Cisco Firepower App for Splunk User Guide

Revised: April 17, 2019

Welcome

This is the documentation for the Cisco Firepower App for Splunk, available from Splunkbase at https://splunkbase.splunk.com/app/4388/.

Discover and investigate threats using threat and traffic data from Firepower Management Center (FMC). Splunk can store far more data than FMC can, so you have greater visibility into activity on your network.

This app is a significant improvement on the existing Cisco Firepower eNcore App for Splunk (https://splunkbase.splunk.com/app/3663/). You can run both apps in parallel if you choose to do so.

Set Up the App

Requirements, Prerequisites, and Limitations

- Cisco Firepower App for Splunk presents security and network event information sent to Splunk from Firepower Management Center running version 6.0 or later.

  Available functionality is affected by your Firepower version.

- Before you can use this app, your Firepower event data must be in Splunk.

  To bring your Firepower data into Splunk, use the Cisco eStreamer eNcore Add-on for Splunk. This technical add-on (TA) is available from https://splunkbase.splunk.com/app/3662/.

  Documentation for this TA is available from https://www.cisco.com/c/en/us/support/security/defense-center/products-programming-reference-guides-list.html.

- The types of data available for analysis are described at https://splunkbase.splunk.com/app/3662/.

Install

Before you begin

Meet the requirements and prerequisites in Requirements, Prerequisites, and Limitations, on page 2.

Procedure

Step 1 Go to https://splunkbase.splunk.com/app/4388/.

Step 2 Log into Splunk as an Admin.

Step 3 Download the app.

Step 4 Select **Apps > Manage Apps**.

Step 5 Click **Install App from File**.

Step 6 Navigate to the app “Cisco Firepower App for Splunk.”

Step 7 Click **Upgrade app**.

This will do a fresh install if you do not have an existing installed version of this app, or overwrite any previous version.

Step 8 Restart Splunk as instructed.

Best Practices

Configure network settings (specifically, identify your home network) so you can easily identify attacks that originate inside your network.

Configure

At a minimum, you should specify the IP addresses that define your internal and external networks so you can easily see the threats that originate within your network.

Procedure

Step 1 Access the standard Splunk location to configure settings for an app:

a) In the top left corner of the window, select **App: Cisco Firepower App for Splunk > Manage Apps**.
b) In the row for Cisco Firepower App for Splunk, click **Set Up**.

Step 2 Specify the IP addresses and ranges on your internal network, so you can determine exploit direction:

a) In the **Homenet Settings** section:
b) Specify the IP addresses and ranges that define your internal network.

Step 3 Enable the ability to right-click applicable data to quickly pivot to view the data in Firepower Management Center.

For example, host profile information is available only on the FMC.

a) In the **FMC Link** section:
b) Enter the IP address of the FMC management interface.

Step 4 Click **Save**.

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 5**.**

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 Configuration Guide 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.

Troubleshooting

Review Existing Instructions

Verify that you have met requirements and prerequisites described in Set Up the App, on page 2.

Getting Support

This app is provided as-is, with no warranty, and is community-supported. Try the following:

- Cisco communities, for example:
  - https://community.cisco.com/t5/security/ct-p/4561-security
  - https://cisco.com/go/ngfw-community
- Splunk community: Splunk Answers
- Report bugs and request features: fp-4-splunk@cisco.com

Firepower Information

For information about Firepower (not specific to Splunk), 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* 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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.