Correlation Rules

Last updated: Jun. 6, 2025

Overview

Create query-based correlation rules that, when triggered, can generate custom incidents and detections. Build your own correlation rules from scratch or apply rule templates that CrowdStrike provides.

Requirements

Subscription: Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB

Default roles:

- Falcon Administrator
- NG SIEM Administrator
- NG SIEM Analyst
- NG SIEM Analyst - Read Only
- NG SIEM Security Lead

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

Understanding correlation rules, custom incidents, and custom detections

When you create a correlation rule, you configure a recurring schedule that determines when and how often the associated search query runs.

You can optionally configure notifications that are sent to your specified recipients each time the associated search produces an error or warning.

If a search operation returns results that indicate suspicious activity, a custom incident or detection is generated. Custom incidents or detections that are generated through correlation rules appear alongside your other CrowdStrike-generated incidents, facilitating monitoring, investigation, and triage. For more info, see Incident Investigation [/documentation/page/r2f1bac9/xdr-incident-investigation] and Detection Monitoring [/documentation/page/ke886083/unified-detections-monitoring].

An activity log shows the history of your completed searches, including searches that generated errors.

An audit log shows the history of changes to your correlation rules.

Sensor rules

In addition to correlation rules, the **Rules** tab also displays sensor rules, which are the built-in rules that trigger sensor detections. Although you can't create, edit, or delete sensor rules, you can view details such as the rule name, description, and any associated MITRE ATT&CK tactic or technique.

Correlation rule templates

As an alternative to creating a correlation rule from a blank canvas, you can create a rule based on a template that CrowdStrike provides and then modify its settings as needed.

> **Note:** To create correlation rules based on templates, Next-Gen SIEM capabilities must be enabled on your CID.

Choose from templates developed by CrowdStrike or by selected third-party developers.

Templates are designed to address a variety of threats.

Correlation rule version states

Correlation rule versions provide flexibility in creating and managing correlation rules.

- **Draft:** When you're updating a correlation rule, use drafts to save work in progress.
- **Unpublished:** To facilitate review and testing, set the status of a correlation rule version as unpublished.
- **Published:** When you're ready to use a version of the correlation rule to run queries, set the status to **Published**. You cannot delete a published version of a correlation rule. To delete a published version of a correlation rule, you must first publish a different version as active.

Correlation rule states

- **Active:**
  - An active rule will continue to execute searches and generate new incidents or detections from those searches.
- **Inactive:**

- If you deactivate a rule, its **Status** changes to **Inactive** and all further searches stop. You can resume the rule by reactivating it. For more info, see Activate or deactivate a correlation rule [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#bd3509ad].
- Deactivating a rule prevents any new queries from running and new incidents and detections from being generated, but the configured rule remains available for use for 30 days. After 30 days, the deactivated rule is deleted permanently. However, any previously generated incidents and detections continue to appear in their respective lists.

Frequency and timing

When you create a correlation rule, you specify a search frequency and a search window. The search frequency determines how often the Falcon platform runs the search. The search window determines the period of time that's searched.

After you activate a correlation rule, the first instance of the associated search runs at your specified start time and generates results for the specified interval.

The first time an incident or detection is generated for a given query, a time window is established between the first and last events.

To ensure that all relevant data is searched, configure a search window that's at least as long as the search frequency. Overlapping searches help to ensure that all relevant data is included, regardless of when logs are uploaded. However, with overlapping searches, a given event or indicator might appear in more than one resulting incident.

If more than 5 searches are scheduled to run at the same time, they're placed in a queue and then run as resources become available. If a given search isn't complete by the time the next search is scheduled to start, the next instance of the search fails.

If a running search hasn't completed after 60 minutes, it times out. If a specific search is timing out frequently, consider editing the associated correlation rule to refine its query syntax. For more info, see Edit a correlation rule [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#e34b3bf0].

You can retry a failed search manually. For more info, see Retry a search [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#dd70bf43].

