IBM Security QRadar Risk Manager
Version 7.1.0 (MR1)

Getting Started Guide

Note: Before using this information and the product that it supports, read the information in “Notices and trademarks”on page 1.

CONTENTS

ABOUT THIS GUIDE

1 INTRODUCTION

2 DEPLOY QRADAR RISK MANAGER

3 COLLECTING NETWORK DATA

4 MANAGING AUDITS WITH QRADAR RISK MANAGER

ABOUT THIS GUIDE

This guide describes typical customer use cases for IBM Security QRadar Risk Manager. The instructions provided will enable you to effectively get started with the features and capabilities of QRadar Risk Manager.

Documentation conventions

The following conventions are used throughout this guide:

▶ Indicates that the procedure contains a single instruction.

NOTE

Indicates that the information provided is supplemental to the associated feature or instruction.

⚠ **CAUTION**

Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.

⚠ **WARNING**

Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.

Audience

This guide assumes that you have QRadar SIEM administrative access permissions and appropriate configuration information for your network devices.

Technical documentation

For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacting customer support

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

1 INTRODUCTION

Welcome to your IBM Security QRadar Risk Manager evaluation.

QRadar Risk Manager is a separately installed risk appliance that integrates with IBM Security QRadar SIEM to provide powerful security analytic, simulation, and visualization tools.

QRadar Risk Manager enhances QRadar SIEM with the following features:

- Centralized risk management
- Topology views of your network
- Configuration monitoring of your network devices
- Connection views between network devices
- Firewall rule searching and rule event counting
- Device and path searching of your network devices
- Monitoring for policy and audit compliance
- Simulations of network changes
- Topology port and vulnerability searching for network devices

Centralized risk management, compliance for increased intelligence of information may involve the cooperation of many internal teams. As a next generation SIEM with an additional Risk Management appliance, we have reduced the number of steps required from first generation SIEM products and provided network topology and risk assessment for assets managed in QRadar SIEM.

After you complete the evaluation process, you will have consolidated all your system, security, risk analysis, and network information through aggregation and correlation, providing complete visibility into your network environment. You will have defined a portal into your environment that provides more visibility and efficiency than you could have achieved through manual processes and other point product technologies.

We hope you enjoy the QRadar Risk Manager solution and the value our Risk Manager appliance and second-generation SIEM technology offers.

Use cases

The following use cases are included to assist with your evaluation:

- Case 1: Centralizing configuration audit
- Case 2: Viewing network paths using topology
- Case 3: Visualize the attack path of a QRadar SIEM offense
- Case 4: Assessing assets with suspicious configurations (PCI Section 1)
- Case 5: Assessing assets with questionable communications (PCI Section 10)
- Case 6: Monitoring for policy violations
- Case 7: Prioritizing asset risk by vulnerability
- Case 8: Prioritizing asset vulnerabilities by zone or network communications
- Case 9: Simulating attacks on network assets
- Case 10: Simulating the risk of network configuration changes

2 DEPLOY QRADAR RISK MANAGER

Before you can get started with IBM Security QRadar Risk Manager, you must first install the QRadar Risk Manager evaluation appliance.

Your QRadar Risk Manager appliance is installed with the latest version of QRadar Risk Manager software. The software requires activation and you must assign an IP address to the QRadar Risk Manager appliance. For assistance activating your software and assigning an IP address, contact your Q1 Labs field engineer.

The appliance is ready to accept information from your network devices. For more information, see *IBM Security QRadar Risk Manager User Guide* on the Qmmunity web site, https://qmmunity.q1labs.com.

About the Installation Process

To deploy QRadar Risk Manager in your environment:

1. Ensure the latest version of QRadar SIEM is installed.
2. Ensure all pre-installation requirements are met. See Before you begin
3. Set-up and power on your QRadar Risk Manager appliance. See Set up a QRadar Risk Manager appliance.
4. Install the QRadar Risk Manager plug-in on your QRadar SIEM Console. See Installing the QRadar Risk Manager plug-in.
5. Establish communications between QRadar SIEM and the QRadar Risk Manager appliance. See Establishing communications.
6. Define user roles for your QRadar Risk Manager users. See Defining user roles.

Before you begin

Before you begin the installation process, you must review the following topics:

- Browser support
- Port requirements
- Unsupported QRadar Risk Manager features

Browser support

QRadar Risk Manager supports the following web browsers:

- **Mozilla Firefox** - We are committed to supporting the Mozilla Firefox web browser. Due to Mozilla's short release cycles, it is no longer feasible to perform exhaustive compatibility testing on each Mozilla Firefox release. We have adopted a best effort strategy to support the Mozilla Firefox browser, in which compatibility issues are aggressively tracked and corrected as they are reported.
- **Internet Explorer 8.0 and 9.0, with Compatibility View enabled** - For instructions on how to enable Compatibility View, see Enabling compatibility view.

Enabling compatibility view

To enable compatibility view for a Microsoft Internet Explorer web browser:

Step 1 Launch your Microsoft Internet Explorer web browser.

Step 2 Press the F12 key to open the Developer Tools window.

Step 3 Configure the following compatibility settings:

Table 4-1 Internet Explorer web browser compatibility settings

Browser Version	Option	Description
Internet Explorer 8.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 8.0**.
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards**.
Internet Explorer 9.0	Browser Mode	From the **Browser Mode** drop-down list box, select **Internet Explorer 9.0**.
	Document Mode	From the **Document Mode** drop-down list box, select **Internet Explorer 7.0 Standards**.

Port requirements

Ensure any firewall located between the QRadar SIEM Console and QRadar Risk Manager allows traffic on the following ports:

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Time)

Unsupported QRadar Risk Manager features

QRadar Risk Manager does not support:

- High Availability (HA)
- Dynamic Routing
  - Border Gateway Protocol (BGP)
  - Open Shortest Path First (OSPF)
  - Routing Information Protocol (RIP)
- IPv6

Set up a QRadar Risk Manager appliance

The QRadar Risk Manager evaluation appliance is a two-unit rack mount server. Rack rails and shelving are not provided with evaluation equipment. Prior to installing the QRadar Risk Manager evaluation appliance, ensure that you have the following:

- space for a two-unit appliance
- rack rails and shelving (mounted)
- USB keyboard and standard VGA monitor for Console access (optional)

The QRadar Risk Manager appliance includes four network interfaces. For this evaluation, use the interface labeled ETH0 as the management interface.

