JUNIPER NETWORKS | Engineering Simplicity

Juniper Secure Analytics Risk Manager Getting Started Guide

Published
2022-05-09

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Secure Analytics Risk Manager Getting Started Guide
7.5.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to understand how to perform basic JSA Risk Manager configuration, begin collecting event and flow data, and generate custom or default reports.

1

CHAPTER

Get Started with JSA Risk Manager

Get Started with JSA Risk Manager

JSA Risk Manager is a separately installed appliance. Use JSA Risk Manager to monitor device configurations, simulating changes to your network environment, and prioritize risks and vulnerabilities in your network.

JSA Risk Manager is accessed from the **Risks** tab on the JSA console.

JSA Risk Manager enhances JSA by providing administrators with tools to complete the following tasks:

- Centralize risk management.
- Use a topology to view your network.
- Configure and monitor network devices.
- View connections between network devices.
- Search firewall rules.
- View existing rules and the event count for triggered rules.
- Search for devices and paths for your network devices.
- Monitor and audit your network to ensure compliance.
- Define, schedule, and run exploit simulations on your network.
- Search for vulnerabilities.

Centralized risk management and compliance for increased intelligence of information might involve the cooperation of many internal teams. As a next generation SIEM with an additional Risk Management appliance, we reduce the number of steps that are required from first-generation SIEM products. We provide network topology and risk assessment for assets that are managed in JSA.

During the evaluation process, you consolidate your system, security, risk analysis, and network information through aggregation and correlation, providing complete visibility into your network environment. You also define a portal to your environment, which provides visibility and efficiency that you cannot achieve by using manual processes and other point product technologies.

2
CHAPTER

Deploy JSA Risk Manager

Deploy JSA Risk Manager

Your JSA Risk Manager appliance is installed with the latest version of JSA Risk Manager software.

You must install the JSA Risk Manager evaluation appliance. The software requires activation and you must assign an IP address to the JSA Risk Manager appliance.

The appliance is ready to accept information from your network devices.

For information about using JSA Risk Manager, see the *Juniper Secure Analytics Risk Manager User Guide*.

To deploy JSA Risk Manager in your environment, you must:

1. Ensure that the latest version of JSA is installed.
2. Ensure all pre-installation requirements are met.
3. Set-up and power on your JSA Risk Manager appliance.
4. Add JSA Risk Manager as a managed host on your JSA console.
5. Establish communication between JSA and the JSA Risk Manager appliance.
6. Define user roles for your JSA Risk Manager users.

Before You Install

You must complete the installation process for an JSA console before you install JSA Risk Manager. As a best practice, install JSA and JSA Risk Manager on the same network switch.

Before you install the JSA Risk Manager evaluation appliance, ensure that you have:

- space for a two-unit appliance
- rack rails and shelving that are mounted

Optionally, you might want a USB keyboard and standard VGA monitor to access the JSA console.

RELATED DOCUMENTATION

Configure Port Access on Firewalls | 5

Configure Port Access on Firewalls

Firewalls between the JSA console and JSA Risk Manager must allow traffic on certain ports.

Ensure that any firewall located between the JSA console and JSA Risk Manager allows traffic on the following ports:

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

RELATED DOCUMENTATION

Identify Network Settings

You must gather information about your network settings before starting the installation process.

Gather the following information for your network settings:

- Host name
- IP address
- Network mask address
- Subnet mask
- Default gateway address
- Primary Domain Name System (DNS) server address

- Secondary DNS server (optional) address
- Public IP address for networks that use Network Address Translation (NAT) email server name
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

RELATED DOCUMENTATION

Unsupported Features in JSA Risk Manager | 6
Supported Web Browsers | 7
JSA Risk Manager Login Information | 8

Unsupported Features in JSA Risk Manager

It is important to be aware of the features that are not supported by JSA Risk Manager.

The following features are not supported in JSA Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP)
- Non-contiguous network masks
- Load-balanced routes

RELATED DOCUMENTATION

Supported Web Browsers | 7
JSA Risk Manager Login Information | 8
Setting Up a JSA Risk Manager Appliance | 9

Supported Web Browsers

IN THIS SECTION

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

The following table lists the supported versions of web browsers.

Table 1: Supported Web Browsers for JSA Products

Web browser	Supported versions
64 bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge.	38.14393 and later
64 bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported as of JSA 7.4.0 or later.

