Cisco Secure Network Analytics

Last updated: Jun. 9, 2025

Overview

Cisco Secure Network Analytics (formerly Stealthwatch) is a network detection and response (NDR) solution that provides enterprise-wide visibility, security analytics, and threat detection. Set up data ingestion for Cisco Secure Network Analytics using a data shipper such as the Falcon LogScale Collector.

Use this connector to ingest the following log or event types:

- Network Scanning Alerts

Requirements

CrowdStrike subscription: Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB.

CrowdStrike clouds: Available in US-1, US-2, EU-1, and US-GOV-1.

CrowdStrike access and permissions:

- Administrator or Connector Manager access to the Falcon console for the respective CID.

Vendor requirements:

- Cisco Secure Network Analytics Management Console Administrative Access

System requirements:

- For the Falcon LogScale Collector, see the list of supported operating system versions [https://library.humio.com/falcon-logscale-collector/log-collector-install.html#log-collector-install-compatibility].
- The size of your Falcon LogScale Collector instance depends on workload. See the LogScale Collector sizing guide [https://library.humio.com/falcon-logscale-collector/log-collector-install-sizing.html].

Setup

> **Important:** Some of these steps are performed in third-party products. CrowdStrike does not validate any third-party configurations in customer environments. Perform the following steps with care, and validate your settings and values before finalizing configurations in the Falcon console.

Step 1: Configure and activate the Cisco Secure Network Analytics Data Connector

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. Click **+ Add connection**.
3. In the **Data Connectors** page, filter or sort by **Connector name**, **Vendor**, **Product**, **Connector Type**, **Author**, or **Subscription** to find and select the connector you want to configure.
4. In the **New connection** dialog, review connector metadata, version, and description. Click **Configure**.

   > **Note:** For connectors that are in a **Pre-production** state, a warning dialog appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, enter a name and optional description to identify the connector.
6. Click the **Terms and Conditions** box, then click **Save**.
7. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate the API key, go to **Data connectors > Data connectors > My connectors [/data-connectors/connectors]**, click **Open menu** for the data connector, and click **Generate API key**.
8. Copy and safely store the API key and API URL to use during connector configuration.

   > **Important:** Record your API key somewhere safe as it displays only once during connector setup.

Step 2: Configure your data shipper

You can use any data shipper that supports the HEC API [https://library.humio.com/logscale-api/log-shippers-hec.html] to complete this step. We recommend using the **Falcon LogScale Collector**.

1. In the Falcon console, navigate to **Support and resources > Resources and tools > Tool downloads [/support/tool-downloads]**.
2. Install the LogScale Collector based on your operating system. For example, `LogScale Collector for Windows - X64 vx.x.x`.
3. Open the LogScale Collector configuration file in a text editor. For file location, see Create a configuration - Local [https://library.humio.com/falcon-logscale-collector/log-collector-config.html#log-collector-config-editing-local].
4. Edit the `config.yaml` file. Examples of configuration files for syslog servers:

   - Linux

```
dataDirectory: /var/lib/humio-log-collector
sources:
  syslog_udp_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

- Windows

```
dataDirectory: C:\ProgramData\LogScale Collector\
sources:
  syslog_port_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

- Mac

```
dataDirectory: /var/local/logscale-collector
sources:
  syslog_port_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio

sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

5. Verify the `sources` and `sinks` sections are correct.

- Check that no other services are listening on port 514. For example, this command is commonly used to check for listening ports on Linux:

```
sudo netstat -lpn
```

  - If port 514 is not available, select a different port and confirm it is not in use. Update the `port` number.
  - If you're configuring multiple sources in the same configuration file, each sink must have a distinct port. For example, you cannot have two Humio sinks listening on port 514.

- Check the local firewall and confirm that the configured port is not being blocked.

> **Important:** For Windows Firewall, add the LogScale Collector to your traffic allowlist.

- Add the `token` and `url` generated during data connector setup. Remove `/services/collector` from the end of the `url`.

6. Save and exit the `config.yaml` file.

7. Restart the Falcon LogScale Collector.

- For Linux, run this command in your terminal:

