Netsurion | EventTracker®

How to - Configure CrowdStrike Falcon to forward logs to EventTracker

EventTracker v9.2 and above

Publication Date: August 17, 2020

Abstract

This guide provides instructions to configure CrowdStrike Falcon to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2 or above and **CrowdStrike Falcon**

Audience

Administrators who are assigned the task to monitor CrowdStrike Falcon events using EventTracker.

Table of Contents

1. Overview

CrowdStrike Falcon's next-gen antivirus protects against all types of attacks from commodity malware to sophisticated attacks with one solution — even when offline.

EventTracker helps to monitor events from CrowdStrike Falcon. EventTracker's reports provide detailed information of all events, alerts are helpful to determine and stop the attack and suspicious activities in real-time, and dashboards will help you to analyze all the security-related events in a single console. Also, we can create and save log search rules/queries under the saved search feature for real-time and historical log search.

2. Prerequisites

The **Falcon SIEM Connector** provides users a turnkey, SIEM-consumable data stream. The Falcon SIEM Connector.

- Transforms Falcon Streaming API data into a format that a SIEM can consume
- Maintains the connection to the CrowdStrike Falcon Streaming API and your SIEM
- Manages the data-stream pointer to prevent data loss

Before using the Falcon SIEM Connector, you must contact **support@CrowdStrike Falcon.com** to enable access to the Falcon Streaming API (formerly "Falcon Firehose API"). Learn more about **How to get access to CrowdStrike Falcon APIs.**

The CrowdStrike Falcon SIEM Connector (SIEM Connector) runs as a service on a local Linux server. The resource requirements (CPU/Memory/Hard drive) are minimal. The system can be a VM (Virtual Machine).

- **Credentials:** The Falcon SIEM Connector uses our Streaming API, so you must have a Streaming API key to use the SIEM Connector. Your API credentials apply to your entire account (customer ID), not to an individual user.
- **EventTracker Agent** should be installed in the system.
- **OS:** CentOS/RHEL 6.x-7.x (64-bit)
- **Connectivity:** Internet connectivity and ability to connect the CrowdStrike Falcon Cloud (HTTPS/TCP 443)
- **Communication:** Ability to communicate with syslog listener.
- **Time:** The date and time on the host running the Falcon SIEM Connector must be current (NTP is recommended)

3. Integrating CrowdStrike Falcon with EventTracker

CrowdStrike Falcon logs we can get by using syslog, JSON(default), CEF, and LEEF.

3.1 Reset an API Key

Manage your API key and UUID in **Support > API Key**.
Warning: When you reset your API key, the previous key is invalidated. This affects any existing applications that use the previous key.
1. In the Falcon console, go to Support > API Key.
2. Click Reset API.
3. Copy the API key and UUID to a safe place. The API key is only shown once.

3.2 Default Directories

Installation: /opt/CrowdStrike Falcon
Service script:
-CentOS: /etc/init.d/cs.falconhoseclientd
-Ubuntu: /etc/init/cs.falconhoseclientd
Logs: /var/log/CrowdStrike Falcon/falconhoseclient/

4. Installing the SIEM Connector for a Single CID (Customer ID)

Administrative (root) permissions are required to install and configure the SIEM Connector. Administrative permissions are not required to run the SIEM Connector.

