Integrating Vectra Detect (QUX) Signal into Crowdstrike NGSIEM v1

Version: October 2024

Table of Contents

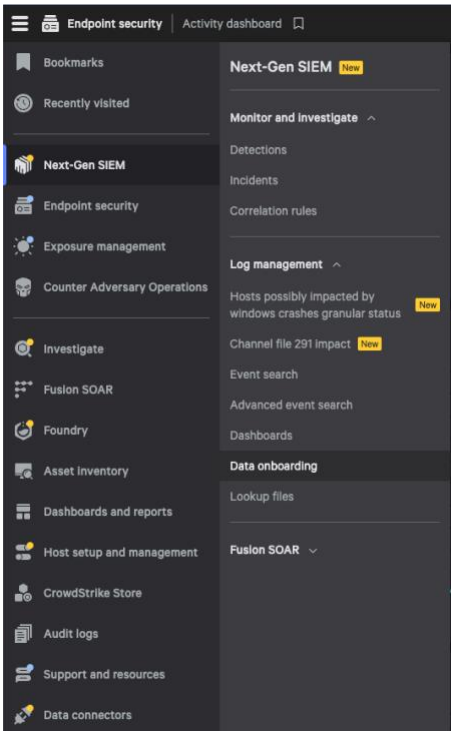
Overview

Integrating **Vectra Detect** data with **CrowdStrike NextGen-SIEM** enables seamless threat detection and enhanced security visibility. This guide outlines the steps required to configure and direct Vectra's log output to CrowdStrike's NG-SIEM platform. By leveraging syslog output directed through a log collector (such as Humio), the data is transmitted to CrowdStrike's NextGen-SIEM using the HEC (HTTP Event Collector) data connector. A custom parser within NG-SIEM processes this data, ensuring that it is accurately parsed and stored in CrowdStrike's NextGen-SIEM environment. This setup allows security teams to monitor Vectra alerts and events within the broader CrowdStrike ecosystem, supporting improved threat correlation and streamlined incident response.

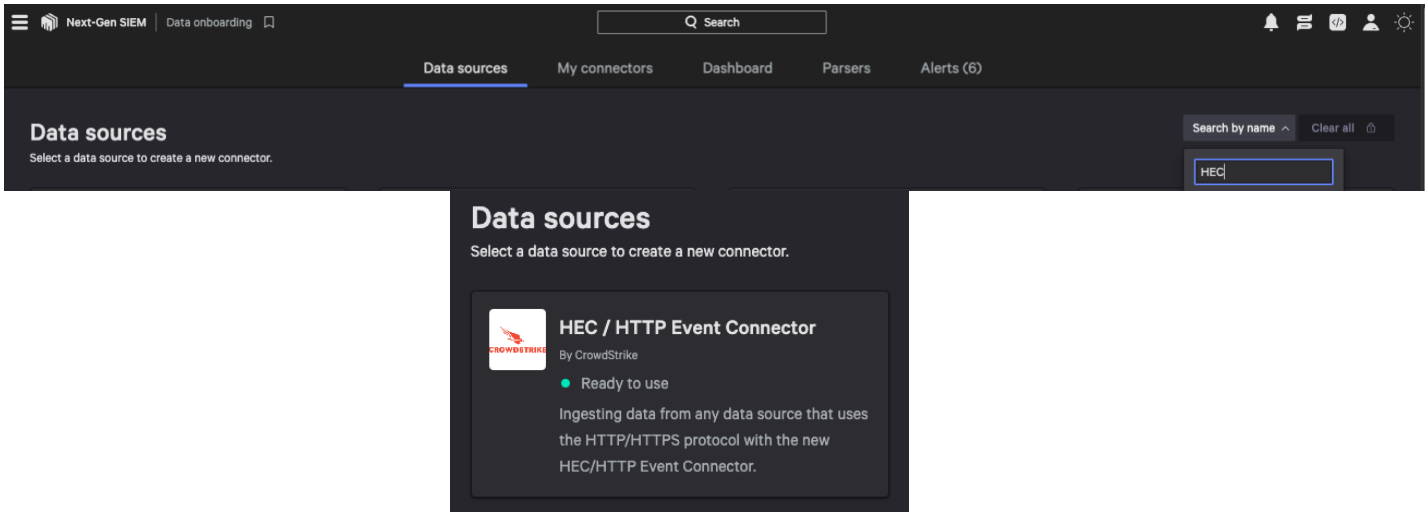
Prior to continuing, please download the required parser (Vectra-Detect-QUX-Oct-31.yaml) from:
https://support.vectra.ai/s/article/KB-VS-1838

