About Falcon Next-Gen SIEM

Last updated: May 30, 2025

Overview

CrowdStrike Falcon Next-Gen SIEM unifies security operations, bringing together threat detection, investigation, and response in one platform so you can quickly expose adversaries and stop breaches. Falcon Next-Gen SIEM extends CrowdStrike's detection and response, threat intelligence, and expert services to all data sources and amplifies the speed and efficiency of incident response for enhanced visibility and protection.

For more info about getting started with Next-Gen SIEM, see Set up Falcon Next-Gen SIEM [/documentation/page/cffa5af8/set-up-next-gen-siem].

Requirements

Requires one or more of these subscriptions:

- Falcon Next-Gen SIEM 10GB
  - 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
- NG SIEM Administrator
- NG SIEM Security Lead
- NG SIEM Analyst
- NG SIEM Analyst - Read Only

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

Additional requirements for third-party integrations:

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

Understanding Falcon Next-Gen SIEM

Unify detection and response across your security stack by ingesting third-party telemetry. Hunt, detect, and investigate adversary activity across attack surfaces from a unified interface in the Falcon console.

- **Detection monitoring and incident investigation:** CrowdStrike monitors activity across your specified domains and data sources. CrowdStrike correlates and analyzes data in real time upon ingestion, and automatically generates detections and incidents when suspicious activity is detected. Incidents bring together related detections, associated processes, and the connections between them to show coordinated activity you should prioritize for investigation.
- **Event search:** Search cross-domain data to hunt for suspicious activity or further investigate detections and incidents.
- **Custom incidents and detections from correlation rules:** Create query-based correlation rules that, when triggered, can generate custom incidents and detections. They appear alongside CrowdStrike-generated incidents and detections to facilitate monitoring and triage.
- **Third-party data integration:** Create data connectors that automate and manage ingestion from CrowdStrike Store applications and third-party data sources to get your data into the Falcon console.
- **Response actions:** Perform targeted response actions, manually from within an incident, or automatically through a Falcon Fusion SOAR workflow. Optionally, extend Next-Gen SIEM response capabilities with supported third-party integrations.

Data sources

Extend Falcon platform telemetry by ingesting security telemetry from third-party vendors. Upon ingestion, data is parsed and mapped into the CrowdStrike Parsing Standard (CPS) data schema, which provides a common language for correlation and analysis of data from different sources. For more info, see CrowdStrike Parsing Standard (CPS) [https://library.humio.com/logscale-parsing-standard/pasta.html].

How data is processed and stored

Ingested data is parsed and mapped into the CrowdStrike Parsing Standard [/documentation/page/u05f69c9/crowdstrike-parsing-standard] (CPS) data schema which provides a common language for correlation and analysis of data from different sources. For most third-party connectors, data parsing and mapping is done automatically. For custom data sources, customers provide their own parsers and mappings. The CPS data schema can include vendor-specific alerts, events, and indicators. Vendor-specific telemetry is preserved and stored because it can contain information that supports investigation and response.

Measure data ingest

Similar to Falcon LogScale [https://library.humio.com/falcon-logscale-cloud/admin-license-and-usage-how.html], Next-Gen SIEM measures ingested data following this flow:

this flow:

1. Data is submitted from the client through [Third-Party Data Sources [/documentation/category/je6a45b3/next-gen-siem/third-party-integration-and-data-connectors/third-party-integrations]]. For example, third-party integrations or data connectors rely on existing LogScale components, like the [LogScale HEC API [https://library.humio.com/logscale-api/log-shippers-hec.html]] or the [Falcon LogScale Collector [https://library.humio.com/falcon-logscale-collector/log-collector.html]], to ingest data.

2. The third-party integration framework receives the data, and timestamp and timezone metadata are added.

3. Usage is calculated and stored as data arrives.

4. A parser connected to each third-party integration processes events, and extracts or normalizes fields for use in Next-Gen SIEM. Unlike LogScale, Next-Gen SIEM does not currently support the field removal feature in parsing settings.