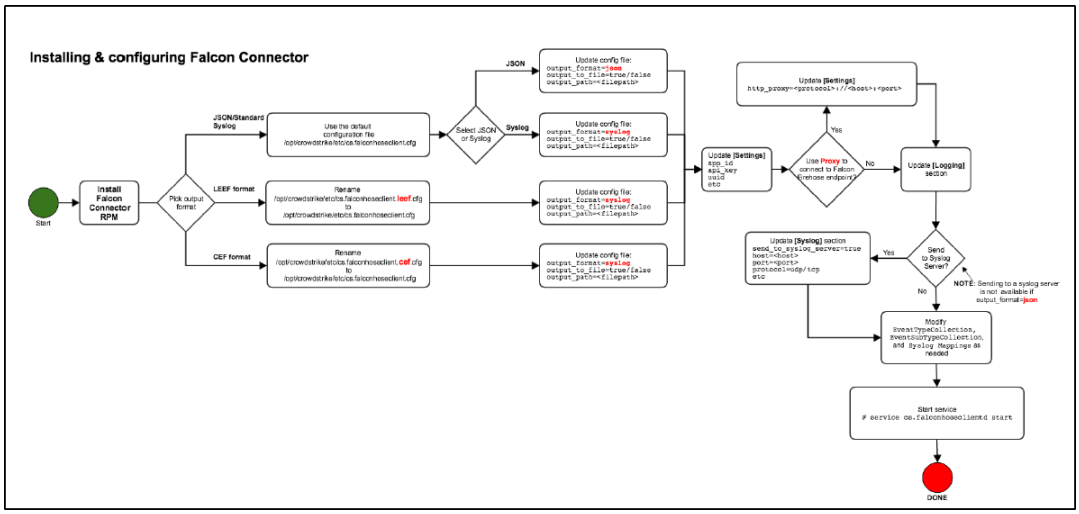

Figure 1

4.1 Downloading the SIEM Connector Installer

- Go to **Support > Tool Downloads.**
- Download the SIEM Connector installer for your operating system:
    1. **CentOS:** Download the latest .rpm installer
    2. **Ubuntu:** Download the latest .deb installer

4.2 Installing the SIEM Connector

- Open a terminal.
- Run the installation command, replacing <installer package> with the installer you downloaded.
    1. **CentOS:** sudo rpm -Uvh <installer package>

        ```
        # sudo rpm -Uvh /path/to/file/cs.falconhoseclient-1.0.70-1.el7.centos.x86_64.rpm
        ```

    2. **Ubuntu:** sudo dpkg -i <installer package>

        ```
        sudo dpkg -i crowdstrike-cs-falconhoseclient_70-siem-release-1.0_amd64.deb
        ```

4.3 Selecting an Output Type

Your output type is defined by which of the sample configuration files you use. The sample configuration files are installed to

- JSON (default)
- Syslog
- Common Event Format (CEF)
- Log Event Extended Format (LEEF)

SYSLOG

1. On your device, edit the file **/opt/CrowdStrike Falcon/etc/cs.falconhoseclient.cfg** in a text editor.
2. Change the value of **output_format** to read:
   output_format: Syslog

4.4 Adding API Credentials to the Configuration File

1. Open **/opt/CrowdStrike/etc/cs.falconhoseclient.cfg** in a text editor.
2. Find the **[Settings]** section.
3. Edit these lines for your environment:
    A. **app_id :** A unique app ID used to label your application. Max: 18 characters.
    B. **api_key :** Your API key, which you can reset at **Support > API Key**.

C. **api_uuid :** Your API UUID, which you can view at **Support > API Key**.

4. Save your changes.
   Do not edit the line for api_url unless you are a Falcon on GovCloud customer. Don't edit the line for the version .

4.5 Syslog Configuration File setting

In the syslog section we must input a few necessary details:

Key	Value	Description
send_to_syslog_server	true	Enable/disable push to the Syslog server. If you do not have a syslog server running, set this to false. Otherwise, the SIEM connector may fail to start.
host	EventTracker's IP Address	Syslog/SIEM host address. It can be IP or hostname. If send_to_syslog_server
port	514	Network port
protocol	UDP	**UDP:** User Datagram Protocol, connectionless transmission model. **TCP:** Transmission Control Protocol, guarantees delivery of data and sequence.

4.6 Configuring SIEM Connector to Your Environment

The rest of the configuration file defines how the SIEM connector formats data from the Streaming API into an appropriate format for your SIEM.
Edit your **/opt/CrowdStrike/etc/cs.falconhoseclient.cfg** file to include the data you want in the format that your SIEM requires.

4.7 Starting the SIEM Connector

After editing the **.cfg file** include the data you want to provide to your SIEM, you are ready to start the SIEM Connector. Run this command at a terminal:
CentOS: sudo service cs.falconhoseclientd start
Ubuntu: sudo start cs.falconhoseclientd