Prepare Data Connector

- Login to the Falcon Console and navigate to ***Next-Gen SIEM*** > ***Data onboarding***.

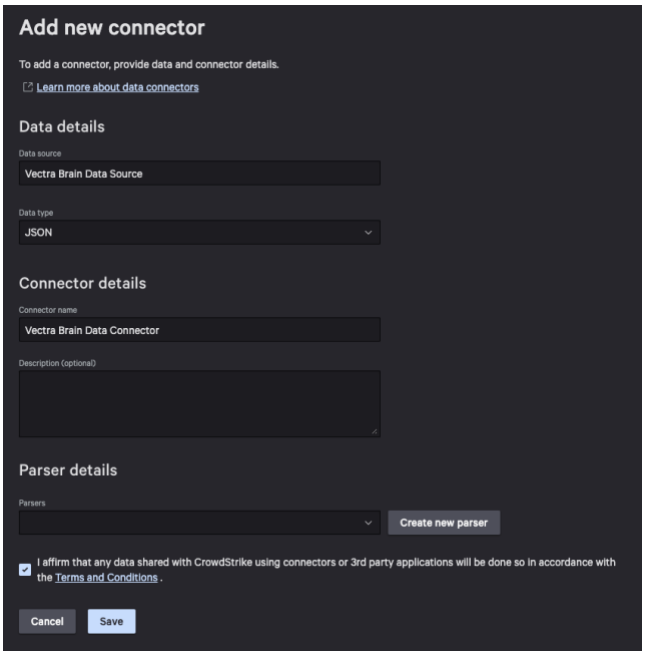


- In the search bar, type ***HEC*** and select it to add a new data connector.

