Tune vulnerability scanners

Published: 2025-02-11

Vulnerability scanners generate a large amount of activity on your network while the system continuously scans applications for security weaknesses. By creating tuning rules you can reduce low-value detections that are associated with known scanner activity.

Here are some important considerations about tuning vulnerability scanners:

- Communicate with the teams in your organization that configure scanners. Effective tuning rules require an understanding of scanning targets and schedules.
- Confirm that your ExtraHop sensor is correctly classifying the location of your scanner. For example, if you are hosting a vulnerability scanner in a part of your network that is not observed by an ExtraHop sensor, that traffic will appear as external. You might need to specify a network locality for the traffic before you can add the remote scanner to a tuning rule.
- If you are dealing with cloud-based scanners or need to create a large number of tuning rules, you can tune detections with the ExtraHop REST API.

Inventory vulnerability scanners and targets

Before you begin creating tuning rules, you should review all vulnerability scanners that are active in your environment.

Inventory your scanners

Compile a list of all the vulnerability scanners that are active in your environment, including the following type of details:

- Applicable IP addresses and hostnames for scanning devices.
- The name of your external scanning provider, such as Teneble or Qualys. Only the provider name is needed for most external scanning services as ExtraHop maintains a library of IP addresses for common cloud-based scanning providers.
- Associated CIDR blocks for less common external scanning services.

Inventory your scanner targets

Compile a list of all networks that are a target of vulnerability scanners. Your list should include all networks, CIDR blocks, or device groups that are regularly scanned by your vulnerability scanners.

You now have a list of vulnerability scanner devices to create tuning rules. Local vulnerability scanner devices should appear in the Vulnerability Scanner device group so that you can add the Vulnerability Scanner device group in a tuning rule. Each of your external scanning services can be added to individual tuning rules.

Review the Vulnerability Scanner device group

Confirm that all of your local scanning devices are discovered and classified in the Vulnerability Scanner device group.

The built-in Vulnerability Scanner device group is a dynamic device group. Devices are added automatically after a pattern of scanning activity is established and the source device is classified as a Vulnerability Scanner. If you do not see an expected scanner in the device group, you can wait to see if the device is added dynamically, or you can follow the next steps to change the device role manually.

1. Review the devices in the Vulnerability Scanner device group.
   a) Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
   b) At the top of the page, click **Assets**.

c) Under Devices by Role, click **Vulnerability Scanner**.
d) Click **Devices** to view a list of the vulnerability scanners in your environment.
e) Review the devices and note any scanners from your compiled list that do not appear in the vulnerability scanner device group.

2. Optional: If the ExtraHop system has not automatically classified a scanner, you can change the device role manually.
   a) In the global search field at the top of the page, type the IP address or hostname of the scanner that does not appear in the Vulnerability Scanner device group.
   b) Click the device in the search results to open the device overview page.
   c) Click **Edit Properties**.
   d) Click the **Device Role** drop-down menu and select **Vulnerability Scanner**.
   e) Click **Done**.

   Confirm that the device now appears in the vulnerability scanner device group. Repeat these steps to add all scanners from your compiled list that do not appear in the device group.
3. Optional: Remove any devices that should not appear in the Vulnerability Scanner device group.
   a) Click the device to open the device overview page.
   b) Click **Edit Properties**.
   c) Click the **Device Role** drop-down menu and select the correct role for the device.
   d) Click **Done**.

Create a tuning rule to hide the Vulnerability Scanner device group

Create a tuning rule to hide all detections where the offender is a device that is a member of the built-in Vulnerability Scanner device group.

Before you begin

- You can hide individual devices directly from detections where the device appears as an offender.
- 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. From the Detection Type drop-down menu select **All Security Detection Types**.
5. From the Offender drop-down menu select **Device Group or Device**.
6. In the Device Group or Device field, type `Vulnerability Scanners` then click on the built-in Vulnerability Scanners device group.
7. From the Victim drop-down menu select the target of your scanner, such as a **Device Group or Device**, **IP Address or CIDR Block**, or **Network Locality**.

   We recommend that you do not select **Any Victim** for your vulnerability scanning rules. Adding specific scanning targets to tuning rules avoids accidentally hiding malicious scanning activity.
8. From the Expiration drop-down menu select a value that reflects your internal policies.

   We recommend selecting an expiration value that will prompt you to review your Vulnerability Scanner device group membership.
9. In the Description field, provide details that will help other administrators or analysts understand the scope of the rule.

   For example: “This tuning rule hides all of the vulnerability scanner devices that are in the built-in Vulnerability Scanner device group. Device group membership was last reviewed by Gary on January 30th.”
10. Click **Save**.

The rule is added to the Tuning Rules table.

Add a tuning rule to hide an external scanning service

Create a tuning rule to hide all detections where the offender is an external scanning service.

Note: External scanning services are tuned by IP addresses or CIDR blocks, which can be masked by load balancers or gateway devices in your network. If you create a rule that is failing to hide an external scanning service, you might need to specify a network locality or create a custom device with the service CIDR block, and then create a tuning rule with your new locality or custom device.

Before you begin

- Obtain the name of your scanning service provider. The ExtraHop system will automatically supply the IP addresses for common external scanning services. For less common providers, obtain the CIDR block associated with the service.
- You can hide individual devices or external scanning services directly from detections where the device appears as an offender.
- 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. From the Detection Type drop-down menu select **All Security Detection Types**.
5. From the Offender drop-down menu select **External Scanning Service**.

   The ExtraHop system maintains a catalog of CIDR blocks associated with external scanning services. Not all services are included. You can click the External Scanning Service drop-down menu to review the full list of covered services and confirm that your services are included.

   If you do not see your service, change your Offender selection to **IP Address or CIDR Block** and enter the CIDR block provided by your external scanning service.
6. In the External Scanning Service field, select one of the following options:
   - Select **Any External Scanning Service** to hide traffic from all IP addresses associated with external scanning services. Then, click **Save**.
   - Select the name of your external scanning service. You can select multiple scanning services. Then, click **Save**.
7. From the Victim drop-down menu select **Any Victim**.
8. From the Expiration drop-down menu select a value that reflects your internal policies.

   We recommend selecting an expiration value that will prompt you to review your active external scanning services.
9. In the Description field, provide details that will help other administrators or analysts understand the scope of the rule.

   For example: “This tuning rule hides all detections where our Qualys or Rapid7 scanning service is the offender. Scanning services were last reviewed by Gary on January 30.”
10. Click **Save**.

    The rule is added to the Tuning Rules table.