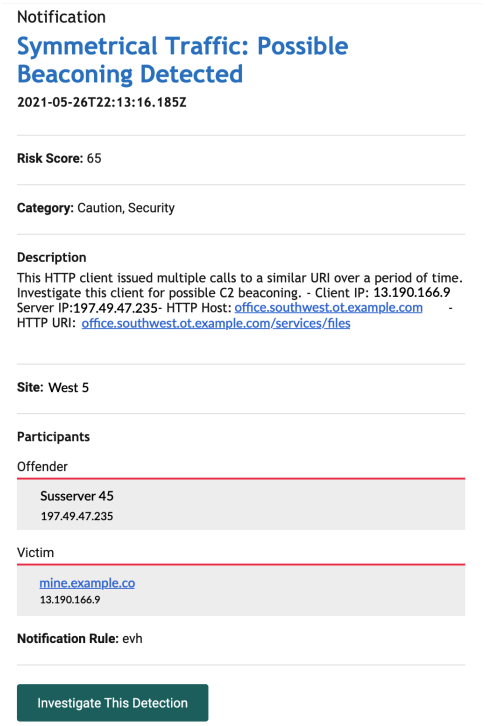
Create a notification rule

Published: 2021-08-31

Detection notification rules enable you to receive a notification when detections that match your specified criteria occur.

A notification email is sent to a recipient list with the same information as the detection card. Click Investigate This Detection to view the detection in the ExtraHop system. Users must be granted access through the Detections Access Control global policy before they can view detections in the ExtraHop system.



Before you begin

- Users must have full-write or higher privileges to create a detection notification.
- Detection notifications are only available from Command appliances and Reveal(x) 360 and require a connection to ExtraHop Cloud Services.
- Email notifications are sent from no-reply@notify.extrahop.com. Make sure to add this address to your list of allowed senders.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Notification Rules**.
3. Click **Create**.
4. Type a unique name for the notification rule in the Name field.
5. In the Description field, add information about the notification rule.
6. In the Criteria section, click **Add Criteria** to specify criteria that will generate a notification.
   The criteria options match the filtering options on the Detections page.
   1. Type
   2. Category

3. Technique
4. Offender
5. Victim
6. Device Role
7. Source
8. Site

7. In the Actions section, type individual email addresses, separated by a comma.
8. Click **Save**.

A notification is sent the first time a detection matches the criteria of a notification rule. A single detection will never generate more than one notification per notification rule.