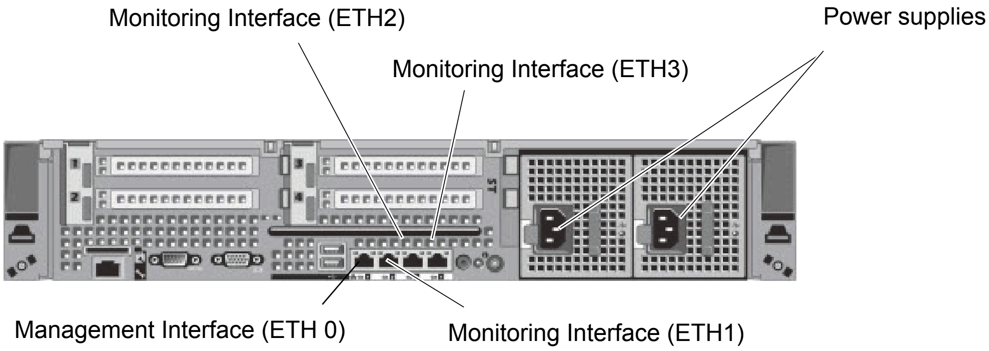
Monitoring Interface (ETH2)
Power supplies
Monitoring Interface (ETH3)
Management Interface (ETH 0)
Monitoring Interface (ETH1)

Figure 4-1 QRadar Risk Manager back pane

NOTE

The graphics in this guide are representations of a QRadar Risk Manager evaluation appliance. Your system may vary, depending on the version of your evaluation appliance.

To install the QRadar Risk Manager appliance:

Step 1 Connect the management network interface to the port labeled ETH0.

Step 2 Ensure that dedicated power connections are plugged into the rear of the appliance.

Step 3 If you want Console access, connect the USB keyboard and standard VGA monitor.

Step 4 If there is a front pane on the appliance, remove the pane by pushing in the tabs on either side and pulling the pane away from the appliance.

Step 5 Power on the appliance.

The power button is located on the front of the appliance.

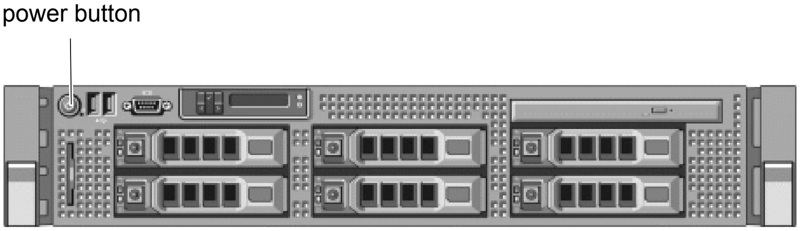

Figure 4-2 QRadar Risk Manager front pane

The appliance begins the boot process. You are now ready to install the QRadar Risk Manager plug-in.

Installing the QRadar Risk Manager plug-in

After you connect and power on your QRadar Risk Manager appliance, you must install the QRadar Risk Manager plug-in on your QRadar SIEM Console. The QRadar Risk Manager plug-in is obtained from the /root folder of the QRadar Risk Manager appliance.

To install the QRadar Risk Manager plug-in:

Step 1 Log in to your QRadar SIEM Console, as root.

Step 2 From your QRadar SIEM Console, type the following command:

```
scp root@<Risk Manager>:/root/risk_manager_for_QRadar*.rpm .
```

Where **`<Risk Manager>`** is the IP address or hostname of QRadar Risk Manager.

The QRadar Risk Manager plug-in is copied to your QRadar SIEM Console:

Step 3 Close all instances of your browser (Mozilla FireFox or Internet Explorer).

CAUTION

The software version of your QRadar SIEM Console must meet the minimum version specified in the QRadar Risk Manager plug-in you are installing. For more information, see the QRadar Risk Manager Release Notes.

Step 4 From your QRadar SIEM Console, type the following command:

```
rpm -Uvh risk_manager_for_QRadar-1.1.0-7.0.0.*.noarch.rpm
```

NOTE

The name of the risk_manager_for_QRadar file includes the version number in the file name. The name of the RPM file is updated with new releases of QRadar Risk Manager.

If your QRadar SIEM Console does not meet the minimum version requirements when the rpm attempts to install, an error message is displayed asking you to update your QRadar SIEM Console.

The QRadar Risk Manager plug-in is installed and the necessary processes are restarted. This process may take an extended period of time.

CAUTION

The rpm installation restarts tomcat on the QRadar SIEM Console. The QRadar SIEM Console interface is momentarily unavailable until installation completes.

You are now ready to establish communications between the QRadar Risk Manager appliance and the QRadar SIEM Console.

Establishing communications

Before you can set-up and configure QRadar Risk Manager, you must establish communications between your QRadar Risk Manager appliance and the QRadar SIEM Console. The following procedure describes the initial handshake between QRadar Risk Manager and QRadar SIEM.

To establish communications:

Step 1 Open your web browser.

Step 2 Clear the cache of your web browser:

NOTE

Before you clear the cache, ensure you have only one instance of your browser open. If you have multiple versions of your browser open, the cache can fail to clear properly.

a If you are using Internet Explorer 8.0, select **Tools > Delete Browsing History > Delete**.

b If you are using Internet Explorer 9.0, click the gear icon in right corner of the browser window, select **Internet Options > General**, and then click **Delete** in the **Browsing History** section.

c If you are using Mozilla Firefox, select **Tools > Options > Advanced > Network > Clear Now**.

NOTE

If you are using Mozilla Firefox, you must clear the cache in Internet Explorer as well as in Mozilla Firefox.

Step 3 Log in to QRadar SIEM:

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

Where **`<IP Address>`** is the IP address of the QRadar SIEM system.

