Third-Party Detection Exclusions

Last updated: May 20, 2025

Overview

For detections generated from ingested third-party data, reduce known unwanted or false-positive detections by creating exclusions. Define criteria for excluding detections generated from integrated third-party data, based on vendor, source product, and other conditions.

A third-party detection exclusion has 2 configurable parts:

- The scope of the exclusion: Specify the vendor and source product for the third-party detections to exclude.
- The conditions of the exclusion: Set one or more conditions for the exclusion to match.

For more info about other types of exclusions, see:

- Machine learning exclusions [/documentation/page/bd0f1c7f/detection-and-prevention-policies#qeece6b6]
- IOA exclusions [/documentation/page/bd0f1c7f/detection-and-prevention-policies#w17527cc]
- Sensor visibility exclusions [/documentation/page/bd0f1c7f/detection-and-prevention-policies#s76b1363]
- Excluding mobile detections [/documentation/page/dfff3f04/configuring-falcon-for-mobile#la01b72f]
- Detections exclusions [/documentation/page/o242b094/falcon-data-protection#h415a6b0] for Falcon Data Protection

Requirements

- **Subscription**: Falcon Insight XDR
- **Role**: Falcon Administrator

Understanding third-party detection exclusions

When you ingest data from third-party sources, the Falcon platform might detect activity that you expect and allow in your environment. By creating third-party detection exclusions, you can stop specific detections from being generated from integrated third-party data. The third-party data is still ingested and available, but the detection does not appear in Next-Gen SIEM **Detections**. For general info about exclusions, see Exclusions [/documentation/page/bd0f1c7f/detection-and-prevention-policies#q73c989a].

Setup

Requires complete setup. In order to exclude detections generated from ingested third-party data, you must create third-party detection exclusions, based on specific criteria you define.

Plan your third-party detection exclusions

When you're creating or editing a third-party detection exclusion, you can review a list of detections that wouldn't have been generated if the current exclusion were live in your environment. Previewing detections that you would no longer see helps you quickly understand the expected effect of an exclusion before you save it.

For more info, see Plan your exclusions [/documentation/page/bd0f1c7f/detection-and-prevention-policies#qbbee61f].

Manage third-party detection exclusions

Create third-party detection exclusions

Create a third-party detection exclusion from within a detection. The exclusion pattern is prepopulated based on the detection. Verify or change the pattern, as needed, before saving the exclusion.

> **Note:** Alternatively, you can create a third-party detection exclusion from scratch on the **Detection exclusions** tab at **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]**.

1. On **Endpoint security > Monitor > Endpoint detections [/activity-v2/detections]**, for the third-party detection from which you want to create an exclusion, click the **Open menu** ⋮ .
2. Select **Create exclusion**.
3. Enter a name and a description for the exclusion. Descriptions are optional but are helpful if you're managing a large number of exclusions.
4. Update the scope and any conditions, as needed.

   > **Important:** When setting the conditions of the exclusion, you must place any wildcard asterisks (*) at the beginning or end of the string. Wildcards are not supported for custom field names.

5. Recommended. Enter a comment for the audit log.
6. If you don't want to activate the exclusion right away, deselect **Activate exclusion on creation**.

7. Click **Next**.

8. Carefully review the list of detections that wouldn't appear if the updated exclusion were already in place.

9. Click **Create exclusion**.

View third-party detection exclusions

From the **Detection exclusions** tab you can view, create, edit, and delete third-party detection exclusions, and view the third-party detection exclusion audit log. By default, the list of exclusions is sorted by **Last modified**.

- Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]**, and then go to the **Detection exclusions** tab.

Edit third-party detection exclusions

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]**, and then go to the **Detection exclusions** tab.

2. Select the exclusion you want to modify.

3. From the **Open menu** ⋮ , click **Edit**.

4. Modify settings as described in Create third-party detection exclusions [/documentation/page/i499c81a/third-party-detection-exclusions-0#b2e0a5d1].

5. Recommended. Enter a comment for the audit log.

6. Click **Next**.

7. Carefully review the list of detections that wouldn't appear if the updated exclusion were already in place.

8. Click **Update**.

Delete third-party detection exclusions

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]**, and then go to the **Detection exclusions** tab.

2. Select the exclusion you want to modify.

3. From the **Open menu** ⋮ , click **Delete**.

4. Review the list of changes that would apply if the exclusion were deleted.

5. Recommended. Enter a comment for the audit log.

6. Click **Delete exclusion**.

View the third-party detection exclusions audit log

View the history of changes to your third-party detection exclusions.

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]**.

2. On the **Detection exclusions** tab, click **See audit log**.

3. Sort the columns to adjust your view of the log. In the **Action** column, logged revisions are defined as **Created**, **Updated**, **Deleted**, **Activated**, or **Deactivated**.

4. Click any revision to see the **Audit log details**.

‹ Detection Monitoring[/documentation/page/ke886083/unifie Correlation Rules › [/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents]