Positive Technologies MaxPatrol

Contents

Positive Technologies MaxPatrol

You can add a Positive Technologies MaxPatrol scanner to your IBM® Security QRadar® deployment.

At intervals that are determined by a scan schedule, QRadar imports XML file results that contain MaxPatrol vulnerabilities. The MaxPatrol scanner imports files from a remote server that contains the exported scan data.

The following table provides Positive Technologies MaxPatrol scanner details:

Table 1-1. Positive Technologies MaxPatrol Scanner details

Vendor	Positive Technologies
Scanner name	MaxPatrol
Supported versions	V8.24.4 and later

Use the following procedures to integrate Positive Technologies MaxPatrol with QRadar

1. Configure your Positive Technologies MaxPatrol scanner to export scan reports. Enable the QRadar compatible XML file vulnerability exports. To obtain the necessary files and configuration procedures, contact Positive Technologies Customer Support.
2. On your QRadar Console, add a Positive Technologies MaxPatrol scanner.
3. On your QRadar Console, create a scan schedule to import scan result data.

Adding a Positive Technologies MaxPatrol scanner

Add a Positive Technologies MaxPatrol scanner to your IBM Security QRadar deployment.

Before you begin

Ensure that the following prerequisites are met: .

- the Positive Technologies MaxPatrol system is configured to export QRadar compatible XML vulnerability reports.
- An SFTP or SMB share is set up and contains .

About this task

The following table describes Positive Technologies MaxPatrol scanner parameters when you select SFTP as the import method:

Table 1-2. Positive Technologies MaxPatrol scanner SFTP properties

Parameter	Description
Remote Hostname	The IP address or host name of the server that has the scan results file.
Login Username	The user name that QRadar uses to log in to the server.

Table 1-2. Positive Technologies MaxPatrol scanner SFTP properties (continued)

Parameter	Description
Enable Key Authentication	Specifies that QRadar authenticates with a key-based authentication file.
Remote directory	The location of the scan result files.
Private Key File	The full path to the file that contains the private key. If a key file does not exist, you must create the `vis.ssh.key` file.
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The `.*\.xml` pattern imports all XML files in the remote directory.

The following table describes Positive Technologies MaxPatrol scanner parameters when you select SMB Share as the import method:

Table 1-3. Positive Technologies MaxPatrol scanner SMB Share properties

Parameter	Description
Hostname	The IP address or host name of the SMB Share.
Login Username	The user name that QRadar uses to log in to SMB Share.
Domain	The domain that is used to connect to the SMB Share.
SMB Folder Path	The full path to the share from the root of the SMB host. Use forward slashes, for example, `/share/logs/`.
File Name Pattern	The regular expression (regex) required to filter the list of files in the Remote Directory. The `.*\.xml` pattern imports all xml files in the remote directory.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. In the **Scanner Name** field, type a name to identify the Positive Technologies MaxPatrol scanner.
5. From the **Managed Host** list, select the managed host that manages the scanner import.
6. From the **Type** list, select **Positive Technologies MaxPatrol Scanner**.
7. Configure the parameters.
8. Configure a CIDR range for the scanner.
9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.

What to do next

For more information about how to create a scan schedule, see Scheduling a vulnerability scan.

Index

A

P