Step 4 Type a username and password to log in to QRadar SIEM.

The default values are:

Username: **`admin`**

Password: **`<root password>`**

Where **`<root password>`** is the password assigned to QRadar SIEM during the QRadar SIEM installation process.

NOTE

If you are using a Mozilla Firefox web browser, the first time you connect to QRadar SIEM you may receive a notice about an untrusted connection. Click **Add Exception...**, then click **Configure Security Exception** to log in to QRadar SIEM. For more information, see your Mozilla documentation.

NOTE

If you are using Internet Explorer, a website security certificate message is displayed. You must select the **Continue to this website option (Not recommended)** to continue.

Step 5 Click **Login To QRadar**.

Step 6 Click the **Risks** tab.

Step 7 Type values for the following parameters:

- **IP/Host** - Type the IP address or hostname of the QRadar Risk Manager appliance.
- **Root Password** - Type the root password of the QRadar Risk Manager appliance.

Step 8 Click **Save**.

The process to establish communications may take several minutes to complete. After the process is complete, the **Risks** tab is available in the QRadar SIEM interface.

If you change the IP address of your QRadar Risk Manager appliance or need to handshake QRadar Risk Manager to another QRadar SIEM Console after communications are established, you can use the **Risk Manager Settings** in the QRadar SIEM **Admin** tab.

Defining user roles

Before you can access QRadar Risk Manager functionality, you must ensure all required users are assigned the appropriate user role permissions. By default, QRadar SIEM provides a default administrative role, which provides access to all areas of QRadar Risk Manager. A user that is assigned administrative privileges (including the default administrative role) cannot edit their own account. Another administrative user must make any required changes.

NOTE

For information about creating and managing user roles, see the *IBM Security QRadar SIEM Administration Guide*.

To assign QRadar Risk Manager user role permissions:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 In the **User Management** pane, click the **User Roles** icon.

Step 4 Click the **Edit** icon next to the user role you want to edit.

Step 5 Select the **Risk Manager** check box.

Step 6 Click **Next**.

Step 7 Click **Return**.

Step 8 Close the Manage Roles window.

Step 9 On the **Admin** tab, click **Deploy Changes**.

When the deploy process completes, the **Risks** tab is available to use in the QRadar SIEM interface.

3 COLLECTING NETWORK DATA

Before you can leverage IBM Security QRadar Risk Manager's key capabilities, you must configure QRadar Risk Manager to read configuration information from the devices in your network. The configuration information collected from your network devices generates the Topology for your network and allows QRadar Risk Manager to understand your network configuration.

Data collected in QRadar Risk Manager is used to populate the Topology with key information about your network environment.

The QRadar Risk Manager data collection is a three step process:

1. Provide QRadar Risk Manager with the credentials to download network device configurations. For more information, see Configuring credentials.
2. Discover the devices to create a device list in Configuration Source Management. For more information, see Discovering devices
3. Backup the device list to obtain the device configurations and populate the Topology interface with data about your network. For more information, see Obtaining device configuration.

NOTE

QRadar Risk Manager MR4 and above includes a feature that allows you to import devices using a comma-separated list. This method can be used to import a large number of devices. For more information, see Device import.

Configuring credentials

To connect firewalls, routers, switches, or Intrusion Prevention System (IPS) devices, your QRadar Risk Manager must be configured with the proper credentials to access and download the device configurations.

Configuration Source Management enables an administrator to input device credentials, allowing QRadar Risk Manager to gain access to a specific device. QRadar Risk Manager can save individual device credentials for a specific network device, or if multiple network devices use the same credentials, you can assign credentials to a group. For example, if all firewalls in the organization have the same username and password. The credentials are associated with the address sets for all the firewalls and used to backup device configurations for all firewalls in your organization.

NOTE

If a network credential is not required for a specific device the parameter can be left blank in Configuration Source Management.

To configure device credentials:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Plug-ins**.

Step 3 In the **Risk Manager** pane, click **Configuration Source Management**.

Step 4 On the navigation menu, click **Credentials**.

Step 5 To configure the network groups:

a In the **Network Groups** pane, click the **Add** icon.

b Type a name for a network group.

c Click **OK**.

The network group is created and you can include the IP addresses for the network devices that share credentials, such as usernames and passwords. This list of IP addresses for a group of network devices is called an address set.

Step 6 To configure the address set:

a In the **Add Address** field, type the IP addresses by range or CIDR that you want to apply to the network group, then click the **Add** icon.

For example, type an IP address range using a dash or wildcard (*) to indicate a range, such as 10.100.20.0-10.100.20.240 or 1.1.1*. If you type 1.1.1.*, all IP addresses meeting that requirement are included.

b Repeat step **a** for all IP addresses you want to add to the address set for this network group.

As you add IP addresses, the window to the left of the Add Address field populates with a list of the IP addresses you’ve added.

After you have added all the IP addresses for your network devices, you can include the credentials required to log in to your network devices and retrieve the device configuration. The information required to log in to a group of network devices is called a credentials set.

Step 7 To configure the credentials set:

a In the **Credentials** pane, click the **Add** icon.

b Type a name for the new credential set.

c Click **OK**.

d Type values for the parameters:

Table 5-1 Credential Parameters

Parameter	Description
Username	Type the username for the credential set. ***Note:*** *When configuring the username with Juniper Networks NSM or a generic XML adapter, you must type a username with access to the Juniper NSM server or a username that allows access to log in to the file repository containing your SED files.*
Password	Type the password for the credential set. ***Note:*** *When configuring the password with Juniper Networks NSM or a generic XML adapter, you must type the password for the Juniper NSM server or the password to log in to the file repository containing your SED files.*
Enable Username	Type the username for second level authentication for the credential set.
Enable Password	Type the password for second level authentication for the credential set.
SNMP Get Community	Type the SNMP Get community name.
SNMPv3 Authentication Username	Type the username you want to use to authenticate SNMPv3.
SNMPv3 Authentication Password	Type the password you want to use to authenticate SNMPv3.
SNMPv3 Privacy Password	Type the protocol you want to use to decrypt SNMPv3 traps.

e Use the move up and move down icons to prioritize the credential sets groups.

