Configure a detection alert

Published: 2021-09-01

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.

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

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Alerts**.
3. Click **Create**.
4. Type a unique name for the alert configuration in the **Name** field.
5. In the **Description** field, add information about the alert.

   Tip: Alert descriptions support Markdown, which is a simple formatting syntax that converts plain text into HTML. For more information, see the Alerts FAQ.
6. In the **Alert Type** section, click **Detection Alert**.
7. In the **Assigned Sources** field, type the name of a device, device group, or application and then select from the search results.
8. Optional: Click **Add Source** to assign the alert to multiple sources. Multiple sources must be of the same type, such as only devices and device groups or only applications.

   Tip: Assign an alert to a device group to efficiently manage assignments to multiple devices.
9. From the **Detection Categories** drop-down list, select one or more categories that you want the alert to monitor. The following groups of categories are also available:

Option	Description
Any category	Monitors detections on assigned sources that occur in any detection category.
IT Operations	Monitors detections that occur on assigned sources in any IT operations category.
Security	Monitors detections that occur on assigned sources in any Security category.

   Note: Detection categories vary by your ExtraHop system.
10. Optional: From the **Protocols** drop-down list, select each protocol you want the alert to monitor.
11. In the Alert Behavior section, select an option to specify when to generate an alert:
    - Alert once when the alert condition is met
    - Alert every *<time interval>* while the alert condition is met

      You can select a time interval from 5 minutes up to 4 hours.
12. From the Severity drop-down list, select a severity level for the alert:
    - Emergency
    - Alert
    - Critical
    - Error
    - Warning
    - Notice

- Info
- Debug

When an alert is generated, the severity level is displayed on the Alerts page and in alert notifications.

13. Optional: In the Notifications section, add an email notification to an alert to receive emails or SNMP traps when an alert is generated.
14. In the Status section, click an option to enable or disable the alert.
15. Optional: Add an exclusion interval to suppress alerts during specific times.
16. Click **Save**.