IBM

Manage Microsoft SCCM scanners

Contents

Chapter 1. Microsoft SCCM scanner overview

IBM® Security QRadar® can import scan reports from Microsoft System Center Configuration Manager (SCCM) scanners.

To integrate an Microsoft SCCM scanner, perform the following steps:

1. On your Microsoft SCCM scanner, configure WMI. See Chapter 2, "WMI enablement on scanner host," on page 3.

2. If automatic updates are not enabled on your QRadar Console, download and install the Microsoft SCCM RPM.

3. On yourQRadar Console, add an Microsoft SCCM scanner. See Chapter 3, "Adding a Microsoft SCCM scanner," on page 5.

4. On your QRadar Console, create a scan schedule to import scan result data. See Scheduling a vulnerability scan.

Chapter 2. WMI enablement on scanner host

Before you can configure a Microsoft SCCM scanner, you must configure your system DCOM settings for each host you want to monitor.

Ensure that the scanner host meets the following conditions:
* You are a member of the Administrators group on that host.
* One the following operating systems is installed:
    – Windows 2000
    – Windows 2003
    – Windows 2008
    – XP
    – Vista software
    – Windows 7

    Note: 32-bit and 64-bit operating systems are supported.
* DCOM is configured and enabled.

    If a firewall is installed on the host or is located between the host and QRadar (such as a hardware or other intermediary firewall), the firewall must be configured to allow DCOM communication. Configure the firewall to allow port 135 to be accessible on the host and allow DCOM ports (random ports above 1024). Depending on the version of Windows that you use, you might also need to configure specific ports to be accessible to DCOM. For more information, see your Windows documentation.
* Windows Management Instrumentation (WMI) is enabled.
* The remote registry service is activated.

For specific instructions about how to configure DCOM and WMI on Windows 2008 and Windows 7, see the documents on the IBM support website:
* Windows 2008 (http://www-01.ibm.com/support/docview.wss?uid=swg21681046)
* Windows 7 (http://www-01.ibm.com/support/docview.wss?uid=swg21678809)

Chapter 3. Adding a Microsoft SCCM scanner

Before you begin

Ensure that WMI is enabled on your scanner host.

Procedure

1. Click the **Admin** tab.
2. Click the **VA Scanners** icon.
3. Click **Add**.
4. Configure the following Microsoft SCCM parameters:

Parameter	Description
Scanner Name	The name to identify your scanner instance.
Managed Host	The managed host from your QRadar deployment that manages the scanner import.
Type	Microsoft SCCM
Host Name	The IP address or host name of the remote server that hosts the scan result files.
Domain	The domain used to connect to the remote server.

5. Configure the remaining parameters.
6. To configure a CIDR range for your scanner:
    a. Type the CIDR range that you want this scanner to consider or click **Browse** to select a CIDR range from the network list.
    b. Click **Add**.
7. Click **Save**.

Index

M
Microsoft SCCM   1
    adding   5

O
overview   1