

Hide detections with tuning rules

Published: 2024-07-12

Tuning rules enable you to hide detections that match specified criteria.

To avoid creating redundant rules, make sure to first add information about your network environment to the ExtraHop system by [specifying tuning parameters](#).

Learn more about [tuning detections](#).

Create a tuning rule

Create tuning rules to streamline your detection list by specifying criteria that hide past, present, and future detections that are of low-value and do not require attention.

Before you begin

Users must have full write or higher [privileges](#) to create a tuning rule.

Learn about [tuning best practices](#).

Add a tuning rule from a detection card

If you encounter a low-value detection, you can create a tuning rule directly from a detection card to hide similar detections in the ExtraHop system.

Before you begin

Users must have full write or higher [privileges](#) to tune a detection.

Learn about [tuning best practices](#).

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...**

If the detection type is associated with a tuning parameter, you will see an option to [suppress the detection](#). If you still want to create a tuning rule, select the Hide detections like these... option and click Save.

5. Specify the [tuning rule criteria](#) and click **Create**.

The rule is added to the Tuning Rules page. Learn more about [managing tuning rules](#).

Add a tuning rule from a hardening detection

Click a hardening detection to view a summary of all assets, detection properties, and network localities associated with that detection type. You can filter the summary by clicking any of the associated values, and then create a tuning rule to hide detections based on the displayed results.

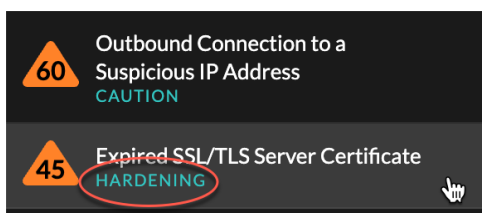
Before you begin

Users must have full write or higher [privileges](#) to tune a detection.

Learn more about [filtering and tuning hardening detections](#).

Learn about [tuning best practices](#).

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 any Hardening detection in the detection list.



4. Filter results on the hardening summary page.
 - a) Click an Affected Asset to only view detections where that asset is a participant in a detection.
 - b) Click a Property Value to only view detections associated with the selected detection property value.
 - c) Click a Network Locality to only view detections where the participant is located in the selected network locality.
5. Click **Create a Tuning Rule**.
Tuning rule criteria are automatically populated to reflect the filtered results of the hardening summary page.
6. Click **Create**.
 The rule is added to the Tuning Rules page. Learn more about [managing tuning rules](#).

Add a tuning rule from the Tuning Rules page

Create tuning rules to hide detections by detection type, participant, or specific detection properties.

Before you begin

Users must have full write or higher [privileges](#) to tune a detection.

Learn about [tuning best practices](#).

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Tuning Rules**.
3. Click **Create**.
4. Specify **tuning rule criteria** and click **Save**.
 The rule is added to the Tuning Rules table.

Tuning rule criteria

Select from the following criteria to determine which detections are hidden by a tuning rule.

Detection type

Create a tuning rule that applies to a single detection type, or choose to have the rule apply to all security or performance detection types, depending on the system module. Rules that encompass all security detection types are typically reserved for activity associated with vulnerability scanners.

Participants

Create a tuning rule that hides detections based on specific offender and victim participants.


Specify participants in a tuning rule with one of the following selections.

Any Offender or Victim

You can specify Any Offender or Any Victim to hide all participants. This option is effective for hiding detections during scheduled testing or vulnerability scanning.

Device Group or Device

You can specify a discovered device or a [device group](#) to hide participants. For example, you can specify the built-in device group for Vulnerability Scanners to hide detections where an internal scanner is a participant.


 **Note:** Tuning rules are applied when detections or tuning rules are created or updated. Tuning rules are not retroactively applied to existing detections when a participant is added or removed from a dynamic device group.

External Scanning Service

You can specify an external scanning service as a participant in a tuning rule. The ExtraHop system hides external scanning services based on the IP address range associated with the service.


IP Address or CIDR Block

You can specify a single IP address or a CIDR block of IP addresses to hide any participant within that range. For example, if a team is performing pen testing on a specific subnet, you can create a tuning rule with the subnet IP addresses to avoid a spike in detections related to enumeration and hacking tools.

 **Note:** Detections are hidden based on the IP address at the time the detection occurs. Because IP addresses for discovered devices and external endpoints can change dynamically, specifying a single IP address is only reliable if the endpoint has a static IP address.


Hostname or Domain

You can specify a hostname, domain name, or Server Name Indication (SNI) to hide a participant that has not been discovered by the ExtraHop system. If you specify a domain name, the tuning rule will hide all subdomains. For example, if you create a tuning rule with vendor.com as the offender, the tuning rule will hide detections with example.vendor.com as the offender. If you specify a subdomain such as example.vendor.com, the tuning rule will only hide detections where the participant ends with that exact subdomain. In this example, test.example.vendor.com would be hidden but test.vendor.com would not.