Security Exceptions and Certificates

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to JSA. For more information, see your Mozilla Firefox web browser documentation.

Navigate the Web-Based Application

When you use JSA, use the navigation options available in the JSA Console instead of your web browser **Back** button.

Enabling Document Mode and Browser Mode in Internet Explorer

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

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 the **Internet Explorer standards** for your Internet Explorer release.

RELATED DOCUMENTATION

JSA Risk Manager Login Information | 8
Setting Up a JSA Risk Manager Appliance | 9
Adding JSA Risk Manager to JSA Console | 10

JSA Risk Manager Login Information

JSA Risk Manager uses default login information for the URL, username, and password.

You access JSA Risk Manager through the JSA console. Use the information in the following table when you log in to your JSA console.

Table 2: Default Login Information for JSA Risk Manager

Login information	Default
URL	**https://<IP address>**, where *<IP address>* is the IP address of the JSA console.
Username	admin
Password	The password that is assigned to JSA Risk Manager during the installation process. **TIP**: As a good security practice, change the root password on your JSA Risk Manager host at regular intervals.
License key	A default license key provides access to the system for 5 weeks.

RELATED DOCUMENTATION

Setting Up a JSA Risk Manager Appliance | 9

Adding JSA Risk Manager to JSA Console | 10

Establishing Communication | 12

Setting Up a JSA Risk Manager Appliance

"Before You Install" on page 4

You install JSA Risk Manager as a separate appliance and then add it to your JSA console as a managed host by using the System and License Management tool on the Admin tab.

The JSA Risk Manager evaluation appliance is a two-unit rack mount server. Rack rails and shelving are not provided with evaluation equipment.

The JSA Risk Manager appliance includes four network interfaces. For this evaluation, use the network interface that is labeled eth0 as the management interface. The other interfaces are monitoring interfaces. All of the interfaces are on the back panel of the JSA Risk Manager appliance.

The power button is on the front panel.

1. Connect the management network interface to the port labeled eth0.
2. Ensure that the dedicated power connections are plugged into the rear of the appliance.
3. Optional: To access the JSA console, connect the USB keyboard and a standard VGA monitor.
4. If the appliance has a front pane, remove the pane by pushing in the tabs on either side and pull the pane away from the appliance.
5. Press the power button on the front to turn on the appliance.

> **NOTE**: If the LED light is flashing, the appliance is turned off.

The appliance begins the startup process.

RELATED DOCUMENTATION

Adding JSA Risk Manager to JSA Console | 10

Establishing Communication | 12

Adding the Risk Manager User Role | 13

Adding JSA Risk Manager to JSA Console

If you want to enable compression, then the minimum version for each managed host must be JSA console 2014.1 or JSA Risk Manager 2014.1.

To add a managed host that is not NATed to your deployment where the Console is NATed, you must change the JSA console to a NATed host. You must change the console before you add the managed host to your deployment. For more information, see the *Juniper Secure Analytics Administration Guide*.

You must add JSA Risk Manager as a managed host to JSA console.

1. Open your web browser.
2. Type the URL, **https://<*IP Address*>**, where <*IP Address*> is the IP address of the JSA console.
3. Type your user name and password.
4. Click the **Admin** tab.
5. In the **System Configuration** pane, click **System and License Management**.
6. In the **System and License Management** window, click **Deployment Actions**, and then select **Add Host**.
7. Enter values for the following parameters:

Option	Description
Host IP	The IP address of JSA Risk Manager.
Host Password	The root password for the host.
Confirm Host Password	Confirmation for your password.
Encrypt Host Connections	Creates an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running JSA console 2014.1 or JSA Risk Manager 2014.1.
Encryption Compression	Enables data compression between 2 managed hosts.

(Continued)

Option	Description
Network Address Translation	To enable NAT for a managed host, the NATed network must be using static NAT translation. For more information, see the *Juniper Secure Analytics Administration Guide*.

8. If you select the **Network Address Translation** check box, then you must enter values for the NAT parameters:

Option	Description
NAT Group	The network that you want this managed host to use. If the managed host is on the same subnet as the JSA console, select the console of the NATed network. If the managed host is not on the same subnet as the JSA console, select the managed host of the NATed network.
Public IP	The public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks that use NAT.

