulnerabilities contained in vulnerability saved searches**.
12. Identify your QRadar Vulnerability Manager high risk vulnerability saved search, click **Add**, then click **OK**.
13. Click **Save Question**.
14. In the Questions pane, select your question from the list and on the toolbar click **Monitor**.

    Restriction: The **Event Description** field is mandatory.
15. Click **Dispatch question passed events**.
16. In the **Vulnerability Score Adjustments** field, type a risk adjustment percentage value in the **Percentage vulnerability score adjustment on question fail** field.
17. Click **Apply adjustment to all vulnerabilities on an asset** then click **Save Monitor**.

What to do next

On the **Vulnerabilities** tab, you can search your high risk vulnerabilities and prioritize your vulnerabilities

Related concepts:

"IBM Security QRadar Risk Manager and IBM Security QRadar Vulnerability Manager integration" on page 15
IBM Security QRadar Vulnerability Manager integrates with QRadar Risk Manager to help you prioritize the risks and vulnerabilities in your network.

Related tasks:

"Saving your vulnerability search criteria" on page 41
In IBM Security QRadar Vulnerability Manager, you can save your vulnerability search criteria for future use.

Identifying vulnerabilities with an IBM Endpoint Manager patch

In IBM Security QRadar Vulnerability Manager, you can identify the vulnerabilities that have an available fix.

After you identify your vulnerabilities that have an available fix, you can investigate detailed fix information in the Vulnerability Details window.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search**
4. In the Search Parameters pane configure the following options:
   a. In the **first list** select **External Reference of type**.
   b. In the **second list** select **Equals**.
   c. In the **third list** select **IBM Endpoint Manager Patch**.
   d. Click **Add Filter**.
   e. Click **Search**.

      The By Vulnerability Instances page shows the vulnerabilities that have an available fix.
5. Optional: Order your vulnerabilities according to their importance by clicking the **Risk Score** column heading.
6. Optional: To investigate patch information for a vulnerability, click a vulnerability link in the **Vulnerability** column.
7. Optional: In the Vulnerability Details window, scroll to the bottom of the window to view the vulnerability patch information.

   The **Site ID** and **Fixlet ID** are unique identifiers that you use to apply vulnerability patches by using IBM Endpoint Manager.

   The **Base** column indicates a unique reference that you can use to access more information on a knowledge base.

Identifying the patch status of your vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can identify the patch status of your vulnerabilities.

By filtering patched vulnerabilities, you can prioritize your remediation efforts on the most critical vulnerabilities in your organization.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, select **Search** > **New Search**.
4. In the **first list** in the Search Parameters pane, select **Patch Status**.
5. In the **second list**, select a search modifier.
6. To filter your vulnerabilities according to their patch status, select one of the following options from the third list:

Option	Description
Pending Downloads	Select this option to show vulnerabilities that are scheduled to be patched
Pending Restart	Select this option to shows vulnerabilities that are patched after the scanned asset is restarted

Option	Description
Fixed	Select this option to show vulnerabilities that are patched by IBM Endpoint Manager

7. Click **Add Filter**.
8. Click **Search**.

Related concepts:

"IBM Endpoint Manager integration" on page 15
IBM Security QRadar Vulnerability Manager integrates with IBM Endpoint Manager to help you filter and prioritize the vulnerabilities that can be fixed.

Chapter 7. Vulnerability exception rules

In IBM Security QRadar Vulnerability Manager, you can configure exception rules to minimize the number of false positive vulnerabilities.

When you apply exception rules to vulnerabilities, you reduce the number of vulnerabilities that are displayed when you search your data.

If you create a vulnerability exception, the vulnerability is not removed from QRadar Vulnerability Manager.

Viewing exception rules

To display vulnerability exceptions, you can search your vulnerability data by using the appropriate search filters.

To view exception rules, click the **Vulnerabilities** tab, then click **Vulnerability Exception** in the navigation pane.

Related tasks:

"Reducing the number of false positive vulnerabilities" on page 45
In IBM Security QRadar Vulnerability Manager, you can automatically create exception rules for vulnerabilities that are associated with a specific type of server.

