Specify custom parameters for detections

Published: 2020-02-23

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 custom parameters and these detections are not generated if the custom parameters are left empty.

If your ExtraHop deployment includes a Command appliance, we recommend that you configure these settings on the Command appliance, and then transfer management from connected Discover appliances to the Command appliance.

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

1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click the System Settings icon and then click **Custom 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 like your firewalls or routers.
L2 Devices	By default, L2 devices are ignored by rules-based detections because they can create duplicate entries for L2 and L3 layer data. Select this option to identify detections on new L2 devices that have not yet reached standard analysis.
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 to 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.
Related Records	By default, transactions that directly result in a rules-based detection are committed as records that you can investigate. However, transactions related to the detection that might provide context and deeper insight are not committed.

Option	Description
	Select this option to commit records for transactions related to rules-based detections. Note that this can significantly increase the number of records committed.
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 HTTP Ports	Specify non-standard server ports in your environment that you want rules-based detections to ignore when HTTP traffic is observed on these ports. Type a single HTTP port number per field. If you do not specify a value, detections that rely on this parameter are not generated.
Approved SSH Ports	Specify non-standard server ports in your environment that you want rules-based detections to ignore when SSH traffic is observed on these ports. Type a single SSH port number per field. 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**.