Suppress detections with tuning parameters

Published: 2022-09-21

Provide information about your network environment so that the ExtraHop system can suppress low-value or redundant detections from ever being generated.

You can add tuning parameters from the Tuning Parameters or Network Localities pages, or you can add them directly from a detection card. In addition, you can classify IP address ranges as internal or external to your network.

Learn more about tuning detections.

Specify tuning parameters for detections and metrics

Specify tuning parameters to improve metrics and suppress low-value detections from ever being generated.

If your ExtraHop deployment includes a console, we recommend that you transfer management of all connected sensors to the console.

Note: The fields on this page might be added, deleted, or modified over time by ExtraHop.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Tuning Parameters**.
3. Specify values for any of the following parameters available on the page.

Option	Description
Gateway Devices	By default, gateway devices are ignored by rules-based detections because they can result in redundant or frequent detections. Select this option to identify potential issues with gateway devices such as your firewalls, routers, and NAT gateways.
Inbound Tor Nodes	By default, inbound connections from known Tor nodes are ignored by rules-based detections because they can result in low-value detections in environments with minimal Tor traffic. Select this option to identify detections on inbound connections from known Tor nodes if your environment observes substantial incoming Tor traffic.
Outbound Tor Nodes	By default, outbound connections to known Tor nodes are ignored by rules-based detections because they can result in low-value detections in environments with minimal Tor traffic. Select this option to identify detections on outbound connections to known Tor nodes if your environment observes substantial outgoing Tor traffic.
Accelerated Beaconing Detection	By default, the ExtraHop system detects potential beaconing events over HTTP and SSL.

Option	Description
	Select this option to detect beaconing events faster than the default detection. Note that enabling this option can increase the detection of beaconing events that are not malicious.
Privileged Active Directory Accounts	Specify regular expressions (regex) that match privileged Active Directory accounts in your environment. The parameter list includes a default list of regular expressions for common privileged accounts that you can edit. The ExtraHop system identifies privileged accounts and tracks account activity in Kerberos records and metrics.
Allowed DNS Sinkhole IP Addresses	Specify sinkhole IP addresses that are allowed to be returned in DNS query responses that you want rules-based detections to ignore. Specify a valid IP address or CIDR block. If you do not specify a value, detections that rely on this parameter are not generated.
Approved Public DNS Servers	Specify public DNS servers allowed in your environment that you want rules-based detections to ignore. Specify a valid IP address or CIDR block. If you do not specify a value for this parameter or for **Approved Internal DNS Servers**, detections that rely on this parameter might not be generated.
Approved Internal DNS Servers	Specify internal DNS servers allowed in your environment that you want rules-based detections to ignore. From the drop-down list, start typing the name of the device, and then select a device from the filtered list. If you do not specify a value for this parameter or for **Approved Public DNS Servers**, detections that rely on this parameter might not be generated.
Allowed HTTP CONNECT Targets	Specify URIs that your environment can access through the HTTP CONNECT method. URIs must be formatted as *<hostname>:<port number>*. Wildcards and Regex are not supported. If you do not specify a value, detections that rely on this parameter are not generated.
Approved User Agents	Specify HTTP user agents in your environment that you want rules-based detections to ignore.

Option	Description
	Type a single user agent per field.

4. Click **Save**.

Next steps
Click **Detections** from the top navigation menu to view detections.

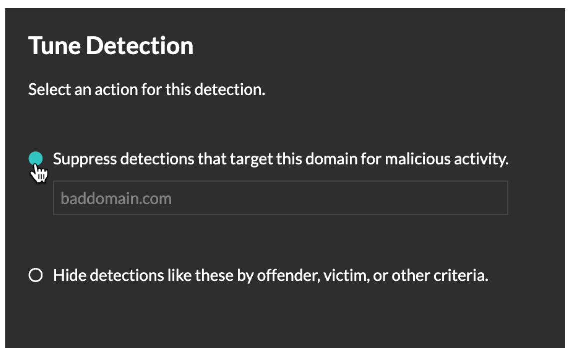
Add a tuning parameter or trusted domain from a detection card

If you encounter a low-value detection, you can add tuning parameters and trusted domains directly from a detection card to keep similar detections from generating.

Before you begin
Users must have full write or higher privileges to tune a detection.

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 the option to suppress the detection by adding a tuning parameter or trusted domain. If the detection does not have an associated tuning parameter, you can hide the detection with a tuning rule.

5. Click the **Suppress detections...** option and click **Save**.

   The Tuning Parameter Added confirmation appears and the new parameter is added to the Tuning Parameters page. For trusted domains, the domain is added under Trusted Domains on the Network Localities page.