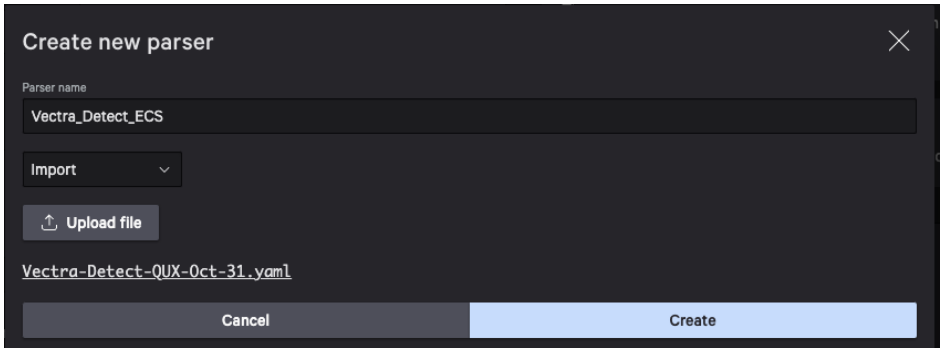


Configure Data Connector

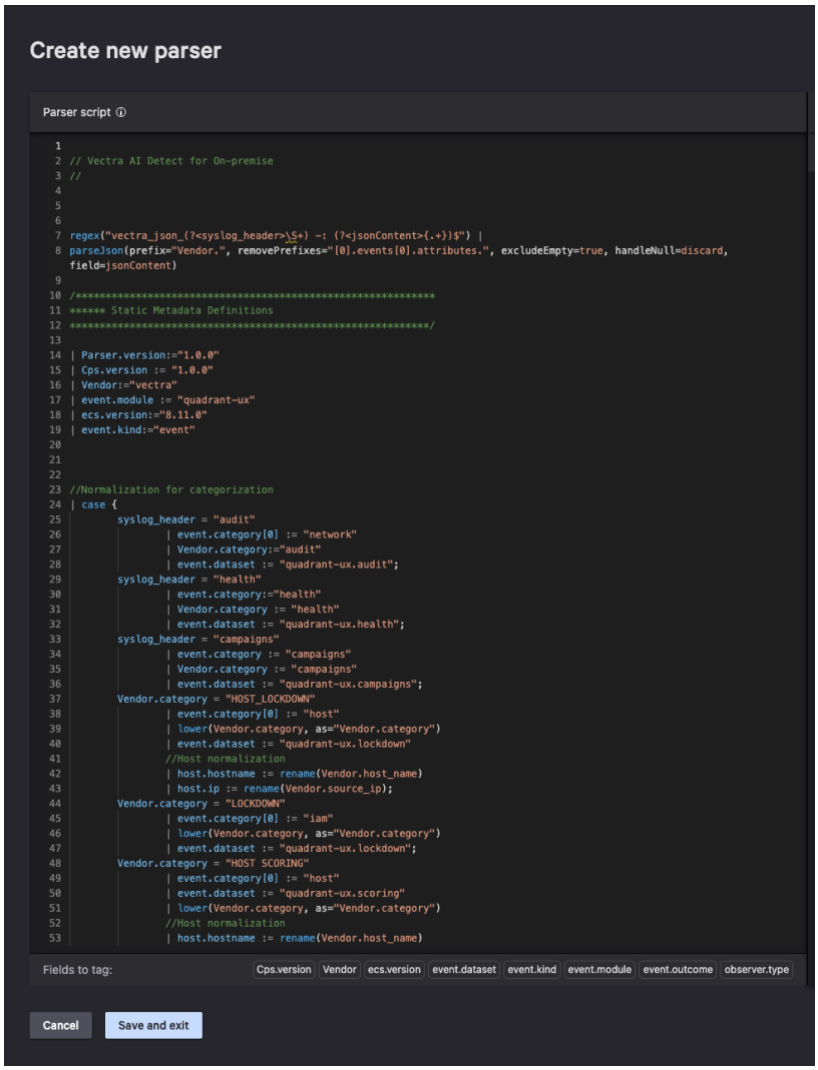
- Provide the details to configure the data connector and then select ***Create new parser.***
  - Data source = friendly name for where the data is coming.
  - Data type = JSON.
  - Connector name = friendly name for the connector processing the data.
  - Description = optional.



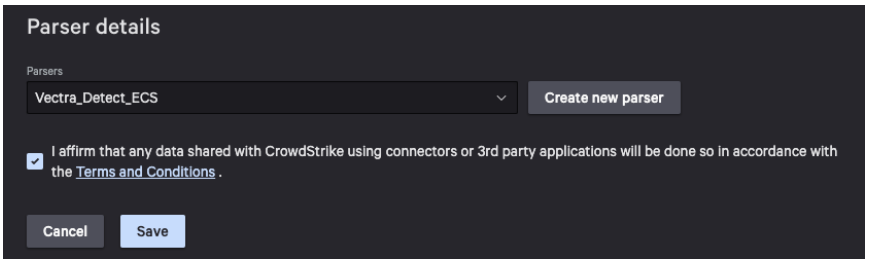
- Provide a name for the parser (example: Vectra_Detect_ECS) and select ***Import*** >***Upload file***. Upload the file (Vectra-Detect-QUX-Oct-31.yaml) that was downloaded from https://support.vectra.ai/s/article/KB-VS-1838.

