Manage detections

Published: 2019-10-18

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**.

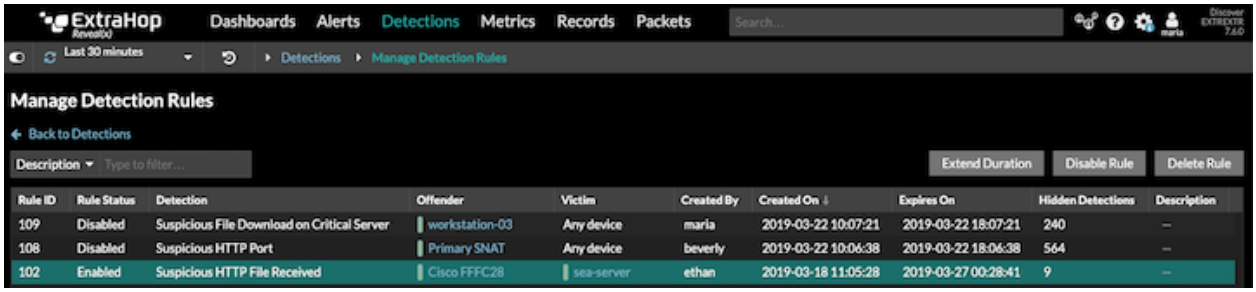
Hide detections from view

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.

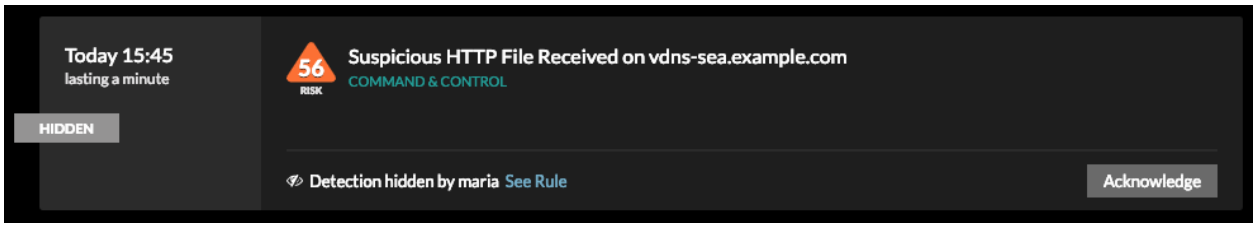
You can view detection rules by clicking **Manage Detection Rules** from the lower-left corner of the Detections page.



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.

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 in the list, click **Hide Detections Like This**.
   A dialog box appears and automatically displays the title, offender, and victim from the selected detection.
3. 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
4. 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.

Specify custom parameters

By providing information about your network environment, you can help improve the quality and accuracy of rules-based detections. These detections are generated from triggers that are authored by ExtraHop.

If your ExtraHop deployment includes a Command appliance, we recommend that you configure these settings on the Command appliance, and then transfer management from connected Discover appliances to the Command appliance.

Note: Parameter fields on this page might be added, deleted, or modified over time by ExtraHop.

1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click the System Settings icon and then click **Custom Parameters**.
3. Specify values for any of the following parameters available on the page.

Option	Description
Gateway Devices	By default, gateway devices are ignored by rules-based detections because they can result in redundant or frequent detections. Select this option to identify potential issues with gateway devices like your firewalls or routers.
L2 Devices	By default, L2 devices are ignored by rules-based detections because they can create duplicate entries for L2 and L3 layer data. Select this option to identify detections on new L2 devices that have not yet reached standard analysis.
Tor Nodes	By default, Tor nodes are ignored by rules-based detections because they can result in low-value detections in environments with minimal Tor traffic. Select this option to identify detections on devices communicating through the Tor network if your environment observes substantial Tor traffic.
Approved Public DNS Servers	Specify public DNS servers allowed in your environment that you want rules-based detections to ignore. Specify a valid IP address or CIDR block.
Approved Internal DNS Servers	Specify internal DNS servers allowed in your environment that you want rules-based detections to ignore.

Option	Description
	From the drop down list, start typing the name of the device, and then select a device from the filtered list.
Allowed HTTP CONNECT Targets	Specify URIs that your environment can access through the HTTP CONNECT method. URIs must be formatted as ***<hostname>:<port number>***. Wildcards and Regex are not supported.
Approved HTTP Ports	Specify non-standard server ports in your environment that you want rules-based detections to ignore when HTTP traffic is observed on these ports. Type a single HTTP port number per field.
Approved SSH Ports	Specify non-standard server ports in your environment that you want rules-based detections to ignore when SSH traffic is observed on these ports. Type a single SSH port number per field.
Approved User Agents	Specify HTTP user agents in your environment that you want rules-based detections to ignore. Type a single user agent per field.

4. Click **Save**.