For Next-Gen SIEM, events are composed of a raw string, fields, and tags. The amount of ingested data is measured in uncompressed bytes. You can view the total volume of data ingested, including a 30 day rolling average for each calendar day based on UTC timezone, in the Connector Dashboard. For more info, see [View ingestion volume dashboard for third-party data connectors [/documentation/page/a76b8289/data-connectors#c5c74224]].

To manually calculate usage size for each event, add the raw string message, plus fields and tags that were not extracted from the rawstring in bytes using this formula:

```
fieldsSizeBytes = @rawstring + fields not extracted from the rawstring + tags not extracted from the
rawstring + timefields size
```

Note: These additional fields and tags do not count towards the usage cost calculation:

- If you use the Falcon LogScale Collector, [fields added by the Log Collector [https://library.humio.com/logscale-repo-schema/logscale-repo-schema-humio-fleet.html#table_searcing-data-event-fields-metadata]]
  . These start with @collect.*.

- Fields added by CPS parsers. This is because the usage calculation is performed before parsing. Examples include fields such as Cps.version and Parser.version. See [CrowdStrike Parsing Standard (CPS) 1.0 [https://library.humio.com/logscale-parsing-standard/pasta.html]] for further details.

- The index field, which is used by the data connector for routing data.

Example: Usage calculation for an event using a HEC structured endpoint

Note: Data connectors that use a HEC structured endpoint include pull connectors, the AWS S3 connector, and streaming connectors that use Azure Event Hubs and GCP.

Ingested event data

```
{"time":1451606400,"fields":{"#type":"json", "test": "abc"},"event":{"x":123}, "index": "repoA"}
```

Usage calculation

```
val fieldsSizeBytes = ("{\"x\":123}" + "test" + "abc" + "#type" + "json").length + timeFieldsSize
```

```
Timefields size = FieldNames.TIMESTAMP.length + java.time.Instant.now().toEpochMilli.toString.length +
FieldNames.TIMEZONE.length + "Z".length
```

Important: When event length is calculated, the entire JSON, including JSON tokens, any non-word character, word character, is considered in length calculation. Non-word characters might not be preserved. Include it in the event to calculate event size properly.

By this calculation, the total size of this event is 58 bytes.

- event: 9 bytes

- test: 4 bytes

- abc: 3 bytes

- #type: 5 bytes

- json: 4

- Time fields size: 33 (`@timestamp` + `@timezone`)

  Note: The `@timestamp` and `@timezone` fields are required. If the `@timestamp` field is not present in the event, an extra 33 bytes of timestamp are added.

Example: Usage calculation for an event using a Raw HEC request

[Ingesting with a Raw HEC request [https://library.humio.com/logscale-api/log-shippers-hec-raw.html]] is calculated differently as raw ingestion is interpreted as the raw message body using this formula:

```
total bytes = ingestJson.length + timeFieldsValueLength + channelLength
```

Ingested event data

```
{"@timestamp": "2025-12-21T13:41:08.533Z", "beat": {"hostname": "testhostname", "name": "testhostname",
"version": "5.0.2"}, "input_type": "log", "message": "some message", "offset": 45, "source": "test.log",
"type": "log", "foo": "barbaz"}
```

Usage calculation

```
Request body bytes:
"{"@timestamp": "2025-12-21T13:41:08.533Z", "beat": {"hostname": "testhostname", "name": "testhostname",
"version": "5.0.2"}, "input_type": "log", "message": "some message", "offset": 45, "source": "test.log",
"type": "log", "foo": "barbaz"}".length + timeFieldsSize + "channel".length + "4".length
```

Important: When event length is calculated, the entire JSON, including JSON tokens, any non-word character, word character, is considered in length calculation. Non-word characters might not be preserved. Include it in the event to calculate event size properly.

By this calculation, the total size of this event is 281 bytes:

- `ingestJson.length`: 240 bytes
- `timeFieldsValueLength`: 33 bytes
- `channelLength`: 8 bytes

Immutability of stored data

Next-Gen SIEM is designed so that data, once digested to a repository, is immutable. You can not modify or edit the data. At rest, the data is encrypted and a checksum process is used on each segment to prevent corruption.

Next-Gen SIEM data in a repository can only be deleted under certain conditions:

- **By time** — Data is automatically purged at the end of the designated retention period.
- **By request** — In extremely rare situations where data was accidentally ingested, contact CrowdStrike Support to request data redaction.