 **Note:** Tuning rules will not hide discovered devices by hostname. You can add discovered devices as tuning rule criteria by specifying an IP address, device, or device group.

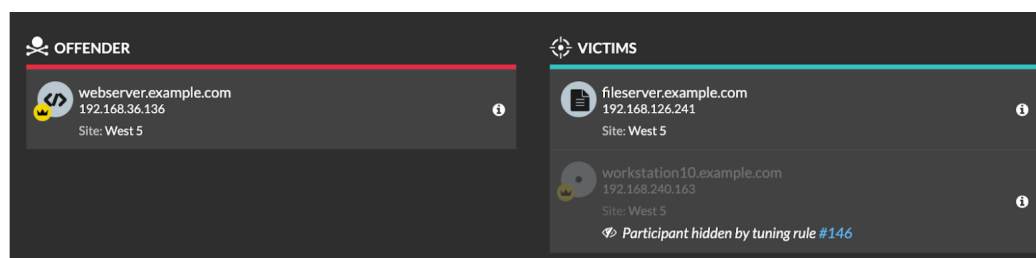
Network Locality

You can specify a [network locality](#) to hide IP address participants in that locality.

 **Note:** Tuning rules will only hide participants with the specific IP addresses that are included in the network locality. If a device is assigned another IP address outside the network locality CIDR block, that device will not be hidden.

Here are some important considerations about tuning participants:

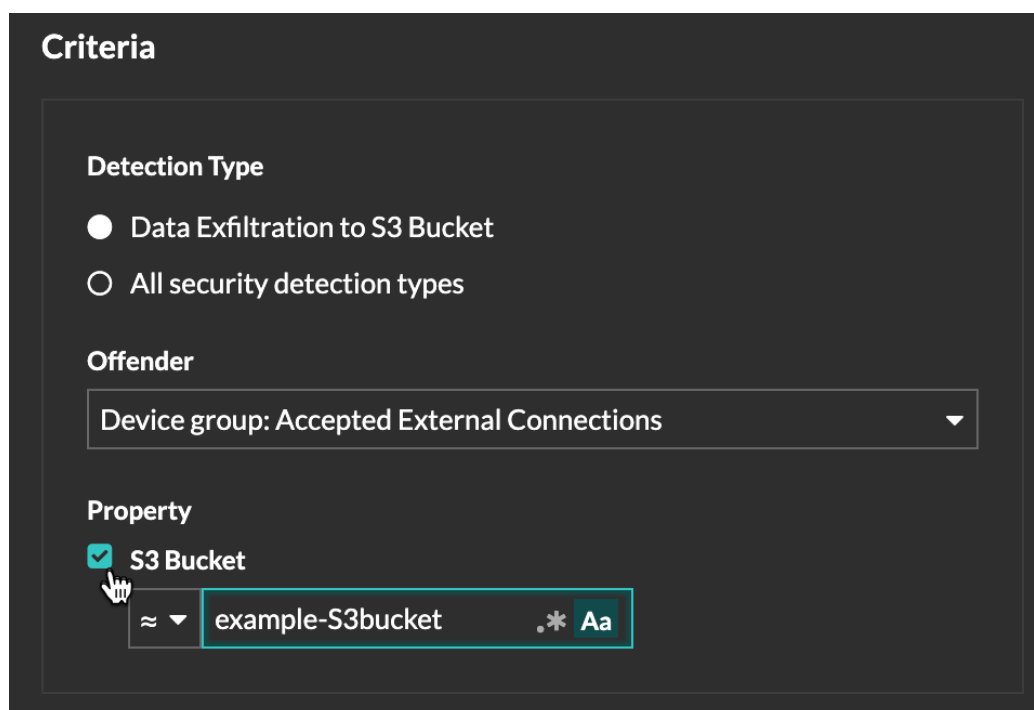
- When the participant criteria for a tuning rule only matches part of the participant list in a detection, the system will hide the specified participants in the tuning rule without hiding the entire detection.



- Participants that are specified as tuning criteria, including CIDR blocks and external scanning services, will be hidden even if they connect through a gateway or load balancer.

Detection properties

Create a tuning rule that hides detections by a specific property. For example, you can hide Rare SSH Port detections for a single port number, or Data Exfiltration to S3 Bucket detections for a specific S3 bucket.



