Hide detections with tuning rules

Published: 2024-03-27

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 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. Learn more about .
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 detection types. Rules that encompass all detection types are typically reserved for activity associated with vulnerability scanners.

Participants

Identify participants in a tuning rule by IP address, device name, or network locality 🗗. 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.
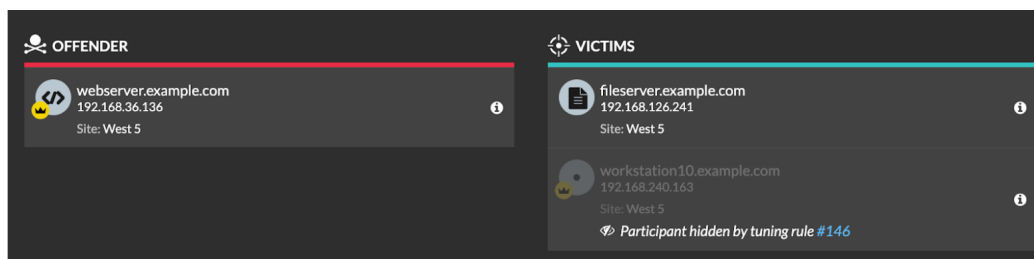
You can opt to hide all offenders or all victims. For example, you can hide the offender in a noisy scan detection regardless of the victim participants.

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.

Criteria

Detection Type

● Hacking Tool Domain Access

○ All detection types

Offender

| webserver.example.com | ▼ |

Victim

| IP Address or CIDR Block | ▼ |

Victim IP Addresses

| 192.168.0.72 ✖   192.168.25.40 ✖   192.168.217.67 ✖ |

Property

☑ Hacking Tool

| ≈ ▼ | Kali Linux | .* 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.

Edit Tuning Rule

Edit this rule to hide future detections that match the following criteria. Matching detections are hidden from view and do not have notifications or trigger events.

Criteria

Detection Type
Data Exfiltration to S3 Bucket

Offender
Device group: HTTP Clients

Victim
Any Victim

Property
☑ S3 Bucket
= ▼ example.bucket .* Aa

Rule Options

Rule expires at 19:05 on Sep 13, 2021

Description

Delete   Enable

Edit Tuning Rule

Edit this rule to hide future detections that match the following criteria. Matching detections are hidden from view and do not have notifications or trigger events.

Criteria

Detection Type
Data Exfiltration to S3 Bucket

Offender
Device group: HTTP Clients   ▼

Victim
Any Victim   ▼

Property
☑ S3 Bucket
= ▼ Any Value .* Aa

Rule Options

Rule expires at 20:09 on Aug 25, 2022

Description

Delete   Disable   Extend Duration   Cancel   Save

- 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 display hidden detections and participants on the Detections page by selecting the **Show Hidden Detections** checkbox, without disabling the tuning rules. 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.