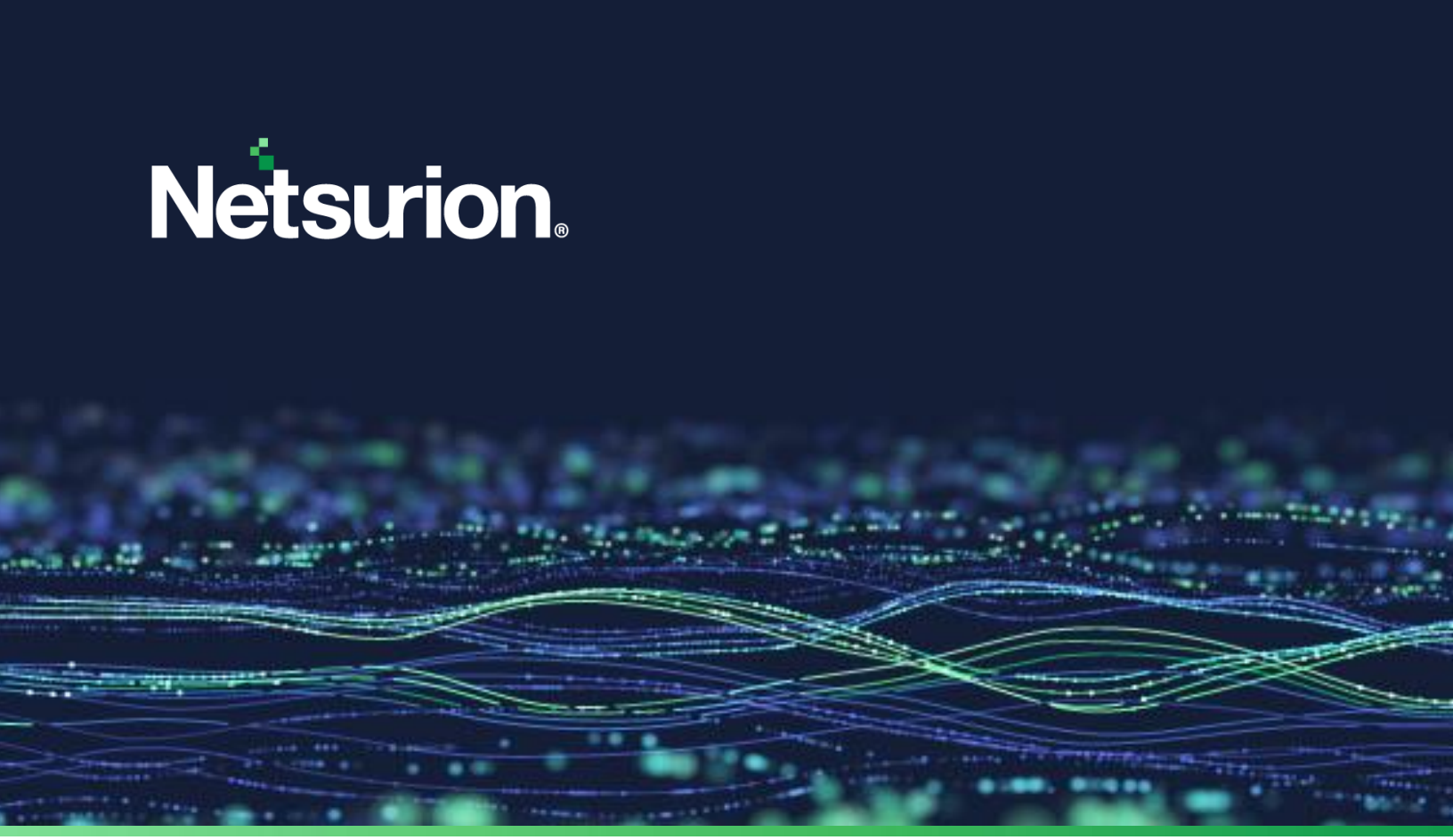


How-To Guide

Integrate CrowdStrike Falcon with Netsurion Open XDR

Publication Date

August 02, 2023

Abstract

This guide provides instructions to configure and integrate CrowdStrike Falcon with Netsurion Open XDR to retrieve its logs via syslog and forward them to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with CrowdStrike Falcon and Netsurion Open XDR 9.3 or later.

Note:

The Falcon SIEM connector used for fetching and sending logs from CrowdStrike to Netsurion Open XDR is provided by CrowdStrike and is being utilized exactly as provided with no modifications.

Audience

This guide is for the administrators responsible for configuring and monitoring CrowdStrike Falcon in Netsurion Open XDR.

Table of Contents

1 Overview

CrowdStrike Falcon is a Security As A Service (SAAS) solution, which provides protection against malware and sophisticated attacks.

Netsurion Open XDR manages logs retrieved from CrowdStrike Falcon. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing any suspicious activities.

2 Prerequisites

- The Falcon SIEM Connector*.

  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, and the system can be a VM (Virtual Machine).

  Benefits of Falcon SIEM Connector

  The Falcon SIEM Connector* provides users with 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.