```
sudo systemctl start humio-log-collector
```

- For Windows, look for **Services** from the search bar, open **Services**, find **Humio Log Collector** and right-click **Restart**.

- For Mac, run this command in your terminal:

```
sudo launchctl kickstart -k system/com.crowdstrike.logscale-collector
```

Step 3: Configure Cisco Secure Network Analytics administrative settings

1. Log in to the Secure Network Analytics Management Console as an administrator.

2. In the menu bar, click **Configuration > Response Management**.

3. From the Actions section in the Response Management menu, click **Add > Syslog Message**.

4. In the Add Syslog Message Action window, configure the following parameters:

- **Name:** Unique name to identify the action
- **IP Address:** Enter the IP Address of the Falcon LogScale Collector

- **Port:** Enter the port the FLC is listening on
- **Format:** Enter this string:

```
alarm_type="{alarm_type_id}" alarm_desc="{alarm_type_description}"
category="{alarm_category_name}" signature="{alarm_type_name}" alarmStatus="{alarm_status}"
src="{source_ip}" dest="{target_ip}" dest_port="{port}" transport="{protocol}"
details="{details}" start="{start_active_time}" end="{end_active_time}" Alarm_ID="{alarm_id}"
Source_HG="{source_host_group_names}" Target_HG="{target_host_group_names}"
Source_HostSnapshot="{source_url}" Target_HostSnapshot="{target_url}" FC_Name="{device_name}"
FC_IP="{device_ip}" Domain="{domain_id}" vendor_severity="{alarm_severity_name}"
severity_id="{alarm_severity_id}" exporterName="{exporter_hostname}"
exporterIPAddress="{exporter_ip}" exporterInfo="{exporter_label}" targetUser="{target_username}"
targetHostname="{target_hostname}" sourceUser="{source_username}"
```

5. Select **Custom** and click **OK** as the format.
6. Click **Response Management > Rules**.
7. Click **Add** and select **Host Alarm**.
8. Provide a rule name in the **Name** field.
9. Create rules by selecting values from **Type** and **Options**. To add more rules, click . . . For a **Host Alarm**, combine as many possible types in a statement.
10. In **Action**, select the previously-created syslog action for both **Active** and **Inactive** conditions.
    Events will now be forwarded to the Falcon LogScale Collector whenever any predefined condition is satisfied.

Step 4: Verify successful data ingestion

> **Important:** Search results aren't generated until an applicable event occurs. Before verifying successful data ingestion, wait until data connector status is **Active** and an event has occurred. Note that if an event timestamp is greater than the retention period, the data is not visible in search.

Verify that data is being ingested and appears in Next-Gen SIEM search results:

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. In the **Status** column, verify data connection status is **Active**.
3. In the **Actions** column, click **Open** menu ⋮ and select **Show events** to see all events related to this data connection in **Advanced Event Search**.
4. Confirm that at least one match is generated.

If you need to run a manual search, use this query in Advanced Event Search:

```
#Vendor = "cisco" | #repo = "3pi_cisco_secure_network_analytics" | #event.module = "secure-network-
analytics"
```

Data reference

Parser

The default parser recommended to parse incoming data for this data connector is **cisco-securenetworkanalytics**. This parser requires logs in syslog format.

Supported timestamp format: `MMM dd HH:mm:ss` (Assuming UTC)

Example: `Sep 12 14:03:02`

Structure

Syslog headers with KV Pair Messages:

```
<log.syslog.priority>timestamp log.syslog.hostname Secure Network Analytics[]: kv_pair_message
```

Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- Network:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#j0rcmxhx]
- Intrusion_detection:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#k7xn9jc3]
- Network:Connection:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#i0veu97i]

For more information about Next-Gen SIEM events, see Next-Gen SIEM Data Reference [/documentation/page/q1f14b54/next-gen-siem-data] .

‹ Cisco Secure Firewall ASA[/documentation/page/eac0ef68/cisco-secure-firewall-asa] Cisco Umbrella › [/documentation/page/j6601c93/cisco-umbrella]