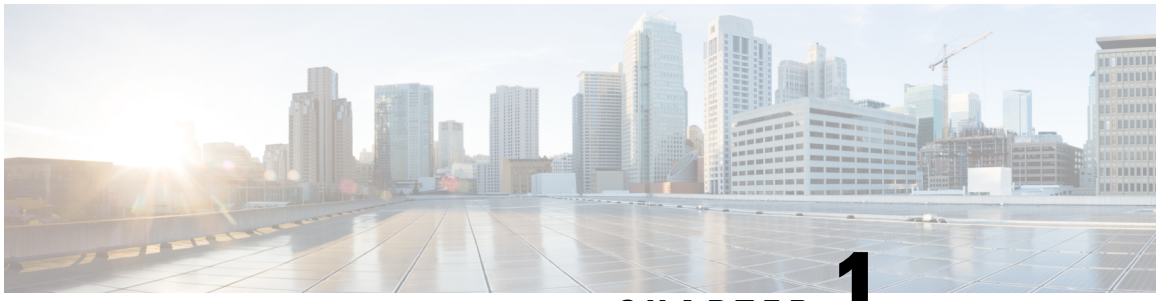
Integration Guide for the Cisco Firepower App for IBM QRadar

First Published: 2020-02-12

Last Modified: 2020-03-10

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Overview

Introduction to the Cisco Firepower App for IBM QRadar

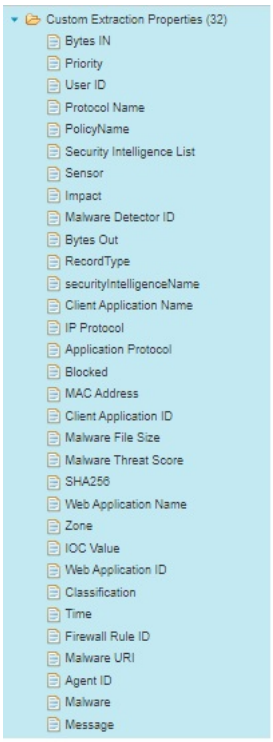
The Cisco Firepower App for IBM QRadar helps you analyze and contain threats to your network by providing insight from multiple security products in QRadar.

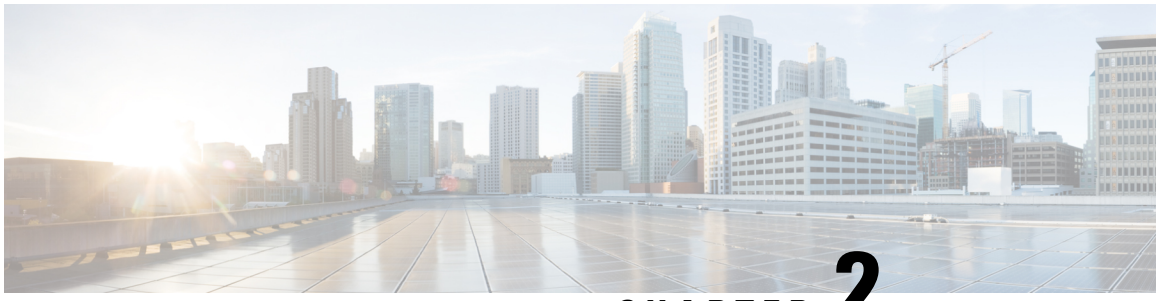
The QRadar Security Information and Event Management (SIEM) tool provides anomaly detection, incident forensics, and vulnerability management.

After you set up the app, you can view event data from your Firepower system in graphical form in the QRadar console.

DSM Custom Field Properties

The following fields are part of the DSM:


Custom Extraction Properties (32)
Bytes IN
Priority
User ID
Protocol Name
PolicyName
Security Intelligence List
Sensor
Impact
Malware Detector ID
Bytes Out
RecordType
securityIntelligenceName
Client Application Name
IP Protocol
Application Protocol
Blocked
MAC Address
Client Application ID
Malware File Size
Malware Threat Score
SHA256
Web Application Name
Zone
IOC Value
Web Application ID
Classification
Time
Firewall Rule ID
Malware URI
Agent ID
Malware
Message



CHAPTER 2

Install and Setup

Requirements and Prerequisites

- Firepower 6.0 or greater

  Available functionality depends on your Firepower version.