9. Click **Add**.

   This process can take several minutes to complete. If your deployment includes changes, then you must deploy all changes.

10. From the **Admin** tab, click **Advanced >Deploy Full Configuration**.

Clear your web browser cache and then log in to JSA console. The **Risks** tab is now available.

RELATED DOCUMENTATION

Establishing Communication | 12

Adding the Risk Manager User Role | 13

Setting Up a JSA Risk Manager Appliance | 9

Establishing Communication

You must establish communication between your JSA Risk Manager appliance and your JSA console before you set up and configure JSA Risk Manager.

The process to establish communications might take several minutes to complete. If you change the IP address of your JSA Risk Manager appliance or need to connect JSA Risk Manager to another JSA console, you can use the **Risk Manager Settings** on the JSA **Admin** tab.

1. Open your web browser, and then clear the web browser cache.
2. Log in to JSA. For information about the IP address, user name or root password, see "Access the JSA Risk Manager User Interface" on page 8.
3. Click the **Risks** tab.
4. Type values for the following parameters:

Option	Description
IP/Host	The IP address or host name of the JSA Risk Manager appliance
Root Password	The root password of the JSA Risk Manager appliance.

5. Click **Save**.

"Adding the Risk Manager User Role" on page 13

RELATED DOCUMENTATION

Adding the Risk Manager User Role | 13
Setting Up a JSA Risk Manager Appliance | 9
Adding JSA Risk Manager to JSA Console | 10

Adding the Risk Manager User Role

You must assign the Risk Manager user role to provide access to JSA Risk Manager.

By default, JSA provides a default administrative role, which provides access to everything in JSA 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: You need the Risk Manager role to access JSA Risk Manager, but you also need the System Administrator role to use all of the JSA Risk Manager functions.

For information about creating and managing user roles, see the *Juniper Secure Analytics Administration Guide*.

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. In the **User Management** pane, click **User Roles**.
4. In the left pane, select the user role that you want to edit.
5. Select the **Risk Manager** checkbox.
6. Click **Save**
7. Click **Close**.
8. On the **Admin** tab, click **Deploy Changes**.

RELATED DOCUMENTATION

Setting Up a JSA Risk Manager Appliance | 9

Adding JSA Risk Manager to JSA Console | 10

Establishing Communication | 12

3

CHAPTER

Manage Audits

Manage Audits

JSA Risk Manager helps to simplify the assessment of network security policies and compliance requirements by helping you answer questions.

Compliance auditing is a necessary and complex task for security administrators. JSA Risk Manager helps you answer the following questions:

- How are my network devices configured?
- How are my network resources communicating?
- Where is my network vulnerable?

Use Case: Device Configuration Audit

IN THIS SECTION

You can use the configuration information for network devices, which is captured by JSA Risk Manager, for audit compliance and to schedule configuration backups.

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; you can capture a historical record or compare a configuration against another network device.

Configuration auditing in JSA Risk Manager provides you with the following options:

- A historical record of your network device configurations.
- A normalized view, which displays device changes when you compare configurations.
- A tool to search for rules on your device.

The configuration information for your devices is collected from device backups in Configuration Source Management. Each time JSA 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

You can view the configuration history of a network device.

You can view history information for network devices that were backed up. This information is accessible from the **History** pane on the **Configuration Monitor** page. The history pane provides information about a network device configuration and the date that the device configuration was last backed up using Configuration Source Management.

The configuration displays the type of files that are stored for your network device in JSA Risk Manager. The common configuration types are:

- **Standard-Element-Document** (SED), which are XML data files that contain information about 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**, which are configuration files that are provided by certain network devices. These files depend on the device manufacturer. A configuration file can be viewed by double-clicking the configuration 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 web browser window.

1. Click the **Risks** tab.
2. On the navigation menu, click **Configuration Monitor**.
3. Double-click a configuration to view the detailed device information.
4. Click **History**.
5. On the **History** pane, select a configuration.
6. Click **View Selected**.

Comparing Device Configurations for a Single Device

You can compare device configurations for a single device.

If the files that you compare are Standard-Element-Documents (SEDs), then you can view the rule differences between the configuration files.

When you compare normalized configurations, the color of the text indicates the following rules:

- 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.