Limitations and considerations

Important constraints and special considerations to be aware of when using correlation rules are outlined below.

Active correlation rules

Your CID can have a maximum of 750 active correlation rules, including searches that generate custom detections, and an unlimited number of inactive rules. If your CID already has 750 active rules, any new rules created are inactive by default. For info about activating and deactivating rules, see Activate or deactivate a correlation rule [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#bd3509ad].

Aggregate functions

Correlation rule queries support aggregate functions. For info about supported functions, see Aggregate Query Functions [https://library.humio.com/data-analysis/functions-aggregate.html].

Entity limitations

Correlation rules can have a maximum of 500 entities associated with them. If there are more than 500 entities associated with a correlation rule, an error will be displayed in the correlation rule's **Details** view. You will need to refine and filter its search query to reduce the number of entities associated with it and remove the error. For info about writing search queries, see Get Started with CrowdStrike Query Language [/documentation/category/nbbb7a91/event-investigation/get-started-with-crowdstrike-query-language].

Rule deactivation

Deactivating a rule prevents any new queries from running and new incidents and detections from being generated, but the configured rule remains available for use for 30 days. After 30 days, the deactivated rule is deleted permanently. However, any previously generated incidents and detections continue to appear in their respective lists.

If the user associated with a correlation rule is removed or has their permissions revoked, the rule is deactivated. Additionally, a notification explaining the deactivation is sent to all notification recipients for that rule. If a different user reactivates the rule, that user becomes the new owner of the rule.

Report generation

Correlation rules are not intended for report generation. Instead, we recommend that you create custom dashboards, which you can export and share with others. For more info, see Customizable Dashboards [/documentation/page/dfe2a579/customizable-dashboards].

Search results

All incidents and detections, including custom incidents and detections generated from correlation rules, appear in the Falcon console for 90 days after they're generated.

Retention

All incidents and detections, including custom incidents and detections generated from correlation rules, appear in the Falcon console for 90 days after they're generated.

Timestamps

When creating correlation rules with data from third party data connector sources, use the Ingest (`@ingesttimestamp`)to limit ingestion delays. For more info, see Timestamps for triggers [https://library.humio.com/data-analysis/automated-alerts-getting-started.html#automated-alerts-getting-started-timestamps].

Error and warning notifications

You can set up automatic delivery of notifications to alert members of your team each time a search instance produces an error or warning.

Recipients cannot unsubscribe from notifications. Only the rule owner, an NG SIEM Administrator, or a Falcon Administrator can remove recipients from the notification settings.

To be notified of full correlation rule search results, along with errors and warnings, create a Fusion SOAR workflow. For more info, see Fusion SOAR [/documentation/page/dc4f8c45/workflows-falcon-fusion-1692362310390.669].

Error and warning notification delivery options

Send error or warning notifications to individual users by email or to groups of users through Slack, PagerDuty, Microsoft Teams, or webhook integrations. For each correlation rule, you can configure one or more delivery methods.

Before you can configure notifications through Slack, PagerDuty, Microsoft Teams, or webhook, you must set up the relevant app integrations through the CrowdStrike Store.

Email

Send notifications to a specified list of email addresses in your approved domains. For each correlation rule, you can designate up to 10 email notification recipients, including people who are not Falcon users.

Slack

Send notifications to one or more channels in your integrated Slack account. A Slack integration through the CrowdStrike Store is required. For info about setting up a Slack integration, see CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

PagerDuty

Configure notifications to automatically open an incident in PagerDuty and alert relevant user groups. Select the PagerDuty source and severity from your connected service to configure notification delivery. A PagerDuty integration through the CrowdStrike Store is required. For info about setting up a PagerDuty integration, see CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

Microsoft Teams

Send notifications to one or more channels in your integrated Microsoft Teams account. A Microsoft Teams integration through the CrowdStrike Store is required. For info about setting up a Microsoft Teams integration, see CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

Webhook

Distribute notifications to other applications through a webhook. A webhook integration through the CrowdStrike Store is required. For info about setting up a webhook integration, see CrowdStrike Store App Integrations [/documentation/page/dfe838e5/crowdstrike-store-app-integrations].