Applying a vulnerability exception rule

In IBM Security QRadar Vulnerability Manager, you can manually apply a vulnerability exception rule to a vulnerability that you decide does not pose a significant threat.

If you apply an exception rule, the vulnerability is no longer displayed in QRadar Vulnerability Manager search results. However, the vulnerability is not removed from QRadar Vulnerability Manager.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities** > **By Network**.
3. Optional: Search your vulnerability data. On the toolbar, click **Search** > **New Search**.
4. Click the **Vulnerability Instances** column link.
5. Select the vulnerability that you want to create an exception rule for.
6. On the toolbar, select **Actions** > **Exception**.
7. In the Notes section of the Maintain Exception Rule window, enter text in the **Comments** text box.

   To apply a vulnerability exception rule, the only mandatory field is the **Comment** text box. All other parameters are optional.
8. Optional: If you want to set an expiry date, ensure that the **Never Expires** check box is not selected.

   If you do not set an expiry date, the system automatically defaults to never expire.

9. Click **Save**.

Related tasks:

"Searching vulnerability data" on page 40
In IBM Security QRadar Vulnerability Manager, you can identify important vulnerabilities by searching your vulnerability data.

Managing a vulnerability exception rule

If you receive new information about a vulnerability, you can update or remove an existing vulnerability exception rule.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Vulnerability Exception**.
3. Click the vulnerability that you want to manage.
4. On the toolbar, select an option from the **Actions** menu.

   Important: If you delete a vulnerability exception rule, no warning is displayed. The vulnerability is immediately deleted.
5. Click **Save**.

Searching vulnerability exceptions

In IBM Security QRadar Vulnerability Manager, you can search your vulnerability data and filter the search results to display vulnerability exceptions.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities** > **By Asset**.
3. On the toolbar, select **Search** > **New Search**.
4. To filter your vulnerability data to include vulnerability exceptions, from the Search Parameters pane, select one of the following options:
   - Include vulnerability exceptions

     Displays all vulnerabilities, including vulnerabilities with an exception rule applied to them.
   - Only include vulnerability exceptions

     Displays vulnerabilities only with an exception rule applied to them.
5. Click **Add Filter**.
6. Click **Search**.

Chapter 8. Vulnerability remediation

Vulnerabilities can be manually or automatically assigned to QRadar users for remediation.

You can track the remediation process by reviewing information about the users who are assigned to remediate vulnerabilities and the dates when vulnerabilities must be remediated.

Manually assigning vulnerabilities to users for remediation

In IBM Security QRadar Vulnerability Manager, you can manually assign vulnerabilities to a QRadar user for remediation.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Manage Vulnerabilities**.
3. Optional: Search your vulnerability data.
4. Select the vulnerability that you want to assign for remediation.
5. On the toolbar, click **Actions** > **Assign/Edit**.

   None of the fields on the Assign/Edit Vulnerability window are mandatory.
6. Optional: Select an alternative user from the **Assigned User** list.

   The default assigned user is **Admin**.
7. Optional: In the **Due Date** list, select a future date when the vulnerability must be remediated.

   If you do not select a date, the **Due Data** is set as the current date.
8. Optional: In the Notes pane, type useful information about the reason for the vulnerability assignment.
9. Click **Save**.

Configuring automatic vulnerability assignments

You can configure IBM Security QRadar Vulnerability Manager to automatically assign vulnerabilities to a QRadar user for remediation.

Automatic remediation is configured on the assets in your network. After you configure the asset, all the vulnerabilities that are associated to an asset are automatically assigned for remediation.

Before you begin

Ensure that the users responsible for remediation vulnerabilities exist in QRadar.

For more information about managing users and roles, see the *Administration Guide* for your product.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**.

3. Select the asset that you want to configure.
4. On the toolbar, click **Edit Asset.**
5. Click the **Owners** pane.
6. In the **Technical User** list, select the user that you want to assign vulnerabilities to.
7. Click **Save**.

Chapter 9. Vulnerability reports

In IBM Security QRadar Vulnerability Manager, you can generate or edit an existing report, or use the report wizard to create, schedule, and distribute a new report.

