Tune detections

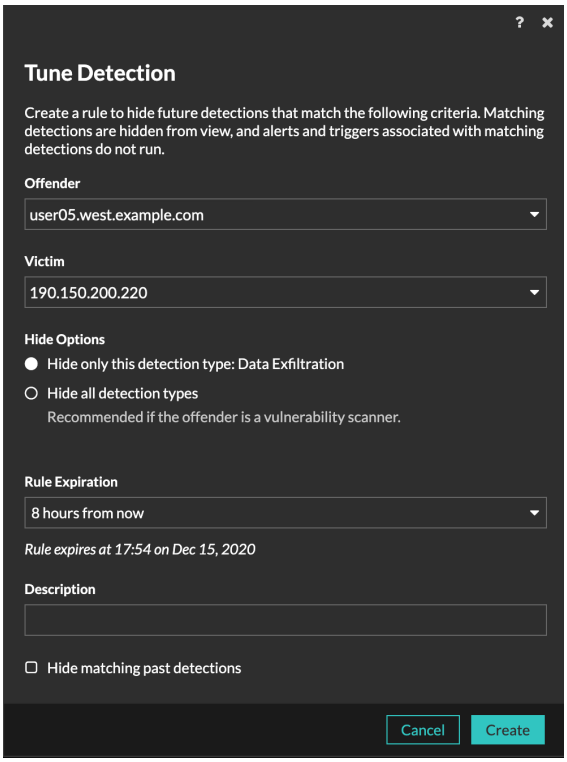
Published: 2021-10-27

Detection tuning enables you to better control which detections are visible or generated for your network.

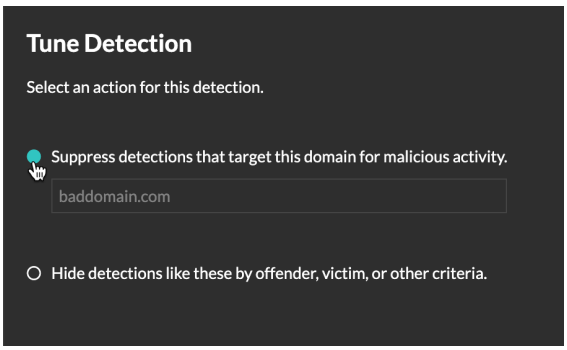
For example, you might want to hide a vulnerability scanner detection that is expected, but occurs frequently. Or, you might have an internal device that regularly phones home to a trusted domain for an external licensing server that results in a Command-and-Control Beaconing detection.

There are two ways to tune a detection: you can hide a detection throughout the system based on specific criteria, or you can add trusted domains and suppress certain detections based on suspicious domain activity.

Most detections can be hidden by creating a tuning rule:



However, if the detection involves suspicious activity for a domain, you must select from the following options:



© 2021 ExtraHop Networks, Inc. All rights reserved.

When you hide a detection, a tuning rule is created on the Manage Tuning Rules page. Detections that match the specified criteria are hidden from view and affect the following system 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 pages, such as the Device Overview page or the Activity page, do not include hidden detections.

When you add a trusted domain, an entry is added to the Network Localities page. Future detections that target malicious domain activity for that trusted domain are suppressed. Note that you can also directly add trusted domains to the Network Localities page.

Tune a detection from a detection card

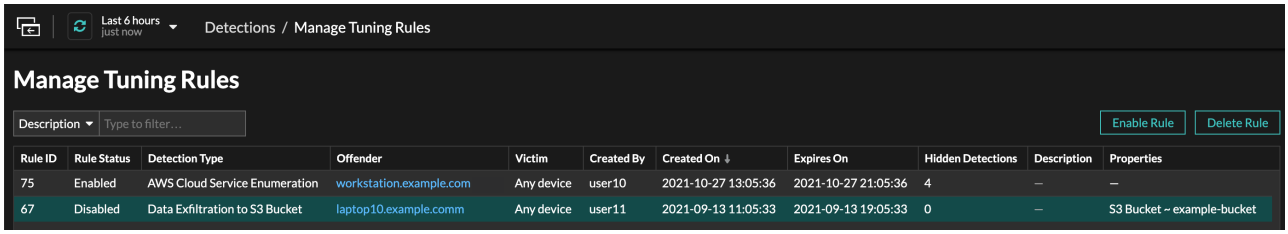
Before you begin
Users must have full write or higher privileges to tune a detection.

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 **Actions** from the lower-left corner of the detection card.
4. Click **Tune Detection...**.
5. Different options appear depending on the type of detection. Select the criteria that you want and then click **Save**.
    - Detections are suppressed for trusted domains, and the domain is added to the Network Localities page.
    - Detections that are hidden are added to the Manage Tuning Rules page.

Manage Tuning Rules

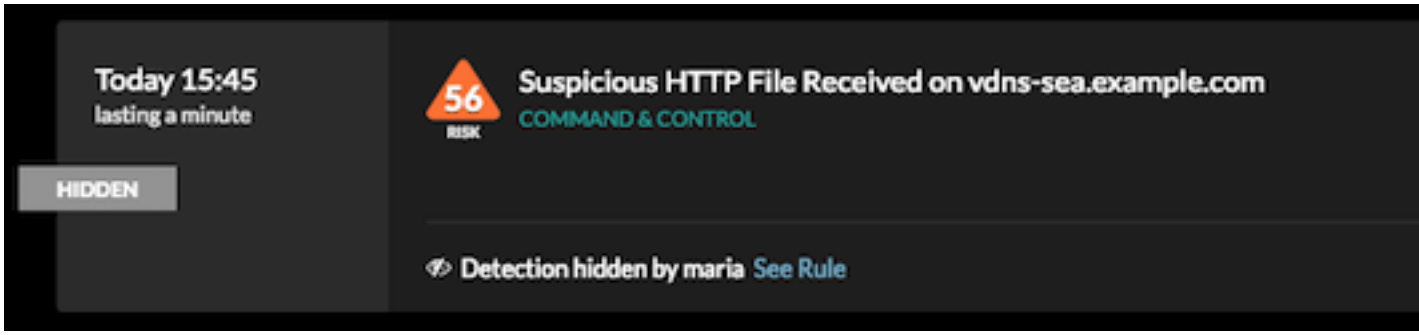
You can extend the duration of a rule, re-enable a rule, and disable or delete a rule from the Manage Tuning Rules page.

Click **Manage Tuning Rules** from the lower-left corner of the Detections page.



- 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 tuning rules. Each hidden detection includes a link to the associated tuning rule, and displays the username of the user that created the rule, similar to the following figure:


Today 15:45
lasting a minute
HIDDEN
56
RISK
Suspicious HTTP File Received on vdns-sea.example.com
COMMAND & CONTROL
Detection hidden by maria See Rule