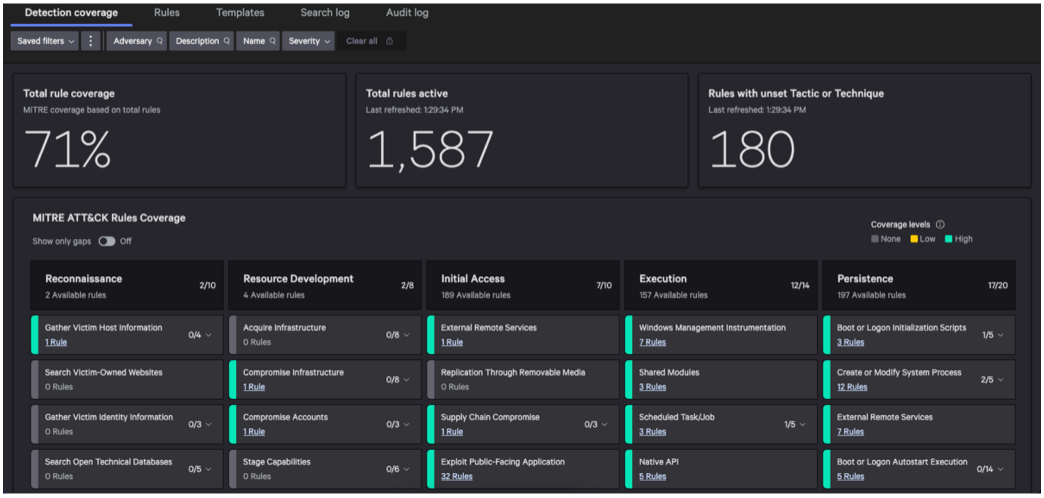
Detection coverage management

Visualize your detection and MITRE ATT&CK Tactics & Techniques coverage with the **Detection coverage** dashboard.

This dashboard displays which MITRE ATT&CK techniques you have coverage for across the Falcon platform, including ingested third-party data from Next-Gen SIEM. You can quickly identify and fill coverage gaps or filter techniques by adversaries to see the associated coverage.

The dashboard widgets show the percentage of tactics and techniques with rule coverage, the number of active rules, and the number of rules without an associated tactic or technique.

To view the dashboard, go to **Next-Gen SIEM > Monitor and investigate > Detection coverage [/xdr/detection-coverage]**.