Move the credential set you want to prioritize first to the top of the list.

f Repeat step **a** to step **f** to add any additional credential sets.

g Click **OK**.

You are now ready to discover network devices.

Discovering devices

The discovery process adds network devices to the topology interface using the credentials you added.

To discover devices:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Plug-ins**.

Step 3 In the **Risk Manager** section, click **Configuration Source Management**.

Step 4 On the navigation menu, click **Discover Devices**.

Step 5 Type an IP address or CIDR range.

This IP address or CIDR range indicates the location of devices you want to discover.

Step 6 Click the **Add** icon.

Step 7 If you also want to search for devices in the network from the defined IP address or CIDR range, select the **Crawl the network from the addresses defined above** check box. This check box is selected by default.

Step 8 Click **Run**.

As devices are discovered the Configuration Manager is updated.

Obtaining device configuration

After you have configured credential sets and have a list of network devices, you must backup your devices to download the device configuration so QRadar Risk Manager can include the device information in the Topology interface. The process of backing up a device to obtain a device configuration can be completed for a single device in the device list, or you can backup all devices from the **Devices** tab.

For more information about scheduling automated backups of device configurations from the **Jobs** tab, see the *IBM Security QRadar Risk Manager User Guide*.

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Plug-ins**.

Step 3 In the **Risk Manager** pane, click **Configuration Source Management**.

Step 4 Click the **Devices** tab.

Step 5 Choose one of the following options:

- To obtain the configuration for all devices, click **Backup All** in the navigation pane. Go to Step 7.
- To obtain the configuration for specific devices, select the individual device. To select multiple devices to backup, hold down the **CTRL** key. Go to Step 6.

Step 6 Click **Backup**.

Step 7 Click **Yes** to continue.

The device configuration is obtained.

If an error occurs, an exclamation icon is displayed in the table. If you want to view the details of the error information, click **View Error**.

Device import

Device import allows you to bulk add a list of adapters and their network IP addresses to the Configuration Source Manager using a comma-separated value file (.CSV). The device import list can contain up to 5000 devices, but the list must contain one line for each adapter and its associated IP address in the import file.

For example,

```
<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>
```

Where:

`<Adapter::Name>` contains the manufacturer and device name, such as Cisco::IOS.

`<IP Address>` contains the IP address of the device, such as 191.168.1.1.

Table 5-2 Device Import Examples

Manufacturer	Name	Example <Adapter::Name>,<IP Address>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Importing a CSV file

To import a master device list to Configuration Source Management from a CSV (comma-separated values) file:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Plug-ins**.

Step 3 In the **Plug-Ins** pane, click **Device Import**.

Step 4 Click **Browse**.

Step 5 Locate your CSV file, click **Open**.

The **File** field populates with the path of your CSV file.

Step 6 Click **Import Devices**.

Problems importing devices

If you receive an error message after trying to import your device, it might be because the import of the CSV file failed. Importing a device can fail if:

- The device list is structured incorrectly. For example, the CSV file might be missing colons or a command, multiple devices are on a single line.
- The device list contains incorrect information. For example, a typo for an adapter name.

If the device import aborts, then no devices from the CSV file are added to Configuration Source Management. A list of valid adapter names for your installed adapters is displayed in the message. If an error is displayed, then you need to review your CSV file to correct any errors. You can re-import the file once the errors are fixed.

4 MANAGING AUDITS WITH QRADAR RISK MANAGER

Compliance auditing is a necessary and complex task for security administrators. IBM Security QRadar Risk Manager helps to simplify the assessment of network security policies and compliance requirements by helping you answer the following questions:

- How are my network devices configured?

  For more information on using QRadar Risk Manager to evaluate this audit question, see Case 1: Centralizing configuration audit.
- How are my network resources communicating?

  For more information on using QRadar Risk Manager to evaluate this audit question, see Case 2: Viewing network paths using topology.
- Where is my network vulnerable?

  For more information on using QRadar Risk Manager to evaluate this audit question, see Case 3: Visualize the attack path of a QRadar SIEM offense.

Case 1: Centralizing configuration audit

QRadar Risk Manager captures configurations for all your network devices for auditing and allows you to schedule configuration backups at any time. These configuration backups provide a centralized and automatic method of recording device changes for your audit compliance. Configuration backups archive configuration changes and provide a historical reference. This allows you to capture a historical record or compare a configuration against another network device.

Configuration auditing using QRadar Risk Manager provides the following key features:

- A historical record of your network device configurations.
- A normalized view displaying devices changes when comparing configurations.
- View and search for rules on your device

The configuration information for your devices is collected from device backups in Configuration Source Management. Each time QRadar Risk Manager backs up your device list, it archives a copy of your device configuration to provide a historical reference. The more often you schedule Configuration Source

Management, the more configuration records you have for comparison and for historical reference.

Viewing device configuration history

To view the configuration history of a single network device:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Configuration Monitor**.

The list of configured devices is displayed.

Step 3 Double-click a configuration to view the detailed device information.

Step 4 Click **History**.

The History pane displays the backup history.

Table 6-3 Device Backup History Parameters

Parameter	Description
Configuration	Displays the type of files stored for your network device in QRadar Risk Manager. The common configuration types can include: • **Standard-Element-Document** - Standard-Element Document (SED) files are XML data files that contain information on your network device. Individual SED files are viewed in their raw XML format. If an SED is compared to another SED file, then the view is normalized to display the rule differences. • **Config** - Configuration files are provided by certain network devices depending on the device manufacturer. A configuration file can be viewed by double-clicking on the config file. ***Note:*** *Depending on your device, several other configuration files might be displayed. Double-clicking these files displays the contents in plain text. The plain text view supports the find (Ctrl +f), paste (Ctrl+v), and copy (Ctrl+C) functions from the browser window.*
Date Obtained	The date that the device configuration was last backed up from Configuration Source Management.

Step 5 On the History pane, select a configuration.

Step 6 Click **View Selected**.

The information contained in the device backup is displayed.