- You must have Administrator user role in your Firepower system
- If you are running the old version 1.0 single dashboard version of the app, remove it from your QRadar platform before installing the new app.
- IBM QRadar version 7.3.1 patched to 73120181123182336 and above.
- PROTOCOL-CiscoFirepowerEstreamer-7.3-20191007145706.noarch and above
- DSM-CiscoFireSIGHTManagementCenter-7.3-20170427133206.noarch and above

(The last two items above are available as downloads from the QRadar platform.)

Get the App

Download the app from https://www.ibm.com/security/community/app-exchange.

Install the App

Before you begin

If you are running the old version 1.0 single dashboard version of the app, remove it from your QRadar platform before installing this version of the app.

Procedure

Step 1 Sign in to QRadar.

Step 2 Go to the **Admin** tab.

Step 3 Select **Extension Management Services**.

Step 4 Install the application as a QRadar Plugin (follow the standard QRadar plug-in instructions.)

Step 5 After the installation, if there are changes, deploy them in QRadar.

Import an FMC Certificate into QRadar

Establish a trust relationship between QRadar and your Firepower Management Center by downloading the PKCS certificate for your FMC and installing it in QRadar.

Procedure

Step 1 Sign in to your Firepower Management Center.

Step 2 Choose **Objects** > **Object Management**.

Step 3 Expand the **PKI** node, and choose **Internal CAs**.

Step 4 Next to the Firepower Management Center's certificate, click the edit button.

Step 5 Click **Download**.

Step 6 Enter an encryption password in the **Password** and **Confirm Password** fields.

Step 7 Click **OK**.

Step 8 Upload the certificate to QRadar using the following command:

```
/opt/qradar/bin/estreamer-cert-import.pl -f <pkcs12_absolute_filepath> options
```

Example:

```
[root@VM199-22 ~]# /opt/qradar/bin/estreamer-cert-import.pl -f yourCertificate.pkcs12 -o 61estre
Successfully generated truststore file [/opt/qradar/conf/61estreamer.truststore].
Successfully generated keystore file [/opt/qradar/conf/61estreamer.keystore].
```

Configure a Log Source

Procedure

Step 1 From the **Admin** tab on the QRadar navigation bar, scroll down to **Log Sources**.

Step 2 Click **Add** to create a new log source.

Step 3 Enter the required parameters for creating the log source:

Option	Value
Log Source Name	Enter a name that uniquely identifies this log source.
Log Source Type	Cisco FireSIGHT Management Center
Protocol Configuration	Cisco Firepower eStreamer
Server Address	IP address or host name of your Firepower Management Center
Server Port	Port number on which your Firepower Management Center is configured to accept connection requests. The default port that QRadar uses for the Firepower Management Center is 8302.
Keystore Filename	he directory path and file name for the keystore private key and associated certificate. By default, the import script creates the keystore file in the following directory: /opt/qradar/conf/estreamer.keystore
Truststore Filename	The directory path and file name for the truststore files. The truststore file contains the certificates that are trusted by the client. By default, the import script creates the truststore file in the following directory: /opt/qradar/conf/estreamer.truststore
Request Extra Data	Select this option to request intrusion event extra data from the Firepower Management Center. For example, extra data includes the original IP address of an event.
Domain	The domain from which the events are streamed.
Log Source Extension	Select “SourcefireDefenseCenter_ext” from the list.

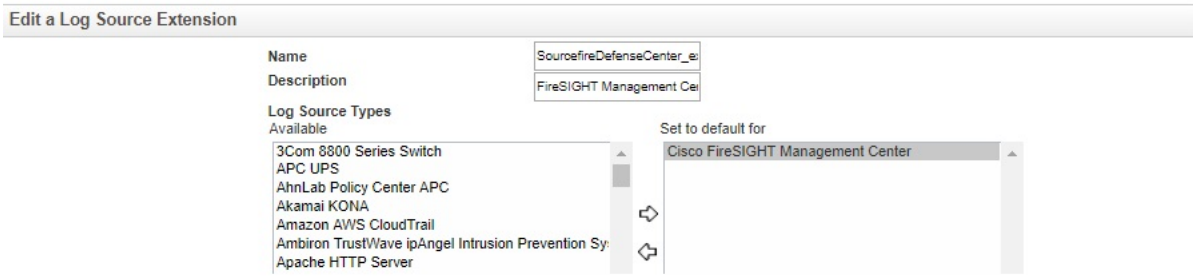
Step 4 Save.

