

Manage detections

Published: 2020-02-23

The Detections page provides tools to manage and triage detections for investigation. You can acknowledge detections that you have reviewed, hide low priority detections from view, or connect detections to cases in your ticket tracking system.

To learn about ticket tracking, see [Configure ticket tracking for detections](#).

Acknowledge detections

Acknowledgements provide a visual way to identify that a detection has been seen. You can acknowledge a detection to let team members know that you are investigating a ticket or that the issue has been triaged and should be prioritized for follow-up.

Here are important considerations about acknowledging detections:

- An acknowledgement does not hide the detection.
- After a detection is acknowledged, a timestamp and the username of person who acknowledged the detection is displayed.
- Users must have limited-write or higher privileges to acknowledge a detection or clear an acknowledgement.
- An acknowledgement can be cleared by any user.
- You can filter the detections list by acknowledgement status.
- Acknowledgements generate entries in the [audit log](#), which is accessed from the Admin UI.

To acknowledge a detection, complete the following steps:

1. Log into the Web UI of the Discover or Command appliance, and then click **Detections** at the top of the page.
2. From a detection, click **Acknowledge** from the lower-right corner.
The detection displays the username and timestamp.

Next steps

To clear an acknowledgement, click **Reset**.

Hide detections from view

Detection rules enable you to hide low-priority detections and increase the discoverability of important detections. For example, you might want to hide a vulnerability scanner detection that is expected, but occurs frequently. Or, you might want to hide detections about expiring certificates because that issue is handled by a different team.

When a rule is enabled, detections that match the specified criteria are hidden from view in the detections list. Hidden detections also affect the following areas:

- Triggers and alerts associated with hidden detections do not run while the rule is enabled.
- Detection markers for hidden detections are not displayed on charts.
- Hidden detections do not appear on activity maps.
- Detection counts on related Web UI pages, such as the Device Overview page or the Activity page, do not include hidden detections.

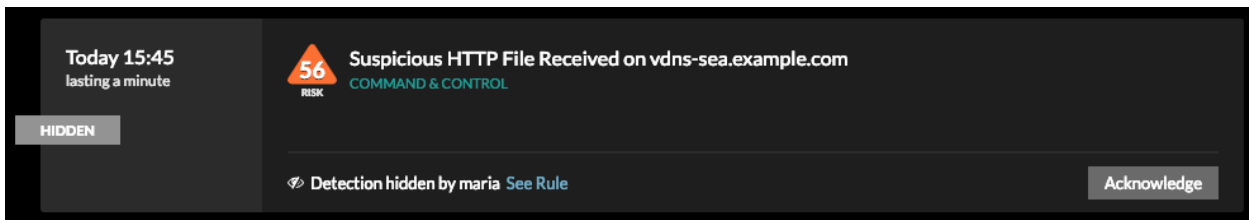
You can view detection rules by clicking **Manage Detection Rules** from the lower-left corner of the Detections page.

Rule ID	Rule Status	Detection	Offender	Victim	Created By	Created On	Expires On	Hidden Detections	Description
109	Disabled	Suspicious File Download on Critical Server	workstation-03	Any device	maria	2019-03-22 10:07:21	2019-03-22 18:07:21	240	--
108	Disabled	Suspicious HTTP Port	Primary SNAT	Any device	beverly	2019-03-22 10:04:38	2019-03-22 18:04:38	564	--
102	Enabled	Suspicious HTTP File Received	Cisco FFFC28	sea-server	ethan	2019-03-18 11:05:28	2019-03-27 00:28:41	9	--

From the Manage Detection Rules table, you can extend the duration of a rule, re-enable a rule, and disable or delete a rule.

After you disable or delete a rule, the rule expires immediately and associated triggers and alerts resume. After you disable a rule, previously hidden detections remain hidden; ongoing detections appear. Deleting a rule displays previously hidden detections.

You can temporarily show hidden detections on the Detections page by selecting the Show Hidden Detections checkbox. Showing hidden detections does not disable detection rules; the option enables you to temporarily view hidden detections to the detections list. Each hidden detection includes a link to the associated detection rule, and displays the username of the user that created the rule, similar to the following figure:



Create a detection rule

Detections that match the specified criteria in the rule are hidden from view in the detections list, activity maps, Device Overview pages, and protocol pages. Hidden detections do not show detection markers on charts, and associated triggers and alerts do not run.

Here are important considerations about detection rules:

- You can only create a detection rule from an existing detection, that detection is not hidden unless the detection is ongoing when the rule is created.
 - You can choose to hide past detections when creating a rule.
 - You must have full-write or higher privileges to create and manage detection rules.
 - Detection rules generate entries in the [audit log](#), which is accessed from the Admin UI.
- Log into the Web UI of the Discover or Command appliance, and then click **Detections** at the top of the page.
 - From a detection in the list, click **Hide Detections Like This**. A dialog box appears and automatically displays the title, offender, and victim from the selected detection.
 - From the **Offender** drop-down list, select one of the following options:
 - An original offender device
 - A device group that contains the original offenders, if available
 - Any device
 - From the **Victim** drop-down list, select one of the following device options:
 - An original victim device
 - A device group that contains the original victims, if available
 - Any device

5. From the **Rule Expiration** drop-down list, select the duration to hide the detection.
Select **Never** to create a rule that never expires.
6. Optional: Type a description of the rule.
7. Optional: Select the **Hide matching past detections** checkbox to hide past detections that match the rule criteria.
8. Click **Create**.
The rule is displayed in the Manage Detection Rules table.