QRadar Vulnerability Manager contains several default reports.

The report wizard provides a step-by-step guide on how to design, schedule, and generate reports.

For more information, see the *IBM Security QRadar SIEM Users Guide*.

Running a default QRadar Vulnerability Manager report

In IBM Security QRadar Vulnerability Manager, you can run a default vulnerability management report.

Procedure

1. Click the **Reports** tab.
2. From the list of reports, click the report that you want to run.

   For example, you might want to show a report of your vulnerability overview for the last seven days.
3. On the toolbar, select **Actions** > **Run Report**, then click **OK**.
4. To view the completed report in a PDF format, click the icon in the **Formats** column.

Emailing high risk vulnerability reports

In IBM Security QRadar Vulnerability Manager, you can send a vulnerability report to the technical contact for each asset.

Emailed reports help to remind your technical administrators that high risk vulnerabilities remain present on their assets. Reports can be scheduled weekly, or monthly.

Procedure

1. Configure the contact details for each asset that you want to report on.
2. Create a contact saved vulnerability search.
3. Create and schedule a vulnerability report for each asset.

Configuring the contact details for an asset

In IBM Security QRadar Vulnerability Manager, if you want to email vulnerability reports, you must configure the technical contact details for the asset that contains the vulnerabilities.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**.

3. On the Assets page, select the asset that you want to assign a technical owner contact.
4. On the toolbar, click **Edit Asset**.
5. In the Edit Asset Profile window, click the **Owners** pane.
6. In the **Technical Owner Contact** field, type an email address for the user who is responsible for asset maintenance.
7. Click **Save**.

Creating a contact saved vulnerability search

In IBM Security QRadar Vulnerability Manager, if you want to email vulnerability reports you must create a saved vulnerability search for the technical owner contact.

Procedure

1. Click the **Vulnerability** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, click **Search** > **New Search**.
4. In the **Search Parameters** pane, configure the following search criteria:
   a. **Technical Owner Contact Equals** <email address>.

      Where <email address> is a valid email address for any technical owner contact in your network.

   b. Click **Add Filter**.
   c. Add the **Risk Equals High** filter to your search criteria.
   d. Click **Add Filter**.
   e. Click **Search**.
5. On the toolbar, click **Save Search Criteria**.
6. Type a name for your saved search.

   Important: Save your search with a recognizable name. Your vulnerability report is generated by using the search that you save.
7. Click **Include in my Quick Searches**.
8. Click **OK**.

Creating and scheduling weekly vulnerability reports for each asset

In IBM Security QRadar Vulnerability Manager, you can create and schedule an asset vulnerability report for the technical contact of each asset.

Procedure

1. Click the **Reports** tab.
2. On the toolbar, select **Actions** > **Create**.
3. Click **Weekly** and then click **Next**.
4. Click the undivided report layout that is displayed on the upper left section of the report wizard and click **Next**.
5. Type a **Report Title**.
6. In the **Chart Type** list, select **Asset Vulnerabilities** and type a **Chart Title**.

7. Optional: If a technical contact owner is responsible for more than five assets and you want to email all asset information, increase the value in the **Limit Assets To Top** list.

   Remember: By using the **Assets** tab, you must ensure that the same technical contact owner is assigned to each asset that they are responsible for.
8. In the **Graph Type** field, select **AggregateTable**.

   If you select any value other than **AggregateTable**, the report does not generate a vulnerability subreport.
9. In the Graph Content pane, click **Search to Use** and select your saved technical contact vulnerability search then click **Save Container Details**.
10. Click **Next** and select your report output type.
11. In the report distribution section of the report wizard, click **Multiple Reports**.
12. In the **List** field, type a comma-separated list of email addresses for the technical contact owner of each asset and click **Finish**.
13. On the Reports list, select the report that you created and on the toolbar, select **Actions** > **Run Report**.

Chapter 10. Vulnerability research, news, and advisories

You can use IBM Security QRadar Vulnerability Manager to remain aware of the vulnerability threat level and manage security in your organization.