Comparing device configurations

QRadar Risk Manager enables you to compare device configurations. Comparing Standard-Element-Document (SED) files allow you to view a comparison table with added, modified, or deleted device rules.

To compare device configurations:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Configuration Monitor**.

The list of configured devices is displayed.

Step 3 Double-click any device to view the detailed configuration information.

Step 4 Click **History** to view the history for this device.

The History table is displayed.

Step 5 Select your comparison type from the table below:

Table 6-4 Device Comparisons

If you want to	Then
Compare two configurations backups from a single device	To compare two configurations from a single device: **1** Select a primary configuration. **2** Press the Ctrl key and select a second configuration for comparison. **3** On the History pane, click **Compare Selected**. If the comparison files are Standard-Element-Documents (SEDs), then the Normalized Device Configuration Comparison window displays a table showing rule differences between the the configuration files. When comparing normalized configurations, the color of the text indicates the following: • **Green Dotted Outline** - Indicates a rule or configuration that was added to the device. • **Red Dashed Outline** - Indicates a rule or configuration that was deleted from the device. • **Yellow Solid Outline** - Indicates a rule or configuration that was modified on the device. **4** Optional. To view the raw configuration differences, click **View Raw Comparison**. ***Note:*** *If the comparison was a config file or another backup type, then the raw comparison is displayed.*

Table 6-4 Device Comparisons (continued)

If you want to	Then
Compare two configurations on different devices	To compare two configurations on separate devices, you must mark a configuration for comparison on one device, then compare a device backup to the marked configuration. To compare device configurations: **1** Select a primary device configuration. **2** Click **Mark for Comparison**. A flag is displayed next to the configuration marked for comparison. **3** From the navigation menu, select **All Devices** to return to the device list. **4** Double-click the device to compare and click **History**. **5** Select another configuration backup to compare with the marked configuration. **6** Click **Compare with Marked**. If the comparison files were Standard-Element-Documents (SEDs), then the Normalized Device Configuration Comparison window is displayed with a table showing rule differences between the backups. When comparing normalized configurations, the color of the text indicates the following: • **Green Dotted Outline** - Indicates a rule or configuration that was added to the device. • **Red Dashed Outline** - Indicates a rule or configuration that was deleted from the device. • **Yellow Solid Outline** - Indicates a rule or configuration that was modified on the device. **7** Optional. To view the raw configuration differences, click **View Raw Comparison**. ***Note:*** *If the comparison was a config file or another backup type, then the raw comparison is displayed.*

Case 2: Viewing network paths using topology

The Topology in QRadar Risk Manager displays your network devices in a graphical representation. A Topology path search can determine how your network devices are communicating and the network path that they use to communicate. Path searching allows QRadar Risk Manager to visibly display the path between a source and destination, along with the ports, protocols, and rules. As an auditing feature QRadar Risk Manager allows you to view how devices communicate, which is especially important on secured or restricted access assets.

Key features include:

- Ability to view communications between devices on your network.
- Topology search filtering for network devices.
- Quick access to view device rules and configuration.
- Ability to view events generated from a path search.

Searching topology To view device communication using a topology search:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

The Topology interface is displayed.

Step 3 From the **Search** list box, select **New Search**.

The Saved Searches window is displayed.

Step 4 In the Search Criteria pane, select **Path**.

The path search option filters the topology model to include all network subnets containing the source IP addresses/CIDR ranges and subnets containing destination IP addresses/CIDR ranges that are also allowed to communicate using the configured protocol and port. The search examines your existing topology model and includes the devices that are involved in the communication path between the source and destination and detailed connection information.

Step 5 Configure the following parameters:

Table 6-5 Path Filter Parameters

Parameter	Description
Source IP/CIDR	Type the IP address or CIDR range on which you want to filter the topology model. Separate multiple entries using a comma separated list.
Destination IP/CIDR	Type the destination IP address or CIDR range on which you want to filter the topology model. Separate multiple entries using a comma separated list.
Protocol	Optional. Using the drop-down list box, select the protocol you want to use to filter the topology model. The options are: • Any Protocol (default) • TCP • UDP • ICMP
Destination Port	Optional. Type the destination port on which you want to filter the topology model. Separate multiple ports using a comma separated list.

Table 6-5 Path Filter Parameters

Parameter	Description
Vulnerabilities	This parameter is only displayed if your topology includes an Intrusion Prevention System (IPS). To filter using vulnerabilities: **1** Click **Vulnerabilities**. **2** Using the **Search By** drop-down list box, select the vulnerability option on which you want to search. The options include: OSVDB Title, CVE ID, Bugtraq ID, or OSVDB ID. **3** Type or select a search parameter. **4** Click **Search**. Search results appear in the Search Results box. **5** For any results on which you want to filter the topology, select the value in the Search Results box. Click **Add**. **6** Repeat for all results on which you want to filter. **7** Click **Submit**.

Step 6 Click **OK**.

The topology path is displayed along with the direction of the search.

Step 7 Move your mouse over a connection line to view detailed connection detail.

If the search connects to a device that contains rules, a device rules link is displayed in the dialog.

The case configuration is complete.

Case 3: Visualize the attack path of a QRadar SIEM offense

Offenses in QRadar Risk Manager are events generated by the system to alert you to a network condition or event. The integration between QRadar Risk Manager and QRadar Risk Manager provides you with the next step, allowing you to visualize the attack path of an offense. Attack path visualization ties offenses with Topology searches, allowing security operators to view the offense detail and the path the offense took through your network.

The attack path provides you with a visual representation of the assets in your network that are communicating to allow an offense to travel through the network. This data can be critical during auditing to prove you monitor for offenses, but also prove the offense does not have an alternate path in your network to a critical asset.

Key features:

- Leverages the existing rule and offense system from QRadar SIEM.
- Displays a visual path for all devices between the source and destination of the offense.
- Quick access to device configurations and rules that allowed the offense.

To view attack paths for offenses:

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **All Offenses**.

The All Offenses page displays a list of offenses that QRadar SIEM has identified on your network. Offenses are listed with the highest magnitude first.