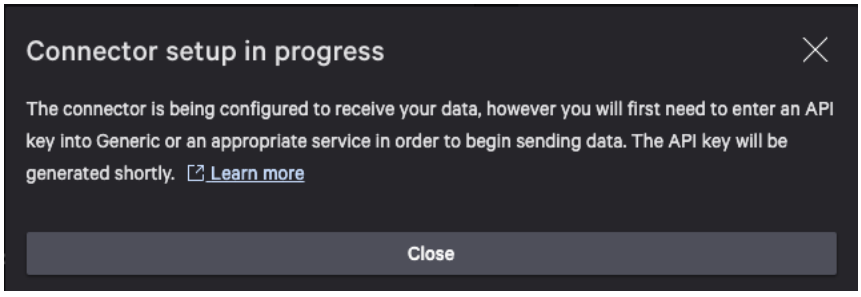


- Once the parser script has loaded select ***Save and exit***.



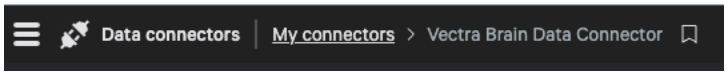
- Select the newly created parser in the dropdown list and click ***Save***.



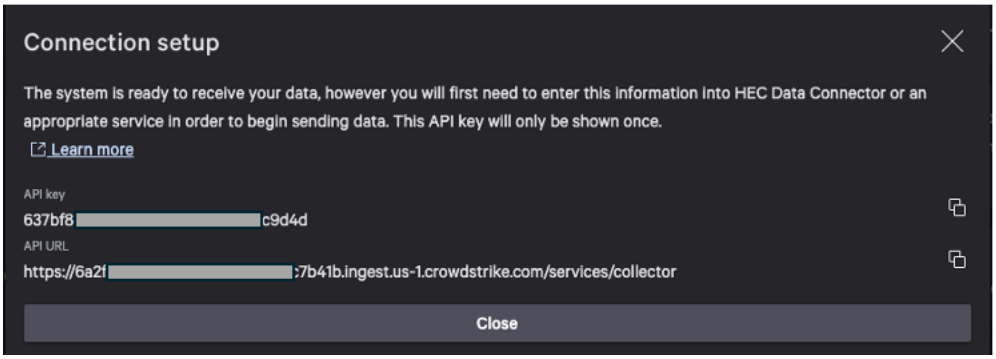


- Once the connector setup has completed processing (a few minutes), a bar will appear where you can select ***Generate API key***.

- Note: If the generate API key link doesn't appear after a few minutes, navigate to ***My connectors*** and then select your new ***connector*** to refresh and the link should appear.



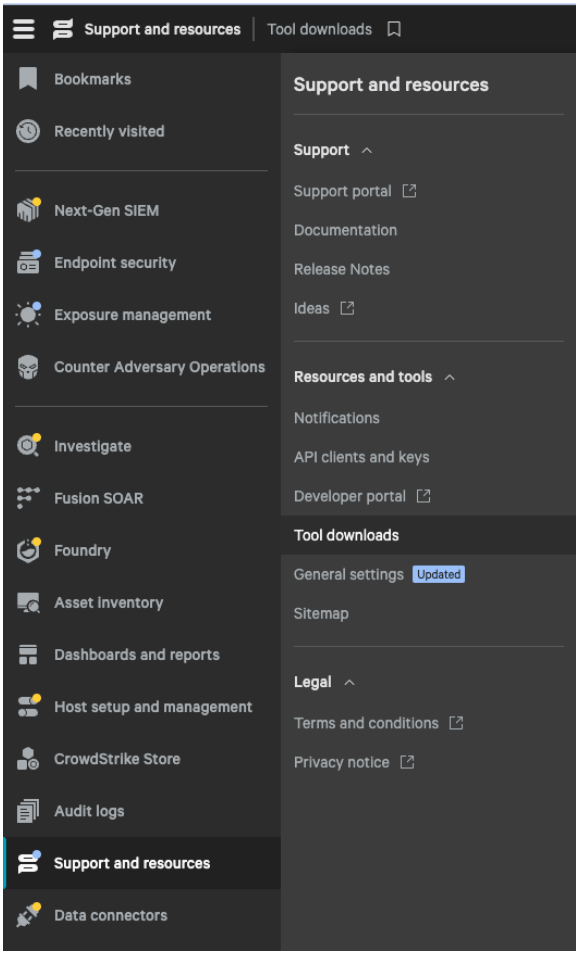
- From the connection setup record the ***API key*** and ***API URL***, the key will only be shown this one time. This data is required for the next step.