A vulnerability library contains common vulnerabilities that are gathered from a list of external sources. The most significant external resource is the National Vulnerability Database (NVD). You can research specific vulnerabilities by using a number of criteria for example, vendor, product, and date range. You might be interested in specific vulnerabilities that exist in products or services that you use in your enterprise.

QRadar Vulnerability Manager also provides a list of security-related news articles and advisories, gathered from an external list of resources and vendors. Articles and advisories are a useful source of security information from around the world. Articles also help you to keep up-to-date with current security risks.

Viewing detailed information about published vulnerabilities

In IBM Security QRadar Vulnerability Manager, you can display detailed vulnerability information.

Using the Research Vulnerabilities page, you can investigate CVSS metrics and access information from IBM X-Force® research and development.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, select **Research** > **Vulnerabilities**.
3. Optional: If no vulnerabilities are displayed, select an alternative time range from the **View** list.
4. Optional: To search the vulnerabilities, on the toolbar, select **Search** > **New Search**.
5. Identify the vulnerability that you want to investigate.
6. Click the vulnerability link in the **Vulnerability Name** column.

Remaining aware of global security developments

In IBM Security QRadar Vulnerability Manager, you can view security news from across the world to help you to keep up-to-date with current security developments.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Research** > **News**.
3. Optional: If no news articles are displayed, select an alternative time range from the **View** list.
4. Optional: To search the news articles, on the toolbar, select **Search** > **New Search**.
5. Identify the news article that you want to find out more about.
6. Click the news article link in the **Article Title** column.

Viewing security advisories from vulnerability vendors

In IBM Security QRadar Vulnerability Manager, you can view the vulnerability advisories that are issued by software vendors. Use advisory information to help you identify the risks in your technology, and understand the implications of the risk.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Research** > **Advisories**.
3. Optional: If no advisories are displayed, select an alternative time range from the **View** list.
4. Optional: If you want to search the security advisories, on the toolbar, select **Search** > **New Search**.
5. Click the advisory link in the **Advisory** column.

   Each security advisory might include vulnerability references, solutions, and workarounds.

Searching vulnerabilities, news, and advisories

In IBM Security QRadar Vulnerability Manager, you can search the latest vulnerability news and advisories that are issued by software vendors.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click one of the following options:
   - **Research** > **Vulnerabilities**.
   - **Research** > **News**.
   - **Research** > **Advisories**.
3. On the toolbar, select **Search** > **NewSearch**.
4. Type a search phrase in the **Phrase** field.
5. Optional: If you are searching news items, select a news source from the **Source** list.
6. In the By Date Range pane, specify the date period for the news or advisory that you are interested in.
7. Optional: If you are searching a published vulnerability, specify a vendor in the By Product pane.
8. Optional: If you are searching a published vulnerability, specify a CVE ID in the By ID pane.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

This glossary provides terms and definitions for the IBM Security QRadar Vulnerability Manager software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

"A" "C" "D" "E" "F" "H" "I" on page 66 "N" on page 66 "O" on page 66 "P" on page 66 "R" on page 66 "S" on page 66 "T" on page 66 "U" on page 66 "V" on page 67

A

advisory
A document that contains information and analysis about a threat or vulnerability.

asset A manageable object that is either deployed or intended to be deployed in an operational environment.

C

CDP See collateral damage potential.

CIDR See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client A software program or computer that requests services from a server.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical assest or on an organization.

common vulnerability scoring system (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A web-based interface from which an operator can control and observe the system operation.

CVSS See common vulnerability scoring system.

D

DNS See Domain Name System.

DNS zone transfer
A transaction that replicates a Domain Name System (DNS) database.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

F

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

H

HA See high availability.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

I

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

IP See Internet Protocol.

N

national vulnerability database (NVD)
A United States repository of standards-based vulnerability management data.

NVD See national vulnerability database.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

operational window
A configured time period within which a scan is permitted to run.

P

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

R

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

S

scan exclusion list
A list of assets, network groups, and CIDR ranges that are not ignored by scans.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

T

TCP See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

U

UDP See User Datagram Protocol.

User Datagram Protocol (UDP)
An Internet protocol that provides

unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process.

V

vulnerability
A security exposure in an operating system, system software, or application software component.

Index