Step 3 Double-click an offense to open the offense summary.

Step 4 On the Offenses toolbar, click **View Attack Path**.

The attack path showing the source, destination, and associated devices is displayed.

5 MONITORING POLICIES WITH QRADAR RISK MANAGER

Policy auditing and change control are fundamental processes that allow administrators and security professionals to control access and communications between critical business assets. The criteria for policy monitoring can include monitoring of assets and communications for the following scenarios:

- Does my network contain assets with risky configurations for PCI Section 1 audits?

  For more information, see Case 4: Assessing assets with suspicious configurations (PCI Section 1).

- Do my assets allow communications using risky protocols for PCI Section 10 audits?

  For more information, see Case 5: Assessing assets with questionable communications (PCI Section 10).

- How do I know when a policy change puts my network in violation?

  For more information, see Case 6: Monitoring for policy violations.

- How do I view vulnerabilities for hardened or high risk assets?

  For more information, see Case 7: Prioritizing asset risk by vulnerability.

- How to I view assets in the network with vulnerabilities and Internet access?

  For more information, see Case 8: Prioritizing asset vulnerabilities by zone or network communications.

The Policy Monitor enables users to define tests based on the risk indicators, then restrict the test results to filter the query for specific results, violations, protocols, or vulnerabilities. IBM Security QRadar Risk Manager includes several Policy Monitor questions that are grouped by PCI category, such as PCI 1, PCI 6, and PCI 10 questions. Questions can be created for assets or devices and rules to expose network security risk. Once a question about an asset or a device/rule is submitted to the Policy Monitor, QRadar Risk Manager returns results specified by the level of risk. The Policy Monitor allows you to approve results returned from assets or define how you want the system to respond to unapproved results.

Key features:

- Predefined Policy Monitor questions to assist with workflow
- Analyzing if users have communicated using forbidden protocols.
- Assessing if users on specific networks can communicate to forbidden networks or assets.
- Assessing if firewall rules meet corporate policy.
- Continuous monitoring of policies that generate offenses or alerts to administrators.
- Prioritizing vulnerabilities by assessing which systems can be compromised due to device configuration.
- Policy Monitor questions can help identify compliance issues by identifying the following policy questions:

Case 4: Assessing assets with suspicious configurations (PCI Section 1)

Organizations use their corporate security policies to define risk and what communications are allowed between assets and networks. The Policy Monitor allows you to query your Topology to assess and monitor for risks that could be unknown to assist with compliance and corporate policy breaches. PCI compliance dictates that you identify devices containing cardholder data, then diagram, verify communications, and monitor firewall configurations to protect assets containing sensitive data. QRadar Risk Manager provides methods for quickly meeting these requirements and allow administrators to adhere to corporate policies using the Policy Monitor. Common methods of reducing risk include identifying and monitoring assets communicating with unsecured protocols, for example, routers, firewalls, or switches that allow FTP or telnet connections. QRadar Risk Manager can easily identify assets in your Topology with risky configurations by using the Policy Monitor.

PCI section 1 questions can include the following criteria:

- Assets that allow banned protocols.
- Assets that allow risky protocols.
- Assets that allow out-of-policy applications across the network.
- Assets that allow out-of-policy applications to networks containing protected assets.

To determine assets that communicate using a risky protocols:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

The Policy Monitor interface is displayed.

Step 3 From the **Group** list box, select **PCI 1**.

The Question Editor displays a list of PCI 1 compliance questions.

Step 4 Select the test question **Assess any devices (i.e. firewalls) that allow risky protocols (i.e telnet and FTP traffic - port 21 & 23 respectively) from the internet to the DMZ**.

Step 5 Click **Submit Question**.

QRadar Risk Manager evaluates the question and displays the results of any assets in your topology matching the test question.

Security professionals, administrators, or auditors in your network can approve communications that are not risky to specific assets or create offenses in QRadar SIEM for the behavior.

Case 5: Assessing assets with questionable communications (PCI Section 10)

The Policy Monitor in QRadar Risk Manager allows an organization to identify PCI section 10 compliance by tracking, logging, and displaying access to network assets. QRadar Risk Manager can help to identify PCI section 10 compliance by identifying assets in the Topology that allow questionable or risky communications. QRadar Risk Manager can examine these assets for actual communications or possible communications. Actual communications display assets that have communicated using your question criteria. Possible communications display assets that can communicate using your question criteria.

PCI section 10 questions can include the following criteria:

- Assets that allow incoming questions to internal networks.
- Assets that communicate from untrusted locations to trusted locations.
- Assets that communicate from a VPN to trusted locations.
- Assets that allow unencrypted out-of-policy protocols within a trusted location.

To determine assets that allow communication from the Internet:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

The Policy Monitor is displayed.

Step 3 From the **Group** list box, select **PCI 10**.

The Question Editor displays a list of PCI 10 compliance questions.

Step 4 Select the test question **Assess any inbound connections from the internet to anywhere on the internal network**.

Step 5 Click **Submit Question**.

QRadar Risk Manager evaluates the question and displays the results of any internal assets that allow inbound connections from the Internet.

Security professionals, administrators, or auditors in your network can approve communications to assets that are not considered secure or containing customer data. As additional events are generated, you can create offenses in QRadar SIEM to monitor this type of risky communication.

Case 6: Monitoring for policy violations

QRadar Risk Manager can continuously monitor any predefined or user-generated question in the Policy Monitor using monitor mode to generate events in QRadar Risk Manager. When you select a question to be monitored, QRadar Risk Manager analyzes the question against your Topology every hour to determine if an asset or rule change generates an unapproved result. If QRadar Risk Manager detects an unapproved result, an offense can be generated to alert you to a deviation in your defined policy. QRadar Risk Manager can monitor the results of ten questions simultaneously in monitor mode.

Key features of question monitoring include:

- Monitoring for rule or asset changes hourly for unapproved results.
- Categorizing of unapproved results using your high and low level event categories.
- Generating offenses, e-mails, syslog messages, or dashboard notifications on unapproved results.
- Using event viewing, correlation, event reporting, custom rules, and dashboards in QRadar SIEM.