1. Click the **Risks** tab.
2. On the navigation menu, click **Configuration Monitor**.
3. Double-click any device to view the detailed configuration information.
4. Click **History** to view the history for this device.
5. Select a primary configuration.
6. Press the Ctrl key and select a second configuration for comparison.
7. On the **History** pane, click **Compare Selected**.
8. Optional. To view the raw configuration differences, click **View Raw Comparison**.

   If the comparison is for a configuration file or another backup type, then the raw comparison is displayed.

Comparing Device Configurations for Different Devices

You can compare configurations for different devices. If the files that you compare are Standard-Element-Documents (SEDs), then you can view the rule differences between the configuration files.

When you compare normalized configurations, the color of the text indicates the following rules:

- 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.

1. Click the **Risks** tab.
2. On the navigation menu, click **Configuration Monitor**.
3. Double-click any device to view the detailed configuration information.
4. Click **History** to view the history for this device.
5. Select a primary configuration.
6. Click **Mark for Comparison**.
7. From the navigation menu, select **All Devices** to return to the device list.
8. Double-click the device to compare and click **History**.
9. Select another configuration backup to compare with the marked configuration.
10. Click **Compare with Marked**.
11. Optional. To view the raw configuration differences, click **View Raw Comparison**.

    If the comparison is for a configuration file or another backup type, then the raw comparison is displayed.

RELATED DOCUMENTATION

Use Case: View Network Paths in the Topology | 18

Use Case: View Network Paths in the Topology

IN THIS SECTION

The topology in JSA Risk Manager displays a graphical representation of your network devices.

A topology path search can determine how your network devices are communicating and the network path that they use to communicate. Path searching allows JSA Risk Manager to visibly display the path between a source and destination, along with the ports, protocols, and rules.

You can view how devices communicate, which is important on secured or restricted access assets.

Key features include:

- Ability to view communications between devices on your network.
- Use filters to search the topology for network devices.
- Quick access to view device rules and configuration.
- Ability to view events that are generated from a path search.

Searching the Topology

Topology search is used to filter your network topology view, and zone in on network paths, hosts, subnets, and other network elements. Investigate various elements of your network infrastructure by using topology search.

A path search is used to filter the topology model. A path search includes all network subnets that contain the source IP addresses or CIDR ranges and subnets that contain destination IP addresses or CIDR ranges that are also allowed to communicate by 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.

1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. From the **Search** list box, select **New Search**.
4. In the **Search Criteria** pane, select **Path**.
5. In the **Source IP/CIDR** field, type the IP address or CIDR range on which you want to filter the topology model. Separate multiple entries by using a comma.
6. In the **Destination IP/CIDR** field, type the destination IP address or CIDR range on which you want to filter the topology model. Separate multiple entries by using a comma.
7. Optional: From the **Protocol** list, select the protocol that you want to use to filter the topology model.

8. Optional: In the **Destination Port** field, type the destination port on which you want to filter the topology model. Separate multiple ports by using a comma.
9. Optional: Select a protocol from the **Protocol** menu.
10. Optional: Type a destination port.
11. Optional: Click **Select Applications**.
    a. From the **Device Adapter** menu, select the device adapter type.
    b. Type a partial or full search term or leave the **Application Name** field empty, and then click **Search**.
    c. Select any of the displayed applications in the **Search Results** field, and click **Add** to add your selections to the **Selected Items** box.
    d. Click **OK**.
12. Optional: Click **Select Vulnerabilities**.
    a. From the **Search By** menu, select the vulnerability category.
    b. In the **Field** beside the **Search By** menu, enter the ID number of the vulnerability.
    c. Click **Search**.
    d. Select any of the displayed vulnerabilities in the **Search Results** field, and then click **Add** to add your selections to the **Selected Items** box.
    e. Click **Save**.

    If your topology includes an Intrusion Prevention System (IPS), the vulnerabilities search option is displayed. For more information, see the *Juniper Secure Analytics Risk Manager User Guide*.
13. Optional: Click **Select Users/Groups**.
    a. Type a partial or full search term or leave the **User/Group Name** field empty, and then click **Search**.
    b. Select the user or group name in the **Search Results** field, and then click **Add** to add your selections to the **Selected Items** box.
    c. Click **OK**, and then click **Search**.
14. Click **Search** to view the results.