Total rule coverage
MITRE coverage based on total rules
71%

Total rules active
Last refreshed: 1:29:34 PM
1,587

Rules with unset Tactic or Technique
Last refreshed: 1:29:34 PM
180

MITRE ATT&CK Rules Coverage

Show only gaps: Off

Coverage levels: ▨ None 🟨 Low 🟩 High

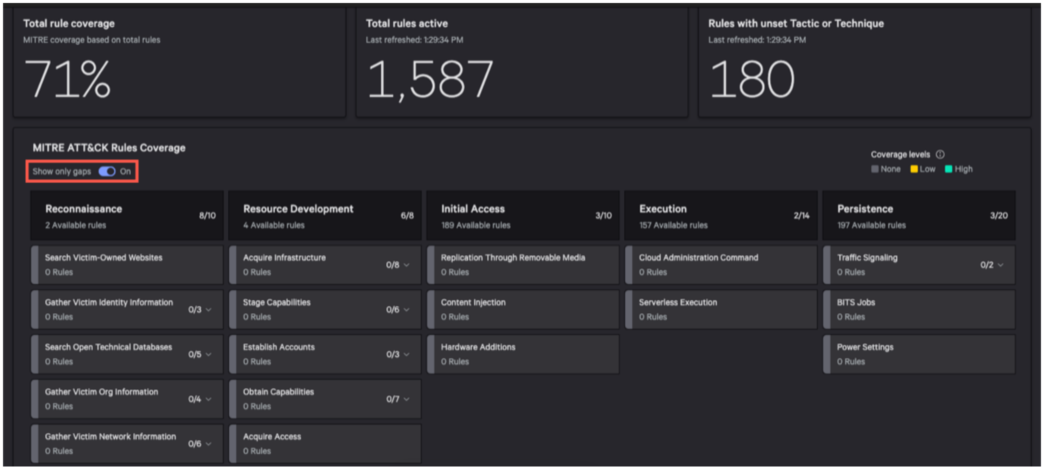
Reconnaissance 2/10 2 Available rules	Resource Development 2/8 4 Available rules	Initial Access 7/10 189 Available rules	Execution 12/14 157 Available rules	Persistence 17/20 197 Available rules
Gather Victim Host Information 0/4 1 Rule	Acquire Infrastructure 0/8 0 Rules	External Remote Services 1 Rule	Windows Management Instrumentation 7 Rules	Boot or Logon Initialization Scripts 1/5 3 Rules
Search Victim-Owned Websites 0 Rules	Compromise Infrastructure 0/8 1 Rule	Replication Through Removable Media 0 Rules	Shared Modules 3 Rules	Create or Modify System Process 2/5 12 Rules
Gather Victim Identity Information 0/3 0 Rules	Compromise Accounts 0/3 1 Rule	Supply Chain Compromise 0/3 1 Rule	Scheduled Task/Job 1/5 3 Rules	External Remote Services 7 Rules
Search Open Technical Databases 0/5 0 Rules	Stage Capabilities 0/6 0 Rules	Exploit Public-Facing Application 32 Rules	Native API 5 Rules	Boot or Logon Autostart Execution 0/14 5 Rules

The dashboard provides these coverage levels based on configured rules and templates:

- **High:** There are one or more active rules associated with the technique
- **Low:** There are one or more inactive rules associated with the technique, or there are templates available but they aren't associated with any rules
- **None:** There are no rules or templates associated with the technique

You can view the associated rules and templates for high and low entries by clicking the **Rules** link for the technique.

To view all tactics that do not have any associated rules or templates, turn on **Show only gaps**.



Total rule coverage
MITRE coverage based on total rules
71%

Total rules active
Last refreshed: 1:29:34 PM
1,587

Rules with unset Tactic or Technique
Last refreshed: 1:29:34 PM
180

MITRE ATT&CK Rules Coverage
Show only gaps On

Coverage levels
None Low High

Reconnaissance 8/10 2 Available rules	Resource Development 6/8 4 Available rules	Initial Access 3/10 189 Available rules	Execution 2/14 157 Available rules	Persistence 3/20 197 Available rules
Search Victim-Owned Websites 0 Rules	Acquire Infrastructure 0/8 0 Rules	Replication Through Removable Media 0 Rules	Cloud Administration Command 0 Rules	Traffic Signaling 0/2 0 Rules
Gather Victim Identity Information 0/3 0 Rules	Stage Capabilities 0/6 0 Rules	Content Injection 0 Rules	Serverless Execution 0 Rules	BITS Jobs 0 Rules
Search Open Technical Databases 0/5 0 Rules	Establish Accounts 0/3 0 Rules	Hardware Additions 0 Rules		Power Settings 0 Rules
Gather Victim Org Information 0/4 0 Rules	Obtain Capabilities 0/7 0 Rules			
Gather Victim Network Information 0/6 0 Rules	Acquire Access 0 Rules			

Correlation rule management

Create a correlation rule from scratch

Create a correlation rule from a blank canvas with no pre-populated fields.

