Hide detections with tuning rules

Published: 2024-04-02

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

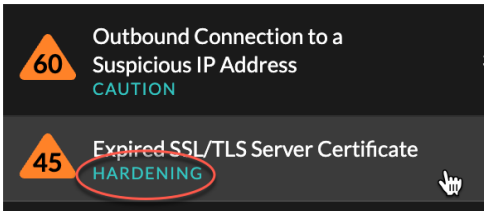
Click a hardening detection to view a summary of all assets, detection properties, and network localities associated with that detection type. You can filter the summary by clicking any of the associated values, and then create a tuning rule to hide detections based on the displayed results.

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.
5. Specify the tuning rule criteria and click **Create**.
   The rule is added to the Tuning Rules page. Learn more about managing tuning rules.

Tuning rule criteria

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

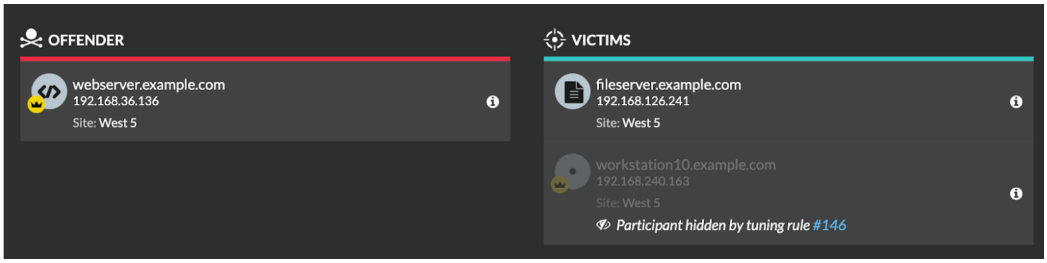
Detection type

You can 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

Identify participants in a tuning rule by IP address, hostname or domain, device name, or network locality. You can also hide participants based on roles identified by the ExtraHop system. For example, when the ExtraHop system identifies an external scanning service, you can hide detections for that specific service, or you can create a tuning rule that hides all external scanning services.

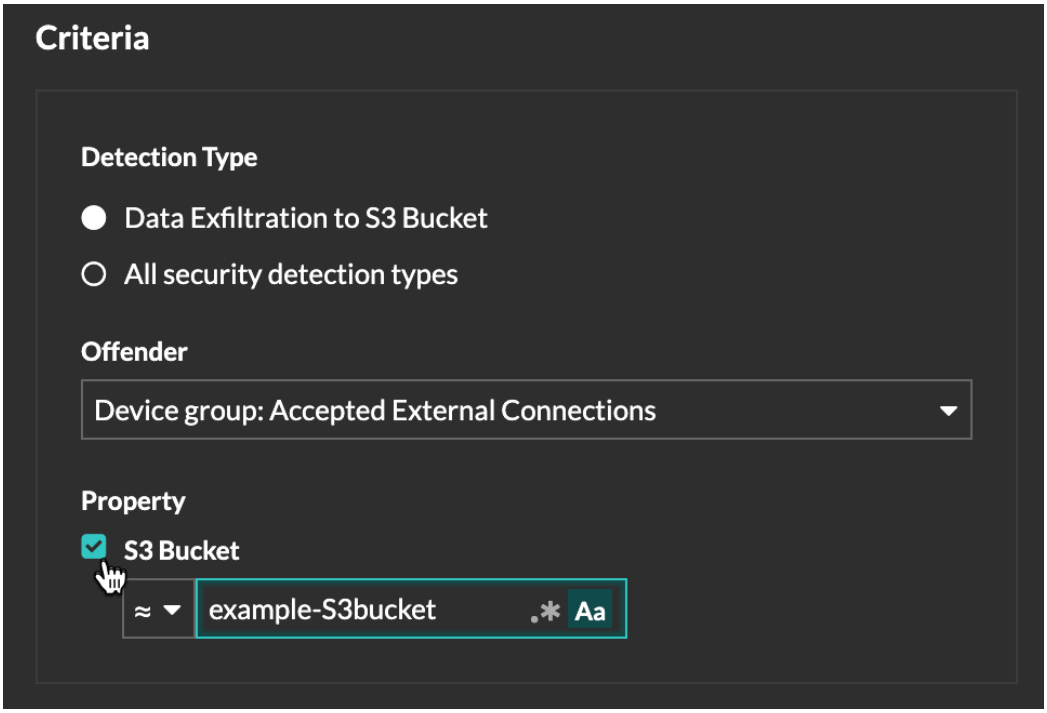
For detections with multiple offenders you can include a list of IP addresses or CIDR blocks, or reference a device group. You can also create tuning rules that hide a single participant without hiding an entire detection.