RELATED DOCUMENTATION

Use Case: Device Configuration Audit | 15

4

CHAPTER

Use Case: Monitor Policies

Use Case: Monitor Policies

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:

- "Use Case: Assess Assets That Have Suspicious Configurations" on page 24
- "Use Case: Assess Assets with Suspicious Communication" on page 25
- "Use Case: Monitor Policies for Violations" on page 26
- "Risk Priority by Vulnerability" on page 28

Use Policy Monitor to define tests that are based on the risk indicators, and then restrict the test results to filter the query for specific results, violations, protocols, or vulnerabilities.

JSA Risk Manager includes several Policy Monitor questions that are grouped by PCI category. For example, PCI 1, PCI 6, and PCI 10 questions. Questions can be created for assets or devices and rules to expose network security risk. After a question about an asset or a device/rule is submitted to Policy Monitor, the returned results specify the level of risk. You can approve results that are returned from assets or define how you want the system to respond to unapproved results.

Policy Monitor provides the following key features:

- Predefined Policy Monitor questions to assist with workflow.
- Determines if users used forbidden protocols to communicate.
- 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 as a result of device configuration.
- Help identifying compliance issues.

Use Case: Assess Assets That Have Suspicious Configurations

IN THIS SECTION

Organizations use corporate security policies to define risks and the communications that are allowed between assets and networks. To assist with compliance and corporate policy breaches, organizations use Policy Monitor to assess and monitor risks that might be unknown.

PCI compliance dictates that you identify devices that contain cardholder data, then diagram, verify communications, and monitor firewall configurations to protect assets that contain sensitive data. Policy Monitor provides methods for quickly meeting these requirements and allows administrators to adhere to corporate policies. Common methods of reducing risk include identifying and monitoring assets that communicate with unsecured protocols. These are protocols such as routers, firewalls, or switches that allow FTP or telnet connections. Use Policy Monitor to identify assets in your topology with risky configurations.

PCI section 1 questions might 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 that contain protected assets.

Assessing Devices That Allow Risky Protocols

Use Policy Monitor to assess devices that allow risky protocols.

JSA Risk Manager evaluates a question and displays the results of any assets, in your topology, that match the test question. Security professionals, administrators, or auditors in your network can approve communications that are not risky to specific assets. They can also create offenses for the behavior.

1. Click the **Risks** tab.

2. On the navigation menu, click **Policy Monitor**.
3. From the Group list box, select **PCI 1**.
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**.
5. Click **Submit Question**.

RELATED DOCUMENTATION

Use Case: Assess Assets with Suspicious Communication | 25
Use Case: Monitor Policies for Violations | 26
Risk Priority by Vulnerability | 28

Use Case: Assess Assets with Suspicious Communication

IN THIS SECTION

Use Policy Monitor to identify PCI section 10 compliance by tracking, logging, and displaying access to network assets.

JSA Risk Manager can help to identify PCI section 10 compliance by identifying assets in the topology that allow questionable or risky communications. JSA Risk Manager can examine these assets for actual communications or possible communications. Actual communications display assets that used your question criteria to communicate. Possible communications display assets that can use your question criteria to communicate.

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.

Finding Assets That Allow Communication

You can find assets that allow communication from the Internet.

JSA 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 don't represent risk in your network. As more events are generated, you can create offenses in JSA to monitor this type of risky communication.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the Group list, select **PCI 10**.
4. Select the test question **Assess any inbound connections from the Internet to anywhere on the internal network**.
5. Click **Submit Question**.

RELATED DOCUMENTATION

Use Case: Monitor Policies for Violations | 26

Risk Priority by Vulnerability | 28

Use Case: Assess Assets That Have Suspicious Configurations | 24

Use Case: Monitor Policies for Violations

IN THIS SECTION

JSA Risk Manager can continuously monitor any predefined or user-generated question in Policy Monitor. You can use monitor mode to generate events in JSA Risk Manager.

When you select a question to be monitored, JSA Risk Manager analyzes the question against your topology every hour to determine if an asset or rule change generates an unapproved result. If JSA Risk Manager detects an unapproved result, an offense can be generated to alert you about a deviation in your defined policy. In monitor mode, JSA Risk Manager can simultaneously monitor the results of 10 questions.