Criteria

Detection Type

- Data Exfiltration to S3 Bucket
- All security detection types

Offender

Device group: Accepted External Connections ▼

Property

- S3 Bucket

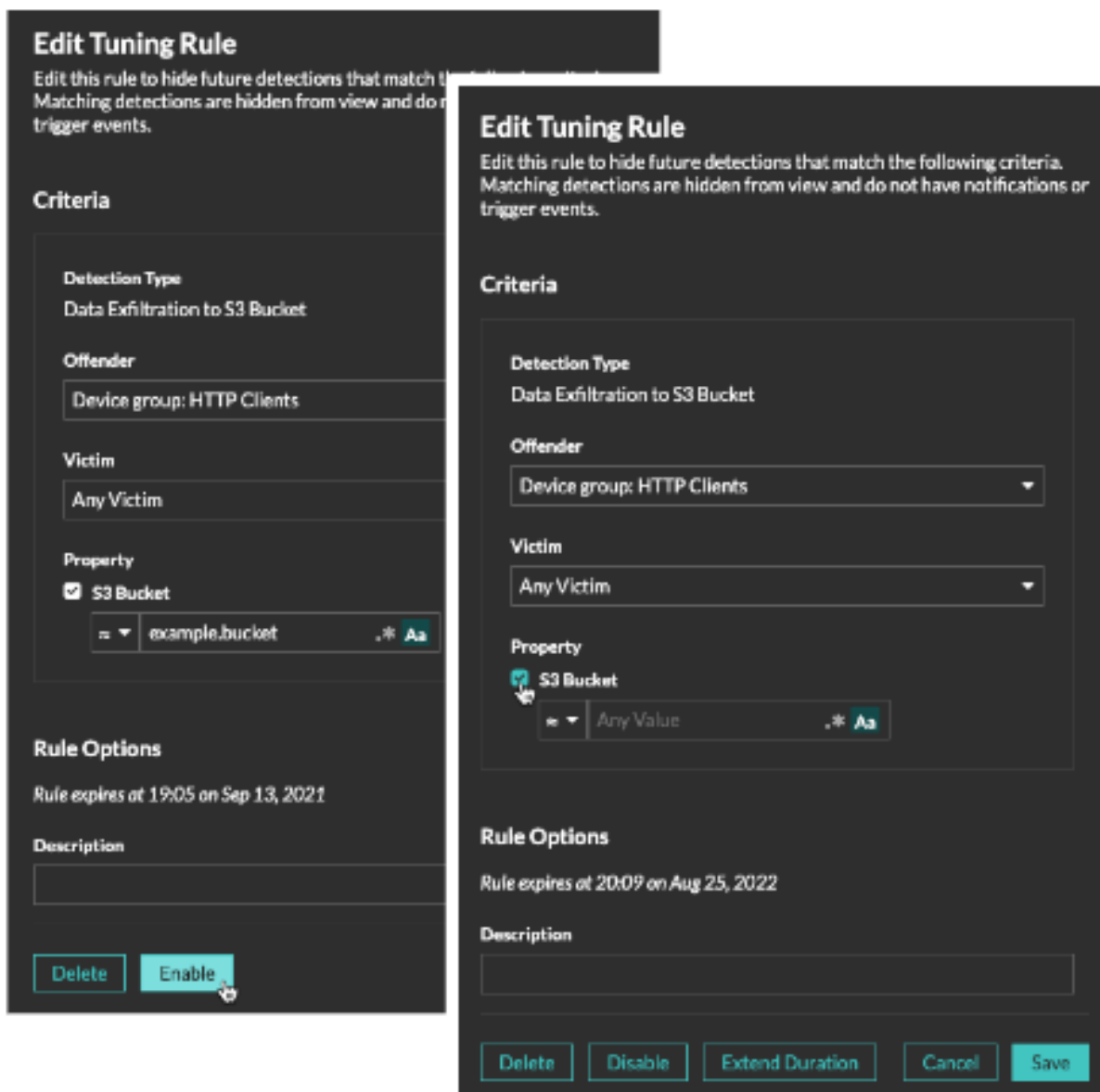
≈ ▼ example-S3bucket . * Aa

Manage Tuning Rules



You can edit the criteria or extend the duration of a rule, re-enable a rule, and disable or delete a rule.

At the top of the page, click the Systems Settings icon  and select **Tuning Rules**.

Click on a tuning rule in the Tuning Rules table to open the Edit Tuning Rule panel. Update participants, rule criteria, or properties to adjust the scope of the rule. Click the buttons at the bottom of the panel to delete, disable, enable, or extend the duration of 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.
- 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.

You can apply the [Hidden status](#)  to the Detections page to only view detections that are **currently hidden**  by a tuning rule.

Each hidden detection or participant includes a link to the associated tuning rule, and displays the username of the user that created the rule. If the detection or participant is hidden by multiple rules, the number of rules that apply appears.

70 VPN Client Data Exfiltration
RISK EXFILTRATION, ACTIONS ON OBJECTIVE

May 24 08:36
lasting an hour

OFFENDER

- VPN Client
192.168.18.45
Site: West 5
Participant hidden by tuning rule #147

VICTIM

- proxy.example.com
192.168.230.45
Site: West 5
Participant hidden by tuning rule #147

Detection hidden by rule #147

Actions ▾

OFFENDER

- webserver.example.com
192.168.36.136
Site: West 5

VICTIMS

- fileserver.example.com
192.168.126.241
Site: West 5
- workstation10.example.com
192.168.240.163
Site: West 5
Participant hidden by tuning rule #146

OFFENDER

- highvalue.example.com
192.168.223.82
Site: West 5
Participant hidden by 2 rules