Step 5 Deploy changes in QRadar.

Configure the Log Source Extension

Procedure

Step 1 If Extension Name is not mapped to the Log source type FireSIGHT Management Center, choose it:



Step 2 Save.

Index CEPs

For more efficient searches, index the CEPs in this procedure.

Procedure

Step 1 Navigate to **Admin > Index Management**.

Step 2 Select the CEP to be indexed and click **Enable Index**.

Step 3 Save.

Step 4 Index the following fields:

- IOC Value
- User ID
- securityIntelligenceName
- Bytes IN
- RecordType
- Bytes OUT

Distinguish Internal and External Networks

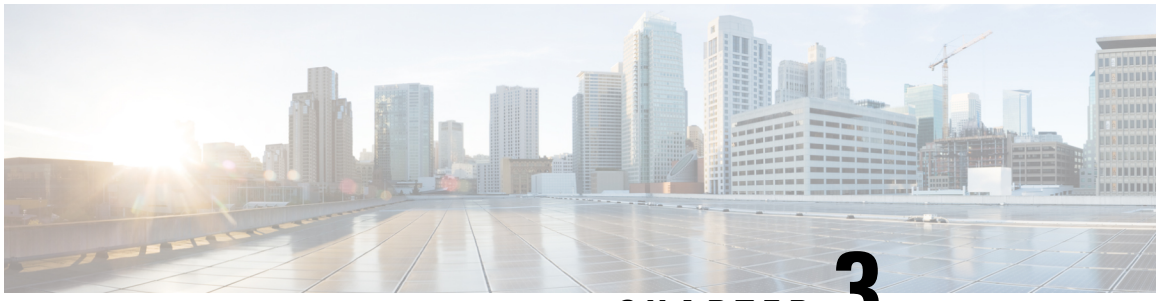
Specify the IP addresses that define your internal and external networks so you can easily identify the threats that originate inside your network.

Procedure

Step 1 In the Homenet settings section:

Step 2 Specify the IP addresses and ranges that define your internal network.

Step 3 Save.



CHAPTER 3

Use the App

Suggested Investigations

- **Confirm that your system is blocking threats that the system has identified:**

  On the Threats > Threat Summary page, filter for threats not blocked, regardless of direction.

  On the Threats > Intrusion Events page, filter for Impact 1 threats not blocked.

- **Look for compromised internal hosts:**

  Attacks initiated by internal hosts always indicate compromise.

  - On the Threats > Intrusion Events page, filter for Impact 3 threats whether or not they were blocked, then click the relevant internal hosts option in the pie chart below the timeline. Investigate the internal IP addresses in the table at the bottom of the page.
  - Then do the same for Impact 2 events.
  - On the Threats > Threat Summary page, filter for Direction originating with internal hosts, whether blocked or not, and investigate internal hosts involved, regardless of whether or not the threats were blocked.

- **Identify hosts affected by malware that entered your network before it was known to be a threat:**

  Identify affected hosts using the retrospective malware events graph on the Threats > Threat Summary page.

- **Look for anomalies on your network, such as unapproved applications or nonstandard ports in use:**

  - Check the graphs on the Network page.
  - Look for activity on uncommon ports, as highlighted on the "Top Server Applications In Use with Least Seen TCP Ports" graph on the Network page.

- **Review the data for for outliers – activity or parameters that are unexpectedly frequently or infrequently seen.**

- **Investigate any unexpected hosts on your network:**

  Level 0 intrusion events without associated host discovery on the network could indicate the presence of a ghost network.

  (Level 0 intrusion events also could indicate that your network discovery policy is not properly implemented.)

- **Look for spikes or trends in high-priority attacks over time or against key hosts (for example, servers):**

  These are easiest to see in the timeline graphs on each page under the Threats menu.

  Select various time ranges to see what stands out.

- **Eliminate large chunks of insignificant data so the important data stands out.**

- **Look carefully at unique events**, which may indicate highly targeted attacks.