Question monitoring provides the following key features:

- Monitor for rule or asset changes hourly for unapproved results.
- Use your high and low-level event categories to categorize unapproved results.
- Generating offenses, emails, syslog messages, or dashboard notifications on unapproved results.
- Use event viewing, correlation, event reporting, custom rules, and dashboards in JSA.

Configuring a Question

You can use Policy Monitor to configure a question to be monitored.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. Select the question that you want to monitor.
4. Click **Monitor**.
5. Configure any of the options that you require to monitor your question.
6. Click **Save Monitor**.

Monitoring is enabled for the question and events or offenses are generated based on your monitoring criteria.

RELATED DOCUMENTATION

Risk Priority by Vulnerability | 28

Use Case: Assess Assets That Have Suspicious Configurations | 24

Use Case: Assess Assets with Suspicious Communication | 25

Risk Priority by Vulnerability

IN THIS SECTION

Vulnerabilities that are detected on your assets can be prioritized by their network location or a connection to another device that is vulnerable.

JSA Risk Manager uses asset information and vulnerability information in policy monitor. This information is used to determine whether your assets are susceptible to input type attacks, such as; SQL injection, hidden fields, and *clickjacking.*

Vulnerability 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 or denial of service.

Finding Assets with Specific Vulnerabilities

JSA Risk Manager evaluates a question and displays the results of assets that contain your vulnerability.

Security professionals, administrators, or auditors can identify assets in your network that contain known SQL injection vulnerabilities. They can promptly patch any assets that are connected to a protected network. As more events are generated, you can create events or offenses in JSA to monitor assets that contain SQL injection vulnerabilities.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Group** list, select **Vulnerability**.
4. Select the test question **Assess assets with SQL injection vulnerabilities on specific localnet(s) (i.e. protected server network)**.
5. Click **Submit Question**.

RELATED DOCUMENTATION

5
CHAPTER

Use Cases for Simulations

Use Case: Simulate Attacks on Network Assets

IN THIS SECTION

You can use a simulation to test your network for vulnerabilities from various sources.

You can use attack simulations to audit device configurations in your network.

Simulations 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.

Creating a Simulation

You can create a simulation for an network attack on an SSH protocol.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation >Simulations**.
3. From the **Actions** list, select **New**.
4. Type a name for the simulation.
5. Select **Current Topology**.
6. Select the **Use Connection Data** check box.
7. From the **Where do you want the simulation to begin** list, select an origin for the simulation.
8. Add the simulation attack, **Attack targets one of the following open ports using protocols**.
9. For this simulation, click **open ports**, and then add port 22.

10. Click **protocols**, and then select **TCP**.

    SSH uses TCP.

11. Click **OK**.

12. Click **Save Simulation**.

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

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

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 the connections that the attack could 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.

RELATED DOCUMENTATION

Use Case: Simulate the Risk Of Network Configuration Changes | 32

Use Case: Simulate the Risk Of Network Configuration Changes

IN THIS SECTION

You can use a topology model to define virtual network models based on your existing network. You can create a network model that is based on a series of modifications that can be combined and configured.

You can use a topology model to determine the effect of configuration changes on your network using a simulation.

Topology 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.
2. Simulate an attack against the topology model.

Creating a Topology Model

You can create a topology model to test network changes and simulate attacks.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulations > Topology Models**.
3. From the **Actions** list, select **New**.
4. Type a name for the model.
5. Select any modifications you want to apply to the topology.
6. Configure the tests added to the **Configure model as follows** pane.
7. Click **Save Model**.

Create a simulation for your new topology model.

Simulating an Attack

You can simulate an attack on ports and protocols.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation >Simulations**.
3. From the **Actions** list box, select **New**.
4. Type a name for the simulation.
5. Select a topology model that you created.
6. From the **Where do you want the simulation to begin** list, select an origin for the simulation.
7. Add the simulation attack, **Attack targets one of the following open ports using protocols**.
8. For this simulation, click **open ports**, and then add port 22.
9. Click **protocols**, and then select TCP.

   SSH uses TCP.
10. Click **OK**.
11. Click **Save Simulation**.
12. From the **Actions** list, select **Run Simulation**.

    The results column contains a list box with the date the simulation was run and a link to view the results.
13. Click **View Results**.

RELATED DOCUMENTATION

Use Case: Simulate Attacks on Network Assets | 31