To configure a question to be monitored:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

The Policy Monitor is displayed.

Step 3 Select the question you want to monitor.

Step 4 Click **Monitor**.

The Monitor Question Results window is displayed.

Step 5 Configure values for the parameters:

Table 7-6 Monitor Question Results Parameters

Parameter	Description
Event Name	Specify the name of the event you want to display in the **Log Activity** and **Offenses** tabs.
Event Description	Specify a description for the event. The description is displayed in the event summary details.

Table 7-6 Monitor Question Results Parameters (continued)

Parameter	Description
Event Details	Configure the following options: • **High-Level Category** - From the drop-down list box, select the high-level event category you want this rule to use when processing events. • **Low-Level Category** - From the drop-down list box, select the low-level event category you want this rule to use when processing events. For more information on event categories, see the *QRadar Users Guide*. • **Ensure the dispatched event is part of an offense (Correlate By:)** - Select this check box if you want to correlate the results of this monitored question by the question or asset. QRadar SIEM can correlate events with destination IP addresses located across multiple networks in the same offense, and ultimately the same incident. If no correlation is detected, a new offense is created. If an offense exists, the event indicates there are multiple events and the incident count is increased for the question or asset. If you select this check box, the following list box options are available: **Question/Simulation** - All events from a question are associated to a single offense. **Asset** - A unique offense is created (or updated) for each unique asset.
Additional Actions	Select the check boxes to indicate the additional actions to be taken when an event is received. The options include: • **e-mail** - Select this check box and type an e-mail address to send a notification if the event occurs. Separate multiple e-mail addresses using a comma. • **Send to Syslog** - Select this check box if you want to log the event. By default, the check box is clear. For example, the syslog output may resemble: `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description` • **Notify** - Select this check box if you want to display events from the monitored question as a System Notification in the QRadar SIEM Dashboard. For more information on the **Log Activity** tab and the QRadar SIEM Dashboard, see the *IBM Security QRadar SIEM Users Guide.*

Table 7-6 Monitor Question Results Parameters (continued)

Parameter	Description
Enable Monitor	Select this check box to enable monitoring of the question. By default, this check box is selected. If you do not want to monitor a question, clear the check box.

Step 6 Click **Save Monitor**.

QRadar Risk Manager enables monitoring for the question and generates events or offenses based on your monitoring criteria.

Case 7: Prioritizing asset risk by vulnerability

Exposed vulnerabilities are a significant risk factor for network assets. QRadar Risk Manager leverages asset information and vulnerability information in the policy monitor to determine if your assets are susceptible to input type attacks, such as; SQL injection, hidden fields, and clickjacking. Vulnerabilities detected on your assets can be prioritized by their network location or a connection to another device that is vulnerable.

Vulnerable asset questions can include the following criteria:

- Assets with new vulnerabilities reported after a specific date.
- Assets with specific vulnerabilities or CVSS score.
- Assets with a specific classification of vulnerability, such as input manipulation, denial of service, OSVDB verified.

To determine assets with vulnerabilities using the Policy Monitor:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

The Policy Monitor interface is displayed.

Step 3 From the **Group** list box, select **Vulnerability**.

The Question Editor displays a list of vulnerability questions.

Step 4 Select the test question **Assess assets with SQL injection vulnerabilities on specific localnet(s) (i.e. protected server network)**.

Step 5 Click **Submit Question**.

QRadar Risk Manager evaluates the question and displays the results of assets containing your vulnerability.

Security professionals, administrators, or auditors can identify assets in your network that contain known SQL injection vulnerabilities and promptly patch any assets connected to a protected network. As additional events are generated, you can create events or offenses in QRadar SIEM to monitor for other assets containing SQL injection vulnerabilities.

Case 8: Prioritizing asset vulnerabilities by zone or network communications

Systems with vulnerabilities in the same network as protected assets are at greater risk for data loss. Detecting vulnerabilities on assets by zone or network are key measures preventing exploits before they occur in your network. PCI section 6.1 and 6.2 stipulate that you review and patch systems within one month of a vulnerability patch release. QRadar Risk Manager assists with automating and prioritizing the patch process. As vulnerabilities are detected on your assets, you can prioritize by the network location or a connection to another device that is vulnerable. This is important for secured networks that can be connected to suspicious regions, or assets that contain a CVSS score greater than your internal policy allows.

Vulnerable asset questions can include:

- Assets with client side vulnerability which have communicated to suspicious geographic regions and contain protected assets.
- Assets with denial of service vulnerabilities in a specific network.
- Assets with mail vulnerabilities in a specific network.
- Assets with vulnerabilities and the specific Common Vulnerability Scoring System (CVSS) score.

To determine assets with vulnerabilities in a specific network

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

The Policy Monitor is displayed.

Step 3 From the **Group** list box, select **Vulnerabilities**.

The Question Editor displays a list of PCI 10 compliance questions.

Step 4 Select the test question **Assess assets with OS specific vulnerabilities on a specific localnet(s)**

This asset test allows you to find vulnerabilities on networks containing

Step 5 Click **Submit Question**.

QRadar Risk Manager evaluates the question and displays the results in the specific location that contains OS specific vulnerabilities.

Security professionals, administrators, or auditors in your network can approve communications to assets that are not considered secure or containing customer data. As additional events are generated, you can create offenses in QRadar SIEM to monitor this type of risky communication.

6 USING SIMULATIONS WITH QRADAR RISK MANAGER

Simulations allow you to define, schedule, and run exploit simulations on your network. Simulations are a pre-exploit activity that allow you to understand how network changes and specific attacks open your network to risk. Simulations allow you to view and understand how your network is protected against attacks from various sources and paths. The process of running simulations allows you to understand how your firewall rules and device configurations withstand network attacks, vulnerabilities, and device changes.

Key features:

- Simulating attacks on your current Topology or against simulated topology models.
- Simulating attacks against assets, allowing you to specify:
  - Networks and IP addresses
  - Building blocks
  - Protocols or open ports
  - Vulnerabilities, using CVSS, dates, or vulnerability classifications
- Simulating attacks to secure your networks from specific attack sources:
  - Internet attacks
  - Specific geographic locations
  - Users who have visited a specific geographic location
  - Remote network locations
- Simulations allow monitoring to identify new exposure to attacks.
- Simulations display theoretical path and attack propagation information.

