Configure detection alert settings

Published: 2018-10-10

You can configure detection alert settings that monitor when a detection has occurred on specific protocols. When the conditions configured in the alert settings are met, the ExtraHop system generates a detection alert, which you can view in the Alert History.

Note: This topic applies to all ExtraHop systems, including ExtraHop Reveal(x).

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

Detection alerts are useful for monitoring unusual behavior that you want to be notified of right away. For example, if you are worried about spikes in SSH sessions on specific servers, you can configure alert settings to watch for detections that occur over SSH and assign the alert configuration to SSH servers.

1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click the System Settings icon and then click **Alerts**.
3. Click **New** to open the Alert Configuration window.
4. Enter a unique name for the alert configuration in the **Name** field.
5. From the **Alert Type** section, click Detection.
6. Click the **Source Type** list and select the data source for the alert configuration.
   The alert configuration can be assigned only to the type of source selected.
7. Select one of the following detection categories:

Option	Description
Any category	Watches for detections on assigned sources that occur over any detection category.
Specific categories	Watches for detections on assigned sources that occur only within specified detection categories. Click **Select Categories** to specify one or more categories. If you select **Security**, all security detection categories will apply. If you select **IT Operations**, all performance detections will apply.

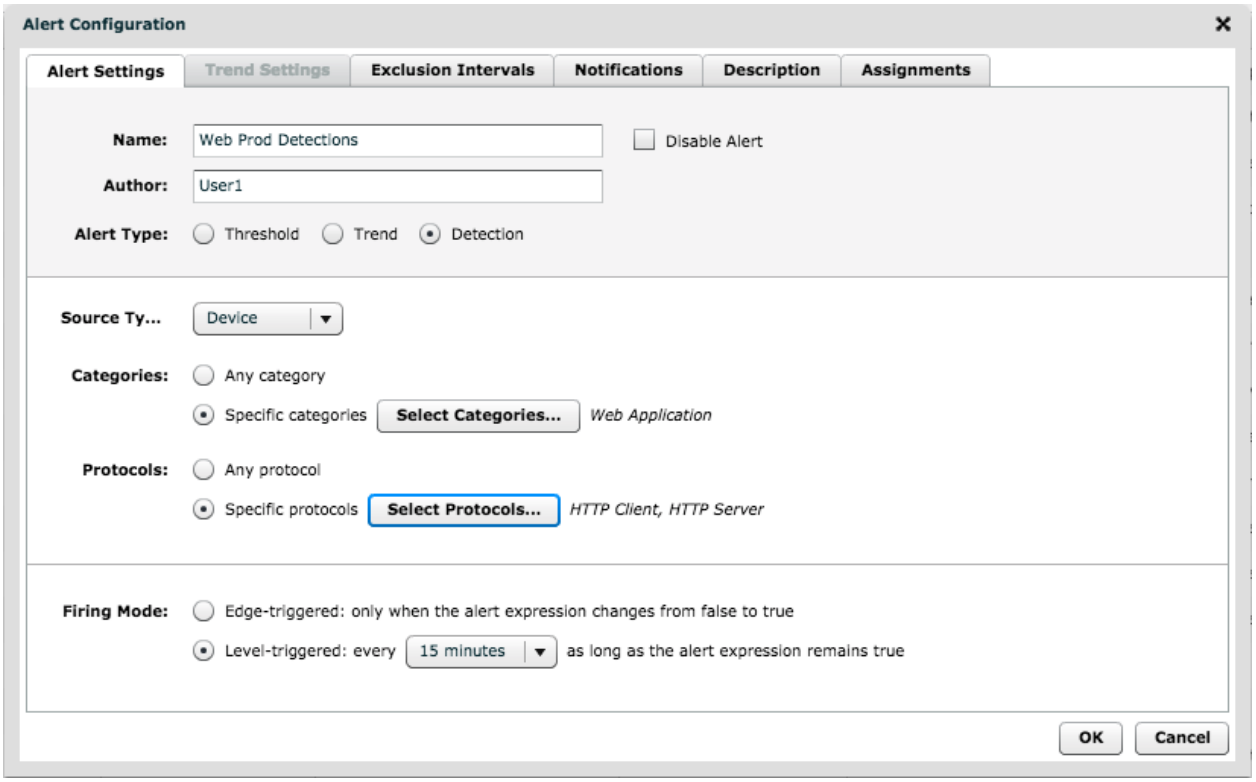
   The detection categories available vary by your ExtraHop subscription. Security detections are only available for ExtraHop Reveal(x). Learn more in Detections.
8. Select one of the following protocols options:

Option	Description
Any protocol	Watches for detections on assigned sources that occur over any protocol.
Specific protocols	Watches for detections on assigned sources that occur only over specified protocols. Click **Select Protocols** to specify one or more categories, such as HTTP Client and HTTP Server.

9. Select one of the following firing modes:

Option	Description
Edge-Triggered	Generates an alert only once when the alert conditions are true. The alert is generated again only if conditions are true after the metric value has returned to normal conditions twice.
Level-Triggered	Generates alerts continuously while the alert conditions are true for the specified time period.

10. Click **OK**.



Next steps

- Alerts cannot be generated until you assign an alert configuration to a source.
- Assign an exclusion interval to an alert to suppress alerts during specific times.
- Add a notification to an alert configuration to receive emails or SNMP traps when an alert is generated.