Tune detections

Published: 2023-06-14

Detection tuning enables you to reduce noise and surfaces critical detections that require immediate attention.

There are two ways to tune detections: you can add tuning parameters that suppress detections from ever being generated, or you can create tuning rules that hide existing detections based on detection type, participants, or detection properties.

Tuning Parameters

Tuning parameters enable you to specify known and trusted domains, DNS servers, HTTP CONNECT targets, and HTTP user agents that should not generate a detection. You can also enable tuning parameters that suppress frequent and redundant detections associated with gateway devices and tor nodes.

Tuning parameters are managed from the Tuning Parameters page and trusted domains are managed from the Network Localities page.

Tuning Rules

Tuning rules enable you to specify criteria that hide detections that have been generated, but are of low-value and do not require attention.

Note: Tuning rules might not hide certain detections if your packet sensors are not running the same firmware version as your console.

Tuning rules hide all past, current, and future detections and participants that match the specified criteria and affect the following system areas:

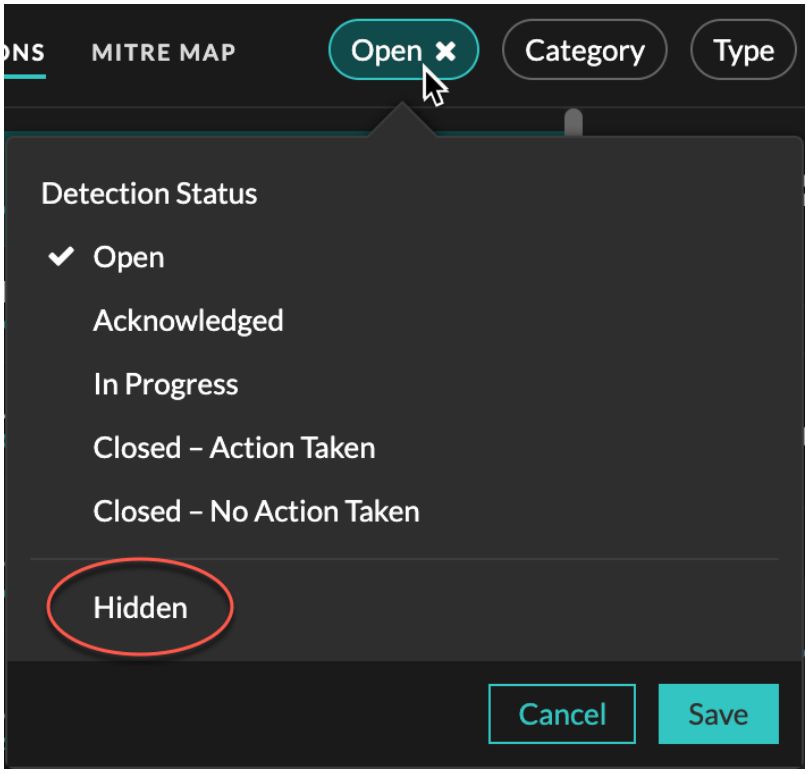
- Hidden detections do not cause related triggers and alerts to run while the rule is enabled.
- Hidden detections do not appear as detection markers in charts.
- Hidden detections do not appear on activity maps, but hidden participants will appear in investigation maps.
- Hidden detections do not appear in detection counts on related pages, such as the Device Overview page or the Activity page.
- Hidden detections and participants do not appear in the Executive Report.
- Hidden detections are not included in email and webhook notifications.

Note: If you do not see detection markers for any detections, confirm that detection markers have not been disabled.

View hidden detections

By applying the Hidden status on the Detections page, you can view detections that are currently hidden by a tuning rule.

The Open filter is selected by default on the Detections page. Click the **Open** filter to access other filter options. If the Open filter is not applied, click **Status** to view filter options, and then click **Hidden**. The summary for only hidden detections appears.



The summary identifies the tuning rules that are currently hiding the selected detections, hidden participants, detection properties, and network localities.

Click any tuning rule, participant, property, or network locality value to view a summary of hidden detections associated with the selected value.

Participants

Lists both Offenders and Victims that are currently hidden. The Offender and Victim lists are ordered by the number of detections where the participant is hidden.

Property Values

Lists the property values associated with the hidden detection type. The Property Values list is ordered by the number of detections where the property value is hidden.

Affected Network Localities

Lists the network localities that contain hidden detections of the selected type. The Affected Network Localities list is ordered by the number of hidden detections in the network locality.

By filtering results for a single tuning rule, participant, property, or locality, you can view the number of hidden detections associated with the specified value. Click the **Show Detections** button to view individual detection cards.

Tuning best practices

It is better to create a single parameter or rule that is more broad instead of creating multiple overlapping parameters and rules.

Here are some recommendations to help optimize your detection tuning:

- Start by adding tuning parameters to avoid detections that involve known or trusted agents. Be sure to review the Tuning Parameters and Network Localities pages for existing parameters to avoid redundancy.

- Determine if you want to hide all detections for a specific participant, such as a vulnerability scanner, and select **All detection types**. If you want to hide by device role, increase the scope to device group.
- When an **IP Address or CIDR Block** is selected in the Offender or Victim dropdown, add or remove entries from the list in the IP Addresses field to increase or reduce the scope of the tuning rule.
- By default, tuning rules expire after 8 hours. You can select a different expiration time from the dropdown or select a new expiration time after you re-enable an expired rule from the Tuning Rules page.
- The ExtraHop system automatically deletes detections that have been on the system for 21 days since the start time of the detection, that are not ongoing, and that are hidden. If a newly created or edited tuning rule hides a detection that matches this criteria, the affected detection will not be deleted for 48 hours.
- When adding a tuning rule, if you identify a device that is not classified correctly, you can change the device role.
- Certain detections might require a precise tuning rule based on a specific property of the detection. Under the Property heading, click the checkbox next to a property to specify a value or regular expression and add criteria for a focused tuning rule.
- Apply the **Hidden** status filter to the Detections page to view detections that are currently hidden by tuning rules.

Learn how to suppress detections with tuning parameters and hide detections with tuning rules.