You can create simulations based on a series of rules that can be combined and configured. The simulation can be scheduled to run on a periodic basis or run manually. After a simulation is complete, you can review the results of the simulation and approve any acceptable or low risk results based on your network policy. This allows you to approve acceptable actions or traffic from your results. After you have tuned your simulation, you can then configure the simulation to monitor the results. Monitoring a simulation enables you to define how you want the system to respond when unapproved results are returned. This response could be an e-mail, the creation of an event, or to send the response to syslog.

IBM Security QRadar Risk Manager helps strengthen your network and test rules and configurations, allowing you to identify audit criteria without making actual network configuration changes.

Simulations help you answer the following questions:

- How can I simulate attacks to understand my network risk?

  For more information, see Case 9: Simulating attacks on network assets.
- How do I assess the risk involved of changing the configuration of my network device?

  For more information, see Case 10: Simulating the risk of network configuration changes.

Case 9: Simulating attacks on network assets

Simulations allow you to test your network for vulnerabilities from various sources. Attack simulations allow you to audit device configurations in your network using QRadar Risk Manager to provide the following key features:

- Simulations display the theoretical path permutations an attack can take against your network.
- Simulations display how attacks can propagate through your network devices to spread to other assets.
- Simulations allow monitoring to detect new exposure sites.

To create a simulation that attacks your network for SSH vulnerabilities:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

The Simulations window is displayed.

Step 3 From the **Actions** list box, select **New**.

The Simulation Editor window is displayed.

Step 4 Type a name for the simulation.

This name that is displayed in the list of simulations.

Step 5 Select **Current Topology**.

Step 6 Select the **Use Connection Data** check box.

Step 7 From the **Where do you want the simulation to begin?** list box, select an origin for the simulation.

Step 8 Add the simulation attack **Attack targets a vulnerability on one of the following ports using protocols**.

Step 9 Configure the following parameters:

- **Ports** - Specify port 22 for this simulation.
- **Protocols** - Specify TCP as Secure Shell (SSH) uses TCP.

Step 10 Click **OK**.

Step 11 Click **Save Simulation**.

Step 12 Select the simulation you created.

Step 13 From the **Actions** list box, select **Run Simulation**.

The results column contains a list box with the date the simulation was run and a link to view the results.

Step 14 Click **View Results**.

A list of assets containing SSH vulnerabilities is displayed in the results, allowing network administrators to approve SSH connections that are allowed or expected in your network. The communications that are not approved can be monitored for events or offenses.

The results that are displayed provide your network administrators or security professionals with a visual representation of the attack path and steps involved with the connections the attack could theoretically take in your network. For example, the first step provides a list of the directly connected assets affected by the simulation. The second step lists assets in your network that can communicate to first level assets in your simulation.

The information provided in the attack allows you to strengthen and test your network against thousands of possible attack scenarios.

Case 10: Simulating the risk of network configuration changes

A topology model from the Simulation navigation menu allows you to define virtual network models based on your existing network. You can create a network model based on a series of modifications that can be combined and configured. topology models allows you to determine the effect of configuration changes on your network using the Simulation functionality.

Toplogy models provide the following key functionality:

- Create virtual topologies for testing network changes
- Simulate attacks against virtual networks
- Lower risk and exposure to protected assets through testing
- Virtual network segments allow you to confine and test sensitive portions of your network or assets.

To simulate a network configuration change:

1 Create a topology model. For more information, see Creating a topology model.

2 Simulate an attack against the topology model. For more information, see Simulating an attack against a topology model.

Creating a topology model

To create a topology model:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

Step 3 From the **Actions** list box, select **New**.

Step 4 Type a name for the model.

Step 5 Select any modifications you want to apply to the Topology.

Step 6 Configure the tests added to the **Configure model as follows** pane.

Step 7 Click **Save Model**.

The topology model is created using your defined network changes. You are now ready to run a simulation against your model.

Simulating an attack against a topology model

Simulating an attack on a topology model is a similar process to the simulation attack created in the previous test case. The difference between the two simulations is that one test uses the current Topology and an attack against a topology model requires you to select the model you want to test again. Simulations against topology models cannot use connection data, as connection data does not exist in the model.

To create a simulation that attacks your network for SSH vulnerabilities:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

The Simulations window is displayed.

Step 3 From the **Actions** list box, select **New**.

The Simulation Editor window is displayed.

Step 4 Type a name for the simulation.

This name that is displayed in the list of simulations.

Step 5 Select a topology model you created.

Step 6 From the **Where do you want the simulation to begin?** list box, select an origin for the simulation.

Step 7 Add the simulation attack **Attack targets a vulnerability on one of the following ports using protocols**.

Step 8 Configure the following parameters:

- **Ports** - Specify port 22 for this simulation.

- **Protocols** - Specify TCP as Secure Shell (SSH) uses TCP.

Step 9 Click **OK**.

Step 10 Click **Save Simulation**.

Step 11 Select the simulation you created.

Step 12 From the **Actions** list box, select **Run Simulation**.

The results column contains a list box with the date the simulation was run and a link to view the results.

Step 13 Click **View Results**.

A list of assets is provided in the results for your network so administrators can approve SSH connections that are allowed or expected in your network.

The results that are displayed provide your network administrators or security professionals with a visual representation of the attack path and steps involved with the connections the attack could theoretically take in your network. For example, the first step provides a list of the directly connected assets affected by the simulation. The second step lists assets in your network that can communicate to first level assets in your simulation.

The information provided in the attack allows you to strengthen and test your network against thousands of possible attack scenarios.

A NOTICES AND TRADEMARKS

What's in this appendix:

- Notices
- Trademarks

This section describes some important notices, trademarks, and compliance information.

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 grant 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 may 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
170 Tracer Lane,
Waltham MA 02451, USA

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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 softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

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

INDEX