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.
2. Click **Create correlation rule**.
3. Enter a name for the rule.
4. Optional. Enter a descriptive comment about the rule.
5. In the **Search query** field, enter the search query that you want to base the rule on. For info about writing search queries, see Get Started with CrowdStrike Query Language [/documentation/category/nbbb7a91/event-investigation/get-started-with-crowdstrike-query-language].
6. Select an event timestamp of **Ingested (`@ingesttimestamp`)** or **Created (`@timestamp`)**.
   - Use **Ingested (`@ingesttimestamp`)** if you want to search by the time the event was received by the CrowdStrike cloud.
   - Use **Created (`@timestamp`)** if you want to search by the time the event was generated locally on the system.
     For more info, see Timestamps for triggers. [https://library.humio.com/data-analysis/automated-alerts-getting-started.html#automated-alerts-getting-started-timestamps]
7. Select a trigger type of **Verbose** or **Summary**.
   - Use **Verbose** if you want 1 incident or detection per result.
   - Use **Summary** if you want a single incident or detection for all results in the search window. **Summary** is the default option.
8. Select an outcome for the rule. Choose between **Incident** or **Detection**.
9. Optional. Test the query, and then modify the query details as needed.
10. Select a severity for the rule.
11. Optional. Assign a MITRE ATT&CK tactic and technique to the rule.
12. Click **Next**, and then configure a schedule for the rule:
    - **Start date** and **Start time:** Specify when the search for the rule will begin running. The start time must be at least 15 minutes from the current time.
    - Optional. **End date** and **End time:** If you want the search for the rule to run for a finite period of time, specify the last day on which to run the search. If no end date is specified, the search runs indefinitely according to the configured frequency.
    - **Search frequency:** Specify how often to run the search for the rule.
    - **Search window:** Specify the period of time that will be searched. To help ensure that all relevant data is searched for incidents and detections, configure a **Search window** value that's at least as long as the **Search frequency** value. For more info, see Frequency and timing [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#d9066fc5].
13. Click **Next**, and then configure notification settings as needed. For more info, see Notification configuration fields for correlation rules [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#g543c9fe].
    - To set up multiple delivery methods, click **Add another notification** after adding a notification method.
14. Click **Finish**.
15. Optional. Add a **Comment**.
16. Click **Continue saving**.

Create a correlation rule from a template

Create a correlation rule from a template with pre-populated values that you can modify as needed.

Note: To create correlation rules based on templates, Next-Gen SIEM capabilities must be enabled on your CID.

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.
2. Click the **Templates** tab. A list of all available templates appears.
3. Filter and sort the templates as needed.
4. For the template that you want to create a rule from, click **Create rule**.
5. Modify the pre-populated values as needed. For more info about configuring rules, see Create a correlation rule from scratch [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#u41a3eb2].
6. Click **Finish**.

Activate or deactivate a correlation rule

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.
2. For the rule that you want to activate or deactivate, click the **Open** menu ⋮ , and then click **Activate** or **Deactivate**.

For more info, see Correlation rule states [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#t828ccf0].

Edit a correlation rule

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.
2. For the rule that you want to modify, from the **Open** menu ⋮ , click **Edit**.
3. Modify the settings as needed. For more info about configuring rules, see Create a correlation rule from scratch [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#u41a3eb2].
4. Click **Update**. A new version of the correlation rule is created.

Manage correlation rule versions

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.
2. Filter and sort the list of rules as needed.
3. For the rule with versions you want to manage, from the **Open** menu ⋮ , click **View versions**.
4. Click the **Open** menu ⋮ for a version to take action.
   - **Edit:** For more info about editing rules, see Create a correlation rule from scratch [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#u41a3eb2].
   - **Publish as active:** Only available for unpublished versions.
   - **Compare with another version:** For more info about comparing versions, see Compare correlation rule versions [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#l609103b].
   - **Delete:** Only available for unpublished versions.
   - **Export rule:** Exports the rule as a YAML file.

Add correlation rule versions

When you edit a correlation rule, a new version is created automatically. You can also create a new version from the **Versions** tab.

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.
2. Filter and sort the list of rules as needed.
3. For the rule with versions you want to manage, from the **Open** menu ⋮ , click **View** versions.
4. Click **Add version**.
   - **Create version:** Create a new version based on the currently published version. For more info, see Create a correlation rule from scratch [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#u41a3eb2].
   - **Import version:** Create a new version from a YAML or YML file. For example, a rule you exported and edited.

