Set up Falcon Next-Gen SIEM

Last updated: May 30, 2025

Overview

Get started with CrowdStrike Falcon Next-Gen SIEM to unify security operations across CrowdStrike and third-party data sources. Falcon Next-Gen SIEM brings together threat detection, investigation, and response in one platform so you can quickly expose adversaries and stop breaches.

Requirements

Requires one or more of these subscriptions:

- Falcon Insight XDR
  - Falcon Next-Gen SIEM 10GB with 7 days of data retention is included.
- Falcon Next-Gen SIEM, or Falcon Complete powered by Next-Gen SIEM
  - Includes additional third-party data ingestion and data retention capabilities.

Sensor support: All supported sensors

Default roles:

- Falcon Administrator
- Connector Manager
- NG SIEM Administrator
- NG SIEM Security Lead
- NG SIEM Analyst

CrowdStrike clouds: Available in US-1, US-2, EU-1, and US-GOV-1. For info about the availability of data connectors in US-GOV-1, see the documentation specific to the data connector.

Additional requirements for third-party integrations: For info about third-party integration requirements, see the CrowdStrike documentation for your applicable integrations.

Prerequisites

Before you set up Next-Gen SIEM, the Falcon sensor must be installed and running on your hosts. Installing the Falcon sensor ensures your endpoint, identity, threat intelligence, and cloud data is available in Falcon Next-Gen SIEM. For more info, see Sensor Deployment and Maintenance [/documentation/category/ea9b123c/sensor-deployment-and-maintenance].

Setup

Once you have the Falcon sensor installed and running on your hosts, CrowdStrike-generated detections are available for monitoring, investigation, and response. Next, set up data connectors to ingest third-party data. Ingesting third-party data improves visibility into your environment, helping threat hunters investigate incidents across systems and providing a more complete picture of an attack.

Planning and preparation

Falcon Next-Gen SIEM unifies data from the Falcon sensor and from third-party sources. If you haven't already, identify 2 or 3 high-value data sources you want to ingest to start setting up Next-Gen SIEM. For example, you may want to ingest data from network activity, identity, cloud user workspaces, or email data sources. Consider threat-based use cases and business cases for bringing in specific data. If you have compliance or regulatory requirements, you may want to prioritize ingesting data that helps you meet those requirements. You must first decide what data to ingest before you continue onboarding data to set up Next-Gen SIEM.

Data onboarding

Ingest data from third-party sources to enrich data available in the Falcon platform and help you identify and stop threats. For many common data sources, you can onboard data using CrowdStrike-developed or partner-developed data connections. If the data source you want to ingest data from does not have an available data connector, set up a custom data connector with a custom parser. Parse any type of data using default or custom parsers. The connector facilitates secure access to the data source, automates ingestion, and sends ingested data to a predefined destination in the CrowdStrike cloud for processing.

Set up a data connector

CrowdStrike develops Falcon Next-Gen SIEM data connectors to streamline the process of ingesting data from common third-party data sources. For maximum compatibility, we recommend using CrowdStrike-developed or partner-developed data connectors for ingesting data. If a data source does not have a CrowdStrike-developed or partner-developed data connector, use a generic data connector. View the list of CrowdStrike-developed and partner-developed data connectors by clicking **Add connection** at **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]** For more info, see Data Connectors [/documentation/page/a76b8289/data-connectors].

For some data connectors that require a data shipper for log forwarding, we recommend the Falcon LogScale collector. You can monitor and manage a Fleet of LogScale collector instances remotely. For more info, see Get Started with Fleet Management [/documentation/page/q81f4f3a/get-started-with-fleet-management].

Use a CrowdStrike Parsing Standard (CPS) compliant parser to transform incoming data into searchable events that trigger detections in Next-Gen SIEM. Parsing the data allows security analysts to understand and work with the data ingested in Falcon. You can use default parsers to parse incoming data in common formats. To parse incoming data in other formats, create and manage your own custom parsers. For more info, see Parsers [/documentation/page/n00d51ed/parsers]. For more info about CPS, see CrowdStrike Parsing Standard [/documentation/page/u05f69c9/crowdstrike-parsing-standard].

For detailed instructions on setting up a CrowdStrike-developed or partner-developed data connector, see Third-Party Data Sources [/documentation/category/je6a45b3/next-gen-siem/third-party-integration-and-data-connectors/third-party-integrations].

Set up a custom data connector and custom parser

If you want to ingest data from a third-party source that does not have a CrowdStrike-developed connector, set up a custom data connector with a custom parser that transforms incoming data into events and detections. Setting up a generic connector enables you to ingest data from a wide variety of log sources into Falcon. Get started using a generic connector, such as the **HEC/HTTP Event connector** or the **Cribl Data Connector**. For detailed instructions on setting up one of these generic connectors, see HEC/HTTP Event Connector [/documentation/page/bdded008/hec-http-event-connector-guide] or Cribl [/documentation/page/b121307d/cribl]. For detailed instructions about setting up a custom parser, see Parsers [/documentation/page/n00d51ed/parsers].