Next-Gen SIEM terms

Item	Description
Detection	A confirmation that activity is malicious or otherwise warrants further investigation. A Next-Gen SIEM detection can be composed of one event or multiple, correlated events. CrowdStrike automatically generates detections for events from supported and connected third-party products.
Incident	A collection of related activity, such as detections, associated processes, and the connections between them. Incidents show coordinated activity that you should prioritize for investigation. **Note:** Some CrowdScore incidents are also available as Next-Gen SIEM incidents. For more info, see CrowdScore incidents as Next-Gen SIEM incidents [/documentation/page/dabdbd2a/incident-monitoring#r1e02695]
Event	A signal that an activity occurred. Examples: • An email was received • A login attempt failed • A file was written
Contextual behavior	Activity that occurred around a detection. Contextual behaviors aren't considered significant on their own. However, they can provide additional context and can help you investigate a detection.

Next-Gen SIEM detection monitoring

CrowdStrike monitors activity across the Falcon platform and your connected third-party domains and data sources. It surfaces suspicious collections of signals and detections in the form of correlated Next-Gen SIEM detections. The types of available CrowdStrike-generated detections, for example, identity, endpoint, mobile, and data protection, depend on your active Falcon subscriptions. The types of third-party detections shown depend on your integrated third-party products. For more info, see Detection Monitoring [/documentation/page/ke886083/unified-detections-monitoring].

Next-Gen SIEM incident investigation

Incidents can be generated automatically by CrowdStrike, from your correlation rules, or manually from the unified **Detections** view.

From Next-Gen SIEM **Incidents**, you can triage, investigate, and respond to cross-domain alerts.

- **Triage:** Filter incidents by data domain, data source, status, severity, and more. Assign detections, update detection status, and comment on detections.
- **Investigate:** In the incident summary, review incident details, including info about the events and detection that triggered the incident. Pivot to the graph explorer to visualize the incident and explore connections between events. Pivot from the summary into event search to view event data associated with the alert.
- **Respond:** In the incident summary, perform response actions through Falcon Identity Protection, Falcon Fusion SOAR, or supported third-party vendors.

CrowdScore incidents are also available as Next-Gen SIEM incidents that can be triaged, assigned, or investigated more deeply. This enables you to view a CrowdScore incident within the context of all available Next-Gen SIEM data across your data domains, including data that originates from the Falcon platform and data that originates from supported third parties. For more info, see CrowdScore incidents as Next-Gen SIEM incidents [/documentation/page/dabdbd2a/incident-monitoring#r1e02695].

Next-Gen SIEM event investigation

Search against cross-domain data to hunt for suspicious activity or further investigate detections and incidents.

- **Events**: Events represent an occurrence, object, or process in the Falcon platform. Event fields represent data in many different formats. For more info, see Events [/documentation/category/j282ed2d/event-investigation/events].
- **Advanced Event Search**: Analyze, explore, and hunt for suspicious or malicious activity in your environment using the CrowdStrike Query Language (CQL). For more info, see Advanced Event Search [/documentation/page/ic5d7b7d/event-search-advanced].
- **Dashboards:** Create your own customized dashboard widgets from a search query. For more info, see Dashboards [/documentation/page/ic5d7b7d/event-search-advanced#r48010d4].

- **Event investigation**: Hunt for adversaries, suspicious activities, suspicious processes, and vulnerabilities. For more info, see Event Investigation [/documentation/category/feb7faf0/event-investigation].

Response actions

Falcon Fusion SOAR adds workflow automation and response orchestration to Next-Gen SIEM. Fusion SOAR workflows perform response actions through the Falcon platform and supported third-party tools. When creating workflows, you can choose from pre-built templates and playbooks, or create custom workflows from scratch. Automating response actions helps improve operational efficiency, reduce response times, and maintain consistent incident-handling procedures. For more info, see Fusion SOAR [/documentation/page/dc4f8c45/workflows-falcon-fusion-1692362310390.669].

Set up Falcon Next-Gen SIEM > [/documentation/page/cffa5af8/set-up-next-gen-siem]