# Manage detections

Published: 2020-05-22

You can acknowledge or hide detections directly from any detection card displayed on the main Detections page.

## 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. You can also filter your view of detections to show only unacknowledged detections.

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, even if they are not the user that originally acknowledged the detection.

To acknowledge a detection, complete the following steps:

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Detections**.
3. Click **Acknowledge** from the lower-left corner of the detection card.

   The detection displays the username and timestamp. Click **Reset** to clear an acknowledgement.

## Hide detections from view

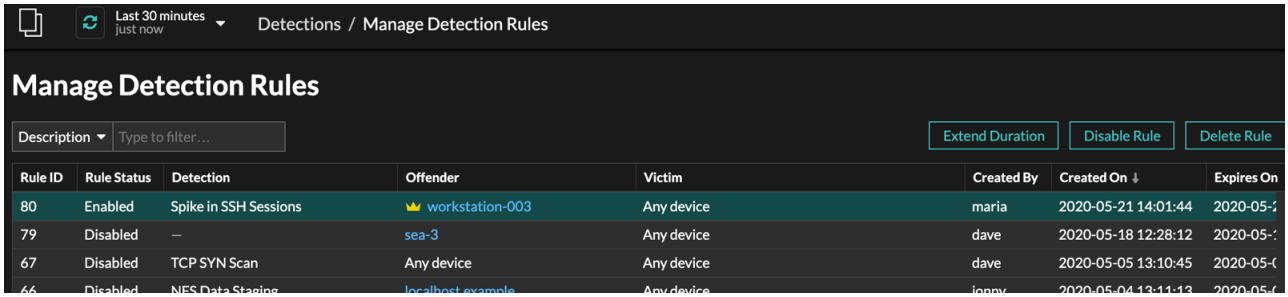
Hidden detections are removed from throughout the system where detections are displayed. By creating a detection rule, you can hide low-priority detections and increase the discoverability of important detections. For example, you might want to hide a vulnerability scanner detection that is expected, 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 and 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.

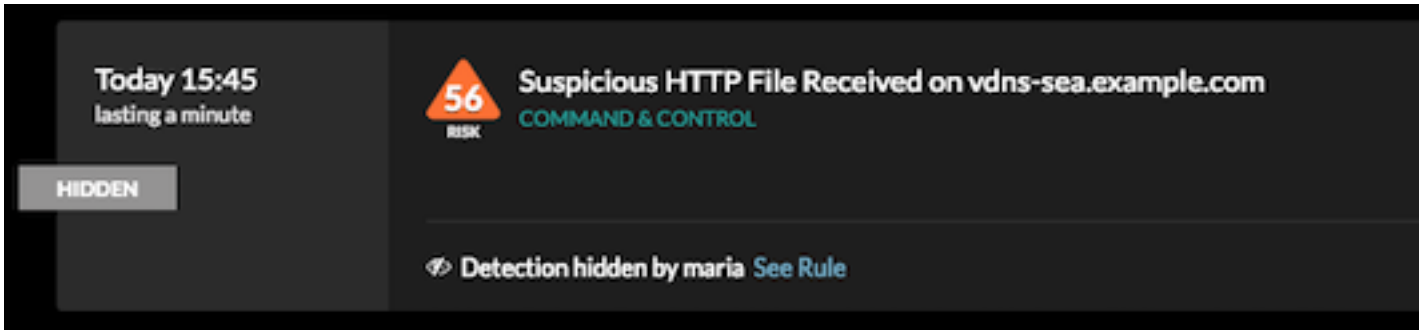
© 2020 ExtraHop Networks, Inc. All rights reserved.




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, without disabling the detection rules. 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

### Before you begin

You must have full-write or higher privileges to create and manage detection rules.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Detections**.
3. From a detection card, click **Hide**.
   A dialog box appears and automatically displays the title, offender, and victim from the selected detection.
4. 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
5. 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
6. From the **Rule Expiration** drop-down list, select the duration to hide the detection.
   Select **Never** to create a rule that never expires.
7. Optional: Type a description of the rule.

8. Optional: Select the **Hide matching past detections** checkbox to hide past detections that match the rule criteria.
9. Click **Create**.
   The rule is displayed in the Manage Detection Rules table.