- **Drill down on interesting items.**

  As you find patterns, hosts, users, applications, ports, etc. that raise flags, drill down and filter to see what other transactions involve the relevant entities. Also right-click items to see if additional information is available.

- **As you explore, look for any other behavior that could be suspicious.** For example:
  - A single URLis unexpectedly associated with multiple IP addresses and MAC addresses over time.
  - A host has unexpectedly connected to 30 different endpoints in the past hour using SSH.

- **Look for events and data associated with a particular IP address:**

  Use the Threats > Context Explorer page.

  Note If your filter includes many IP addresses, the app may become very slow, depending on how you have your data set up.

- **See also** Intrusion Event Impact Levels, on page 11**.**

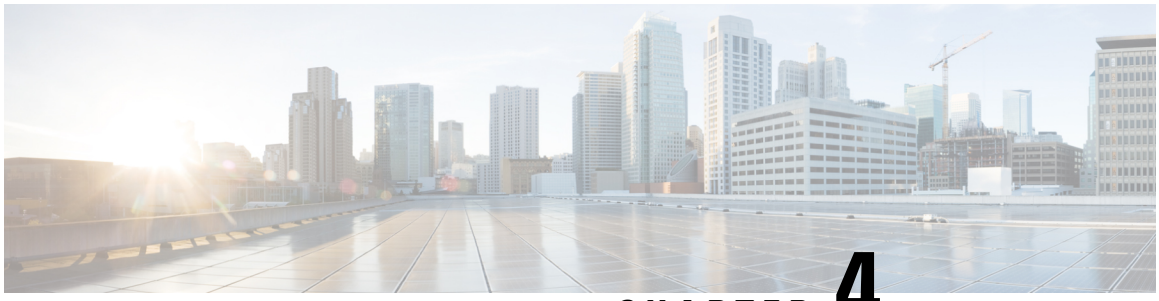
Widget descriptions:

Most of the widgets in this app are the same as their equivalents in the Firepower Management Center. For information about these widgets, see the *Firepower Management Center Configuration Guide* for your version at https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html.

Intrusion Event Impact Levels

Table 1:

Impact Level	Description and Suggested Actions
0	**Unexpected Hosts on the Network** Neither the source nor destination host IP address is within the network as defined in the discovery policy in Firepower Management Center. If your discovery policy is correctly configured, Impact 0 events may indicate unauthorized devices on the network (a ghost network.) Click this impact level and look at the table at the bottom of the page to determine which sensor is seeing this traffic and engage your network team to locate and isolate these devices.
1	**High Priority Intrusion Events** The targeted host is vulnerable to the exploit. These events can be OS, server, or client vulnerabilities, or indications of compromise as defined by Cisco Talos. To see a breakdown of these events by type, see the "Impact 1 – High Priority Events" widget below, or look at the table at the bottom of the page to see a list of at-risk hosts.
2	**Possibly Compromised Hosts** If the exploit originates inside your network, this indicates a compromised host and you should investigate the source IP address. Firepower has not identified a known vulnerability on the destination host to the exploit. However, regardless of the source IP, you should verify that the destination host has not been compromised.
3	**Probably Compromised Hosts** Impact 3 events generally occur only when an internal host is the source of an exploit. An internally-sourced event always indicates a compromised host. Click the relevant widget below to display internally-sourced events in the table at the bottom of the page, then investigate the source IP addresses in that table.
4	**Hosts Not Fully Integrated into the Network** The host is within the expected range of IP addresses as configured in a discovery policy in Firepower Management Center, but has no host profile. The host may be new to your network, for example as part of an acquisition or network buildout that has not yet been properly configured.



CHAPTER 4

More Information

Firepower Information

For information about Firepower (not specific to this integration), see the Firepower Management Center documentation for your version:

- The online help in FMC (Under the Help menu near the top right corner of the browser window.)
- The *Firepower Management Center Configuration Guide* for your version, as HTML or PDF:

  https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html
- Other FMC resources:

  https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

Troubleshooting

This app is provided as-is, with no warranty, and is community-supported. If you have questions, try the followingCisco Communities:

- https://community.cisco.com/t5/security/ct-p/4561-security
- https://cisco.com/go/ngfw-community

Contact Us

Send an email to: fp-qradar-apps@cisco.com