Specify tuning parameters for detections

Published: 2022-05-03

By providing information about your network environment, you can help improve the quality and accuracy of rules-based detections, which are authored by ExtraHop. Some rules-based detections rely on tuning parameters and these detections are not generated if the tuning parameters are left empty.

If your ExtraHop deployment includes a Command appliance or Reveal(x) 360, we recommend that you share and manage settings ⤤ from those systems to all connected ExtraHop systems.

> **Note:** Parameter 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.
	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.
Approved Public DNS Servers	Specify public DNS servers allowed in your environment that you want rules-based detections to ignore.

Option	Description
	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.
	Type a single user agent per field.

4. Click **Save**.

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