Prepare Log Collector

Server for Humio Log Collector. RHEL, Ubuntu, MacOS, Windows with appropriate architecture (ARM/X64) Ubuntu Linux 22.04 AMD/64 was used for this document.

- Log in to Falcon UI and navigate to ***Support and resources > Tool downloads***. Download the appropriate Logscale Collector binaries.



LogScale Collector For MacOS, v1.7.4	6.70MB
LogScale Collector For RHEL - ARM64, v1.6.6	5.94MB
LogScale Collector For RHEL - ARM64, v1.7.1	5.97MB
LogScale Collector For RHEL - ARM64, v1.7.3	5.97MB
LogScale Collector For RHEL - ARM64, v1.7.4	3.30MB
LogScale Collector For RHEL - X64, v1.6.6	6.42MB
LogScale Collector For RHEL - X64, v1.7.1	6.47MB
LogScale Collector For RHEL - X64, v1.7.3	6.48MB
LogScale Collector For RHEL - X64, v1.7.4	3.62MB
LogScale Collector For Ubuntu - ARM64, v1.6...	5.83MB
LogScale Collector For Ubuntu - ARM64, v1.7.1	5.88MB
LogScale Collector For Ubuntu - ARM64, v1.7.3	5.89MB
LogScale Collector For Ubuntu - ARM64, v1.7.4	3.21MB
LogScale Collector For Ubuntu - X64 , v1.6.6	6.30MB
LogScale Collector For Ubuntu - X64, v1.7.1	6.35MB
LogScale Collector For Ubuntu - X64, v1.7.3	6.36MB
LogScale Collector For Ubuntu - X64, v1.7.4	3.51MB
LogScale Collector For Windows - X64, v1.6.6	7.16MB

- Transfer the Logscale Collector binaries to your server and install the application.

```
sudo dpkg -i humio-log-collector_1.7.4_linux_amd64.deb
```

- Edit the ***config.yaml*** file (in this example on Linux it's stored under /etc/humio-log-collector.

```
sudo vi /etc/humio-log-collector/config.yaml
```

- Configure the log collector as appropriate.
  - Sources is where you configure the listening protocol and port and pay close attention to the sink name. This can be any name, but that name must be used in the sinks portion.
  - Sinks is where you provide the destination details for Crowdstrike NextGen-SIEM – this is the data recorded previously during the generate API key step.

IMPORTANT
The URL recorded during the generate API key step includes a full path. When entering the URL into the sink remove the trailing path (/services/collector)

```
dataDirectory: /var/lib/humio-log-collector
sources:
  # listen for syslog from vectra on port 9999
  syslog_tcp_9999:
    type: syslog
    mode: tcp
    port: 9999
    supportsOctetCounting: false
    strict: false
    sink: logscale

sinks:
  # this is referenced in sink under sources and must be type logscale
  # the token and url come from generate api key in the data connector
  logscale:
    type: logscale
    token: 6b3f5redacted8ac395542a
    url: https://cf19cceredactedfd9340ff49336b.ingest.us-1.crowdstrike.com
```