  Note

  ***Falcon SIEM** Connector is provided by CrowdStrike and Netsurion is not liable for any issues or vulnerabilities identified in the SIEM Connector. Contact CrowdStrike support for the issues or vulnerabilities identified in the Falcon SIEM connector.

  Note

  You can use a proxy to access the SIEM Connector, but you must independently login to the proxy. The SIEM Connector does not handle proxy authentication.

- Authorization of API client with READ permission for Event Stream.

  Note

  Event Stream API is enabled by default for all CrowdStrike CIDs. If your CrowdStrike cloud is US-GOV-1 and your CID doesn't have event streams enabled, or if the status is unknown, contact **CrowdStrike Support** for assistance.

- Must have the OS version CentOS/ RHEL 7.x-8.x (64-bit)
- Internet connectivity and ability to connect the CrowdStrike Falcon Cloud (HTTPS/TCP443)
- Ability to communicate with syslog listeners.

- The Data Source Integration package.

Note

To get the Data Source Integration package, contact your Netsurion Account Manager.

3 System Requirements

Recommended System Specifications

For each customer ID (CID) with a standalone virtual machine (VM) running only the Falcon SIEM Connector, we recommend the following system specifications:

- 8 GB RAM
- 12 GB DISK SPACE
- CPUs

4 Integrating CrowdStrike Falcon with Netsurion Open XDR

IMPORTANT

CrowdStrike Falcon logs uses syslog, JSON (default), CEF, and LEEF format.

4.1 CrowdStrike Default Directories

Installation	/opt/CrowdStrike	
Service Script	**CentOS**	/etc/init.d/cs.falconhoseclientd
	Ubuntu	/etc/init/cs.falconhoseclientd
Logs	/var/log/CrowdStrike Falcon/falconhoseclient/	

4.2 Reset the API Key in CrowdStrike

1. In the **Falcon** console, go to **Support > API Key**.

> **Note**
>
> Manage your API key and UUID in Support > API Key.

2. Click Reset API.

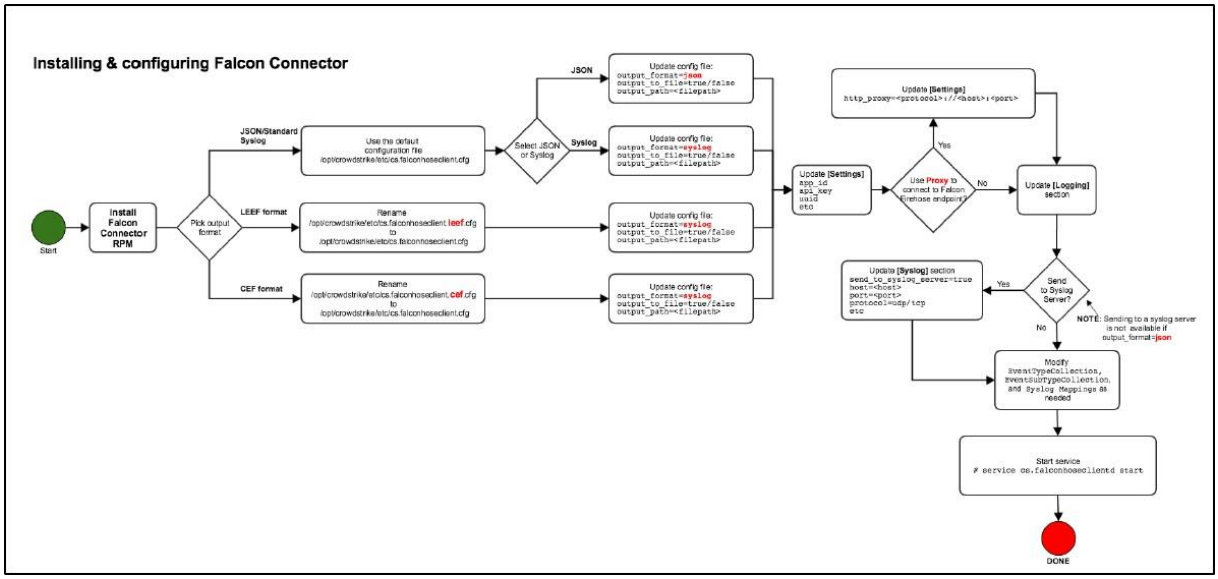
> **WARNING**
>
> When you reset your API key, the previous key is invalidated. This affects any existing application that uses the previous key.

3. Copy the API key and UUID to a safe place. The API key is only shown once.

5 Installing the SIEM Connector For a Single CID (Customer ID)

Administrative (root) permission is required to install and configure the SIEM Connector.

> **Note**
>
> Administrative permission is not required to run the SIEM Connector.



5.1 Downloading SIEM Connector Installer

1. Go to **Support** > **Tool Downloads**.
2. Download the SIEM Connector installer for your operating system.

CentOS	Download the latest .rpm installer
Ubuntu	Download the latest .deb installer

5.2 Installing SIEM Connector

- Open the terminal and run the installation command replacing <**installer package**> with the installer you downloaded.