Compare correlation rule versions

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.
2. Filter and sort the list of rules as needed.
3. For the rule with versions you want to compare, from the **Open** menu ⋮ , click **View versions**.
4. Select 2 versions of the rule.
5. Click **Compare versions**.
6. Optional. Click **Show only differences** to view what's changed.
7. Optional. Select different versions from **Version Before** or **Version After** to compare.

Note: You can also compare a correlation rule version by clicking the **Open** menu ⋮ for a specific version.

Delete a correlation rule

Permanently delete a correlation rule that you no longer need. If you delete a correlation rule, any previously generated incidents and detections continue to appear in their respective lists. Deleting a correlation rule deletes all versions of the rule.

As an alternative to permanent deletion, you can deactivate a correlation rule. Deactivating a rule prevents any new queries from running and new incidents and detections from being generated, but the configured rule remains available for use for 30 days. After 30 days, the deactivated rule is deleted permanently. For more info, see Activate or deactivate a correlation rule [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#bd3509ad].

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.

2. For the rule that you want to delete, from the **Open** menu ⋮ , click **Delete**.

View correlation rules

View your configured correlation rules and any searches that are currently running or queued. Refine the results through sorting, filtering, or specifying which columns are visible.

If the user associated with a correlation rule has been removed or has had their permissions revoked, the rule is deactivated and the **User** field shows a value of **None**. For more info, see Limitations and considerations [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#pe64f557] and Activate or deactivate a correlation rule [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#bd3509ad].

For info about viewing search activity and search results, see View the correlation rules search log [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#ief5926e].

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.

2. Filter and sort the list of rules as needed.

3. Click any rule to see additional details.

View the correlation rules search log

View the activity history of completed searches, including any searches that generated errors.

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.

2. Click the **Search log** tab. A list of all completed searches appears.

3. Adjust your view by filtering or sorting the log entries.

4. Click any activity event to see more details.

View the correlation rules audit log

View the history of changes to your configured correlation rules.

If a correlation rule has been deleted, the **Name** field shows a numerical unique identifier for the rule instead of its configured name. To avoid this, you can deactivate a rule instead of deleting it. For more info, see Activate or deactivate a correlation rule [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#bd3509ad] and Delete a correlation rule [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#lc352e46].

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.

2. Click the **Audit log** tab.

3. Adjust your view by filtering or sorting the log entries.

4. Click any revision to see additional details.

Retry a search

Retry a failed search manually. For more info, see Frequency and timing [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#d9066fc5].

1. Go to **Next-Gen SIEM > Monitor and investigate > Rules [/xdr/rules]**.

2. For the search that you want to retry, click **Retry**.

   Note: The **Retry** option appears only if a search has failed.

Notification configuration fields for correlation rules

During configuration, set up notifications if you want to alert others each time that a search instance produces an error or warning. For more info about notifications and app integrations, see Error and warning notifications [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents#a28ce4f1].

Notification method	Description and options
Send email	Send an email notification to the specified recipients each time the associated search results in an error or warning. In the **Recipients** field, type an email address and then press Enter. You can enter up to 10 email addresses.
Send Slack message	Send a notification to the specified Slack channel each time the associated search results in an error or warning. From the **Name** list, select the applicable channel.

Create PagerDuty incident	Create a PagerDuty incident each time the associated search results in an error or warning. From the **Name** list, select the applicable configuration.
Send Microsoft Teams message	Send a notification to the specified Microsoft Teams channel each time the associated search results in an error or warning. From the **Name** list, select the applicable channel.
Send webhook notification	Send a webhook notification each time the associated search results in an error or warning. From the **Name** list, select the applicable webhook.
None	Don't send notifications to any recipients for the associated search.

< **Third-Party Detection Exclusions[/documenta** **Next-Gen SIEM Event Investigation > [/documentation/page/ha460e4d/next-gen-siem-event-investigation]**