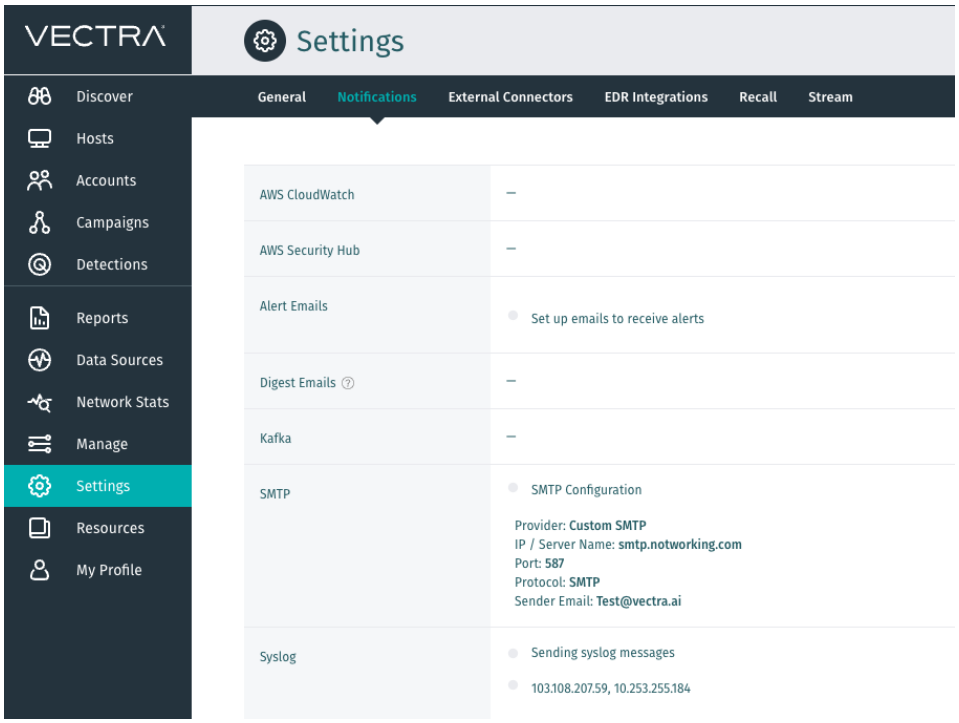
- Enable the log collector to run as a service, start it and verify the status.

```
sudo systemctl enable humio-log-collector.service

sudo systemctl start humio-log-collector.service

sudo systemctl status humio-log-collector.service
```

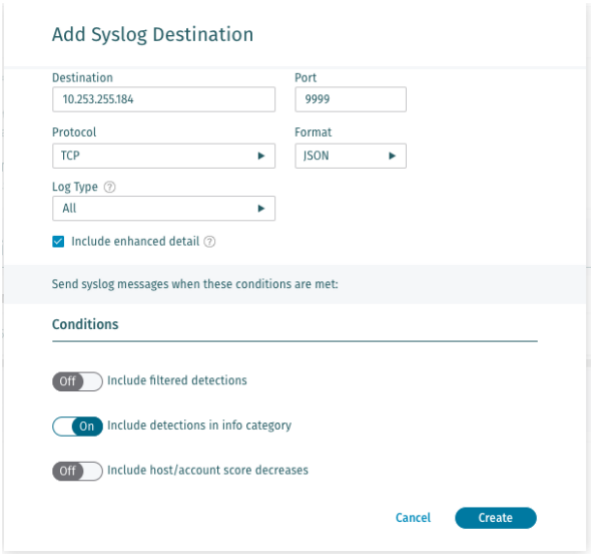
Configure Vectra

Configure Vectra to send syslog to the newly deployed log collector.

- Login to the Vectra UI and navigate to ***Settings*** > ***Notifications*** and select Edit beside the syslog menu.



- Add a new syslog destination and enter the destination data to match the humio log collector settings.

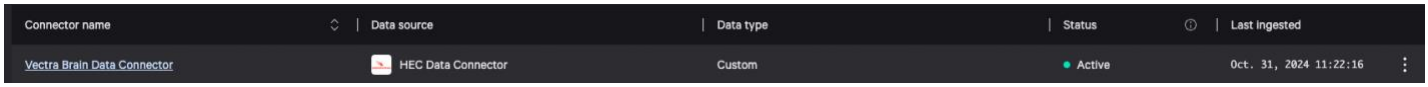


- Use the Test button to dispatch some test syslog messages.  Test

Verify Operations

Confirm data is being ingested successfully into Crowdstrike NextGen-SIEM.

- Login to the Falcon UI and navigate to ***Data connectors*** > ***My connectors***.
- Find the newly provisioned connector and verify the ***status*** is active and ***last ingested*** timestamp is present.



End of Document