Mandiant

CROWDSTRIKE NEXT-GEN SIEM SEARCH INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Crowdstrike to test the efficacy and configuration of the security control using Security Validation jobs.

See the following materials for more information:

- **Crowdstrike documentation (requires authentication)** **(https://falcon.crowdstrike.com/documentation/page/bda96fc1/next-gen-siem-search-apis)**
- **Query syntax** **(https://library.humio.com/data-analysis/writing-queries-manage.html)**

API calls

API	Usage	Required API client scope and permission
• `POST` • `/oauth2/token`	Retrieve OAuth2 token from Crowdstrike	NGSIEM: Write
• `POST` • `/humio/api/v1/repositories/` • `$REPOSITORY_NAME/queryjobs`	Create a query job and execute the search to run in the background.	NGSIEM: Read
• `GET` • `/humio/api/v1/repositories/` • `$REPOSITORY_NAME/queryjobs/$JOB_ID`	Use the query job ID to check the job status and get search results.	NGSIEM: Write

Supported versions

- CrowdStrike Next-Gen SIEM Search API v1

Repositories

Repository name	Description	Required Falcon subscription
All	All event data generated by CrowdStrike and third-party sources.	N/A
Falcon	Endpoint event data and sensor events.	Falcon Insight XDR
Third Party	Event data collected from third-party sources.	Falcon LogScale
IT Automation	Data collected by Falcon for IT module.	Falcon for IT
Forensics	Triage data collected by Falcon Forensics module.	Falcon Forensics

Before you begin

To configure this integration, you need:

- API Client ID
- API Client secret

Getting a Client ID and Secret from Crowdstrike

API client credentials are only displayed when a new API client is created.

1. Log into the CrowdStrike Falcon web interface.
2. Go to **Support and resources > API clients and keys** .
3. Click **Create API client**.
4. Select NGSIEM scope with read and write permissions.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Crowdstrike Next-Gen SIEM Search**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** **(https://docs.mandiant.com/home/msv-proxy-rules)**.
5. Optional: Change the **Protocol** value to determine what protocol is used for requests (**Https** or **Http**).
6. Enter the **Host** value (hostname or IP address) for the Logscale instance. The default is **cloud.us.humio.com** **(https://cloud.us.humio.com)**.
7. Enter a **Port** value. The default is **443.**
8. Enter the **Bearer Token** value that you generated.
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. Optional: Enter the **Repository**. The default is **humio**.
12. Add or remove value for **Queries**. A default **IP Query** is provided.
13. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.
14. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
15. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

b. Update **Query Interval** (seconds).
c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
d. Modify the **Correlation Query Interval**, if necessary (minutes).
e. Select **Discover network devices automatically**, the default and recommended option.

> If unselected, reported events won't include product information for any matching network security technology.

f. Select **Save Suspicious Events**.
g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

16. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
   - The Director can communicate with the integration host on the port and protocol specified.
   - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-integrations).