You can opt to hide all offenders or all victims. For example, you can hide the offender in a noisy scan detection regardless of the victim participants.

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.

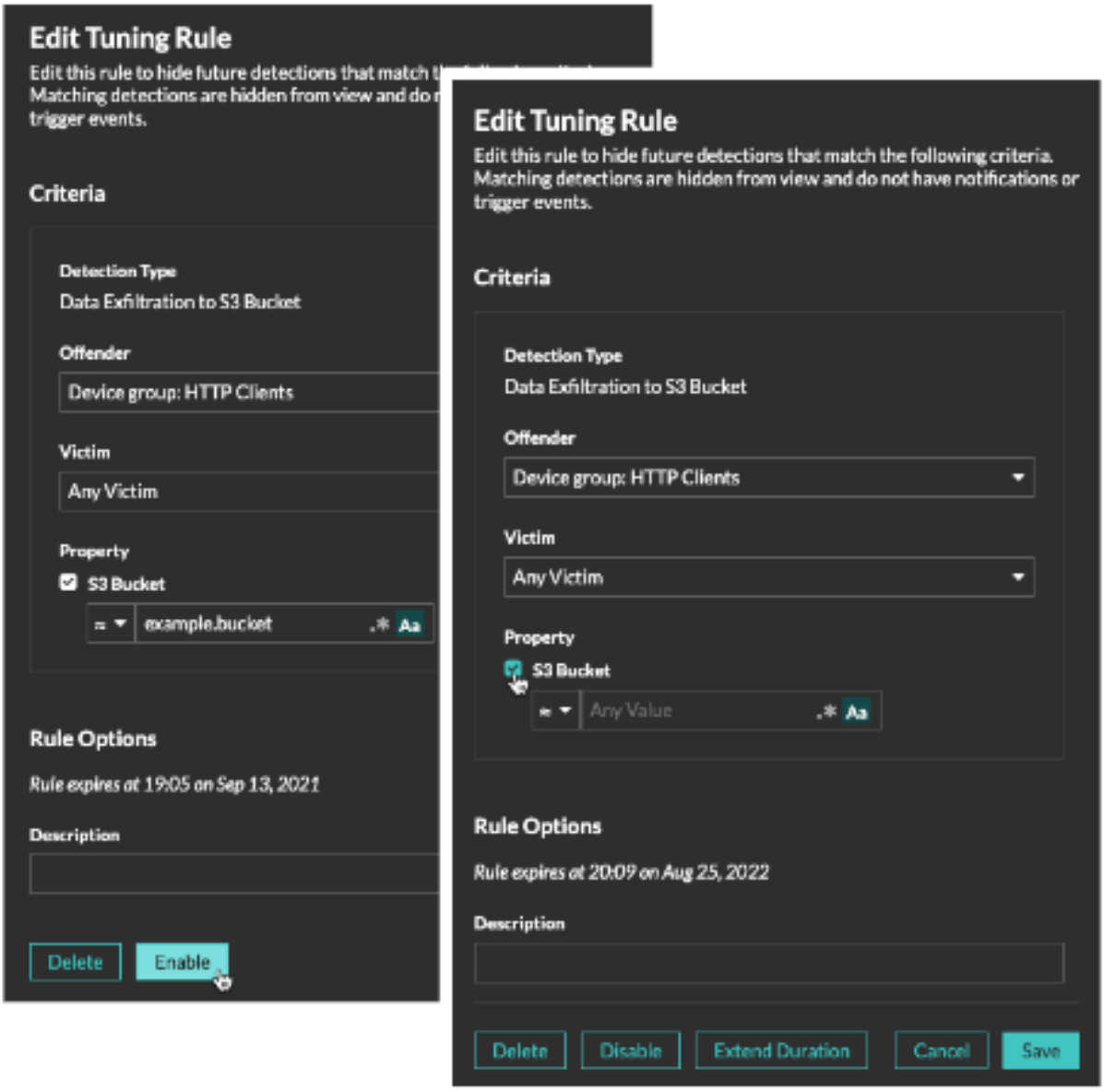


Manage Tuning Rules

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**.

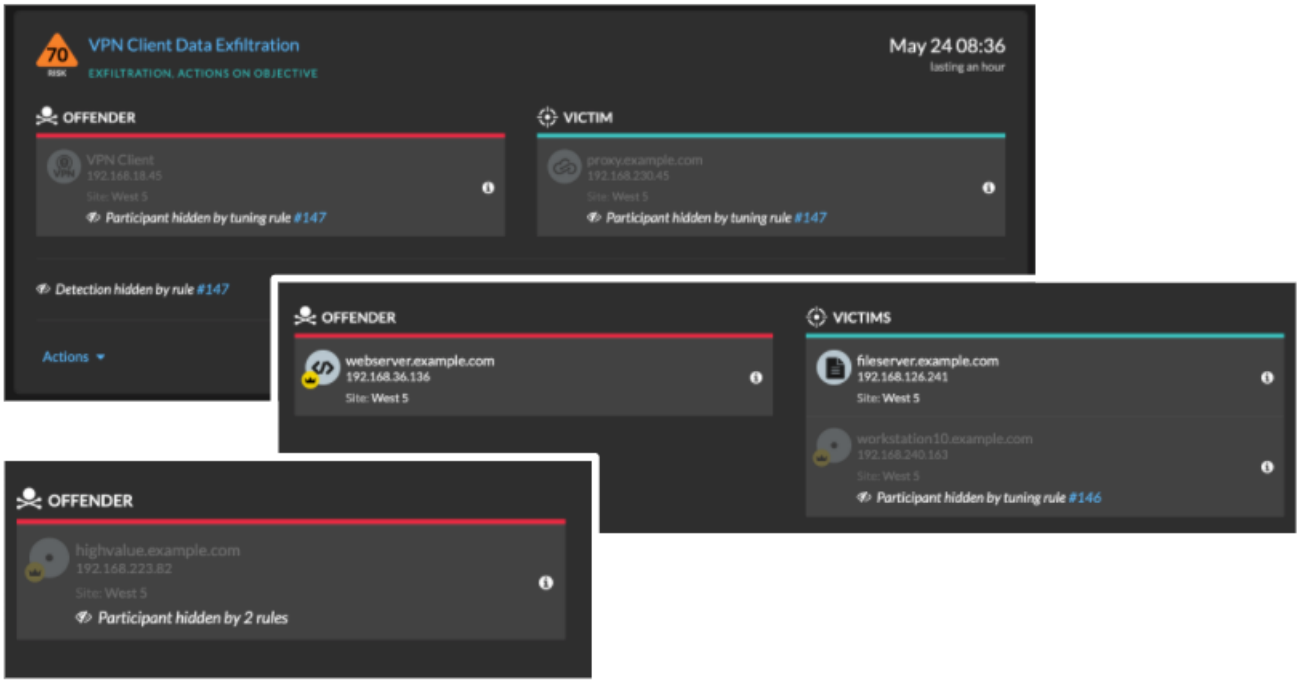
Click on a tuning rule in the Tuning Rules table to open the Edit Tuning Rule panel. Update participants, rule criteria, or properties to adjust the scope of the rule. Click the buttons at the bottom of the panel to delete, disable, enable, or extend the duration of a rule.



- 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
RISK
VPN Client Data Exfiltration
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