FireEye

The FireEye DSM for IBM Security QRadar SIEM accepts rsyslog events in Log Event Extended Format (LEEF).

This DSM applies to FireEye CMS, MPS, eMPS, and MA appliances. QRadar records all relevant notification alerts that are sent by FireEye appliances.

The following table identifies the specifications for the FireEye DSM.

Table 1. FireEye DSM specifications

Specification	Value
Manufacturer	FireEye
DSM name	FireEye MPS
Supported versions	CMS, MPS, eMPS. and MA v5.1 patch level 5
RPM file name	DSM-FireEyeMPS-*QRadar_release-Build_number*.noarch.rpm
Protocol	Syslog
QRadar recorded event types	All relevant events
Auto discovered?	Yes
Includes identity?	No
More information	FireEye website (www.fireeye.com)

To integrate FireEye with QRadar®, use the following procedures:

1. If automatic updates are not enabled, download and install the FireEye MPS RPM on your QRadar Console.
2. For each instance of FireEye in your deployment, configure the FireEye system to forward events to QRadar.
3. For each instance of FireEye, create an FireEye log source on the QRadar Console.

Configuring your FireEye system for communication with QRadar

To enable FireEye to communicate with QRadar, you must configure your FireEye appliance to forward syslog events.

About this task

Procedure

1. Log in to the FireEye appliance using the CLI.
2. To activate configuration mode, type the following commands:

   ```
   enable
   configure terminal
   ```
3. To enable rsyslog notifications, type the following command:

   ```
   fenotify rsyslog enable
   ```

4. To add QRadar as an rsyslog notification consumer, type the following command:

   ```
   fenotify rsyslog trap-sink QRadar
   ```

5. To specify the IP address for the QRadar system that you want to receive rsyslog trap-sink notifications, type the following command:

   ```
   fenotify rsyslog trap-sink QRadar address QRadar_IP_address
   ```

6. To define the rsyslog event format, type the following command:

   ```
   fenotify rsyslog trap-sink QRadar prefer message format leef
   ```

7. To save the configuration changes to the FireEye appliance, type the following command:

   ```
   write memory
   ```

Configuring a FireEye log source in QRadar

QRadar automatically creates a log source after your QRadar Console receives FireEye events. If QRadar does not automatically discover FireEye events, you can manually add a log source for each instance from which you want to collect event logs.

About this task

Procedure

1. Log in to QRadar
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **FireEye**.
7. Using the P**rotocol Configuration** list, select **Syslog**.
8. In the **Log Source Identifier** field, type the IP address or host name of the FireEye appliance.
9. Configure the remaining parameters.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.