  CentOS: `sudo rpm -Uvh <installer package>`

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

  Ubuntu: **`sudo dpkg -i <installer package>`**

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

5.3 Selecting the Output Type

The output type is defined by which of the sample configuration files you use. The sample configuration files are installed to /opt/crowdstrike/etc/. You can choose from these output formats:

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

Note

Recommended to use **Syslog**.

To Set the Syslog Format

1. Go to your system and edit the file **/opt/crowdstrike/etc/cs.falconhoseclient.cfg** in a text editor.
2. Change the value of **output_format** to read.

   ```
   output_format: syslog
   ```

5.4 Adding API Credentials to the CrowdStrike Configuration File.

1. In the **Falcon** console, go to **Support and resources** > **Resources and tools** > **API clients and keys**.
2. Create the API client to use with the SIEM connector and note the API Client ID and Client Secret.
3. Open **/opt/crowdstrike/etc/cs.falconhoseclient.cfg** in a text editor
4. Go to the [**Settings**] section.
5. Edit the following lines for your environment:
   - **app_id:** Uniquely identifies your API connection for troubleshooting.

     Max: 32 characters. The following characters are valid: **a-z**, **A-Z** , **0-9**, **.**, **-**, **_**
   - **client_id:** Your API Client ID.
   - **client_secret:** Your API client Secret.

Note

When creating the APIClient, make sure Read access is selected for Event Streams. The **app_id** must be unique to your environment.

6. After providing the details, save your changes.

5.5 Configuring SIEM Connector for 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 **/opt/crowdstrike/etc/cs.falconhoseclient.cfg** file to include the required data in the format that your SIEM requires.

4.6 Syslog configuration file setting

In the syslog section provide the following necessary details:

Key	Value	Description
send_to_syslog_server	true	Enable/ Disable Push in the Syslog server. If you do not have an Asyslog server running, set this to **False**. Otherwise, the SIEM connector may fail to start.
host	Netsurion Open XDR IP Address/ FQDN+	Syslog/ SIEM host address. It can be the IP or Hostname.

Key	Value	Description
		If send_to_syslog_server is true.
port	514	Network port
protocol	UDP	**UDP:** User Datagram Protocol, connectionless transmission model. **TCP:** Transmission Control Protocol, guarantees delivery of data and sequence.

5.6 Start the SIEM Connector

After editing the **.cfg file** include the required data to provide to your SIEM. Run this command at a terminal.

CentOS: `sudo service cs.falconhoseclientd start`

Ubuntu: `sudo systemctl start cs.falconhoseclientd.service`

6 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integration in Netsurion Open XDR.

The Data Source Integration package contains the following files for CrowdStrike Falcon.

- Categories_CrowdStrike Falcon.iscat
- Alerts_CrowdStrike Falcon.isalt
- Templates_CrowdStrike Falcon.ettd
- Reports_CrowdStrike Falcon.etcrx
- KO_CrowdStrike Falcon.etko
- Dashboards_CrowdStrike Falcon.etwd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in Netsurion Open XDR.

6.1 Alerts

Name	Description
CrowdStrike Falcon: Detection summary event	Generated whenever any suspicious activity detected by CrowdStrike Falcon or malware-related event triggers in CrowdStrike Falcon.
CrowdStrike Falcon: File quarantined	Generated whenever files get quarantined by CrowdStrike Falcon.

6.2 Reports

Name	Description
CrowdStrike Falcon - Threat detected	Provides details about threats in a detection summary event as detected by CrowdStrike Falcon.
CrowdStrike Falcon - Quarantined files	Provides details about files quarantined by CrowdStrike Falcon.
CrowdStrike Falcon - Other detected threat	Provides details about miscellaneous threats detected by CrowdStrike Falcon.
CrowdStrike Falcon - AV scan results	Provides details about results from AV scans performed by CrowdStrike Falcon.
CrowdStrike Falcon - Document access	Provides details about access to documents as part of a detection summary by CrowdStrike Falcon.
CrowdStrike Falcon - Authentication details	Provides details about user authentication details as monitored by CrowdStrike Falcon.
CrowdStrike Falcon - Executable written	Provides details about executables in a detection summary by CrowdStrike Falcon.

6.3 Dashboards

Name	Description
CrowdStrike Falcon - Threat detection by file name	Displays various threats based on filename.
CrowdStrike Falcon - Threat detection by signature	Displays threat detected based on signatures.

CrowdStrike Falcon - Threat detection by computer	Displays threats detected based on the computers they were found on.
CrowdStrike Falcon - Threat detection by category	Displays threats based on categories.

6.4 Saved Searches

Name	Description
CrowdStrike Falcon - Detection summary event	Provides details about detection summary events by CrowdStrike Falcon.
CrowdStrike Falcon - Quarantined files	Provides details about files quarantined by CrowdStrike Falcon.
CrowdStrike Falcon - Document access	Provides details about events related to document access as detected by CrowdStrike Falcon.
CrowdStrike Falcon - AV scan results	Provides details about information obtained from AV scans on endpoints monitored by CrowdStrike Falcon.
CrowdStrike Falcon - Authentication details	Provides details about authentication related to CrowdStrike Falcon.
CrowdStrike Falcon - Executable written	Provides details about executables in a detection summary event as discovered by CrowdStrike Falcon.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support