Connectors use push or pull logic to ingest data. Push-based connectors push data to the Falcon platform. Falcon assigns each push connector a unique ingest URL and secret key to add to the third-party system. For pull-based connectors, you define how Falcon should access and retrieve data from the source, using provider-specific fields. For more info about push-based and pull-based connectors, see Provisioning [/documentation/page/a76b8289/data-connectors#h2818535].

Verify data ingestion

Once you have set up a third-party data connector, verify that the data is being ingested and parsed as you expect. This step is strongly recommended.

- The **Data connections** page (**Next-Gen SIEM > Log management > Data onboarding [/data-connectors]**) shows the status of your connectors, with options to **Show error history** and **Show events** in **Advanced event search**. You can also use **Advanced event search** to test a query and review the matches. For example search queries, see the CrowdStrike documentation for your data source at Third-Party Data Sources [/documentation/category/je6a45b3/next-gen-siem/third-party-integration-and-data-connectors/third-party-integrations].

- Data connector **Alerts** (**Data connectors > Data connectors > Alerts [/data-connectors/alerts]**) can also help identify any connection issues or gaps in data ingestion. You can also manage email notifications for alerts if a data connector is disconnected or stops receiving data.

View and tune detections

Once you've set up a data connection and are ingesting third-party data, we strongly recommend viewing Next-Gen SIEM detections (**Next-Gen SIEM > Monitor and investigate > Detections [/unified-detections]**). The list includes detections that originate from CrowdStrike alongside detections that originate from integrated third-party security products. For more info, see Understanding the unified detections view [/documentation/page/ke886083/unified-detections-monitoring#s8c23405].

If known false positive detections appear, or other detections that don't provide value to your investigations, you can adjust exclusions accordingly.

- Use exclusions to manage the activity that triggers CrowdStrike-generated detections. For more info, see Exclusions [/documentation/page/bd0f1c7f/detection-and-prevention-policies#q73c989a].

- You can also exclude specific detections generated by ingested third-party data, based on criteria you define. For more info about creating these exclusions, see Third-Party Detection Exclusions [/documentation/page/i499c81a/third-party-detection-exclusions-0].

Continue making adjustments until the detections are generated at a level that meets your organization's needs.

Create correlation rules

You can generate custom detections and incidents by using query-based correlation rules. We recommend creating correlation rules from a template, which provides an easy way to start triggering custom detections and incidents based on common threats. For more info, see Correlation Rules [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents].

View the detections or incidents generated from your correlation rule, based on the schedule you configured, to confirm they are being generated as expected.

Configure response actions

Accelerate response times and increase analyst productivity by configuring targeted Next-Gen SIEM response actions. This step is optional.

Set up Falcon Fusion SOAR workflows

Falcon Fusion SOAR (Security Orchestration, Automation, and Response) streamlines analyst workflows by automating actions around specific and complex scenarios. You can create workflows to precisely define the actions you want to occur in response to detections, incidents, policies, cloud security findings, and more. You can create workflows based on a template or from scratch. Set workflows to execute automatically or manually.

You can also create a Fusion SOAR workflow that automatically initiates a specified third-party response action when a triggering condition occurs.

For more info, see Fusion SOAR [/documentation/page/dc4f8c45/workflows-falcon-fusion-1692362310390.669].

Next steps for managing Next-Gen SIEM

After completing the initial steps for setting up Next-Gen SIEM, continue adjusting configurations, investigating threats, and managing third-party data sources. These steps are optional.

- Continue to monitor detections and make adjustments to correlation rules, as needed. Review the **Detection coverage dashboard** to identify and fill any MITRE ATT&CK technique coverage gaps. For more info, see Detection coverage management [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#m4d4146b].

- You can create incidents manually, as needed, based on your investigations. Streamline incident investigation workflows, increase collaboration, and reduce mean time to remediation with the incident workbench. For more info, see Incident Investigation [/documentation/page/r2f1bac9/xdr-incident-investigation].

- Set up additional data connectors to onboard more third-party data sources.
- Continue to monitor data connectors and troubleshoot any issues, as needed. For more info, see Manage alerts for third-party data connectors [/documentation/page/a76b8289/data-connectors#q61afe53] and View ingestion volume dashboard for third-party data connectors [/documentation/page/a76b8289/data-connectors#c5c74224].

‹ About Falcon Next-Gen SIEM[/documentation/page/i5d2 CrowdStrike Parsing Standard › [/documentation/page/u05f69c9/crowdstrike-parsing-standard]