Create a detection notification rule

Published: 2022-06-09

Create a notification rule if you want to receive a notification about detections that match specific criteria.

When a detection that matches your criteria is generated, a notification is sent with information from the detection card.

You can configure the system to send an email to a recipient list or call a specific webhook.

Before you begin

- Users must be granted access through the Detections Access Control global policy and have full write privileges or higher to complete the tasks in this guide.
- Reveal(x) 360 requires a connection to ExtraHop Cloud Services to send notifications through email and webhooks. Reveal(x) Enterprise requires a connection to ExtraHop Cloud Services to send notifications through email, but can send a notification through a webhook without a connection.
- Reveal(x) 360 cannot send webhook calls to endpoints on your internal network. Webhook targets must be open to external traffic.
- Webhook targets must have a certificate signed by a certificate authority (CA) from the Mozilla CA Certificate Program. See https://wiki.mozilla.org/CA/Included_Certificates for certificates from trusted public CAs.
- Reveal(x) Enterprise must connect directly to webhook endpoints to send notifications.
- 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. In the Name field, type a unique name for the notification rule.
5. In the Description field, add information about the notification rule.
6. In the Event section, select **Detection**.
7. In the Criteria section, click **Add Criteria** to specify criteria that will generate a notification.
   - **Minimum Risk Score**
   - **Type**
   - **Category**
   - **Technique**
   - **Offender**
   - **Victim**
   - **Device Role**
   - **Source**
   - **Site**

   The criteria options match the filtering options on the Detections page.
8. In the Actions section, click **Add Action** to specify how the notification will be sent.
   - Click **Send Email** and specify individual email addresses, separated by a comma.
   - Click **Call Webhook** and specify the following settings:
     1. In the Payload URL field, type the URL of the webhook.
     2. In the Payload (JSON) field, type the JSON payload that will be sent to the payload URL.

        See the Webhook Notification Reference for example payloads.
     3. (Optional) In the Custom Headers section, click **Add Header** to specify custom key:value pairs.

Custom headers are added to the header of the webhook HTTP POST request.

4. Click **Save**.
5. Click **Test Connection**.

   A message titled Test Notification will be sent to the Payload URL to confirm the connection.

   Note: After testing the connection, confirm that you received the notification in the target application. Reveal(x) Enterprise displays an error message if the test notification was not successful.

6. Select an authentication type.

   - **No Authentication**
   - **Basic Authentication**

     Enter the username and password for the target application.
   - **Bearer Token**

     Enter the access token for the target application.

9. In the Options section, select the **Enable notification rule** checkbox to enable the notification.

When a detection matches the criteria, a notification is sent. A single detection will never generate more than one notification per notification rule.

Webhook Notification Reference

This guide provides reference information to help you write the JSON payload for webhook-based notifications. The guide contains an overview of the Payload (JSON) interface, a list of detection variables that are available for webhooks, and examples of JSON structure for common webhook targets, such as Slack, Microsoft Teams, and Google Chat.

For more information about notification rules, see Create a detection notification rule.

Payload JSON

ExtraHop webhooks are formatted in JSON, powered by the Jinja2 templating engine. When you create a notification rule and select the webhook option, the webhook editor opens to the right, and you can edit the payload.

You can modify the default payload with custom properties or copy a JSON template for Slack, Microsoft Teams, or Google Chat, from the Examples section.

By default, the payload contains a sample `text` property. The sample JSON in the figure below sends a notification with the text "ExtraHop Detection" followed by the detection title that replaces the variable.

We recommend that you test your connection to the webhook URL before modifying the payload. That way you can be sure any issues are not due to a connection error.

Syntax validation

The webhook editor provides JSON and Jinja2 syntax validation. If you type a line that includes incorrect JSON or Jinja2 syntax, an error appears under the Payload field with the error.

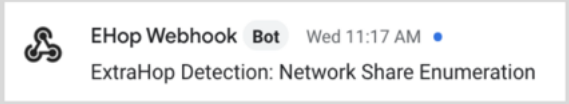
Variables

Detection variables are added to the payload by inserting the variable name between double sets of curly braces ({{ and }}).

For example, the sample in the payload includes a variable for the detection title:

```
"text": "ExtraHop Detection: {{title}}"
```

When a detection matches a notification rule with the variable, the variable is replaced by the detection title. For example, if the notification rule matches the detection for Network Share Enumeration, the variable is replaced with the title in the notification, similar to the following figure:



See a list of detection variables.

Filters

Filters enable you to modify a variable.

Passing JSON

If the variable returns a value that is formatted in JSON, the value is automatically escaped and translated into a string. If you want to pass valid JSON to your webhook target, you must specify the `safe` filter:

```
{{<variable> | safe }}
```

In the following example, the variable returns JSON-formatted detection data about participants directly to the webhook target:

```
{{api.participants | safe }}
```

IF statements

An IF statement can check whether a value is available for the variable. If the variable is empty, you can specify an alternative variable.

```
 {% if {{<variable>}} %}
```

In the following example, the IF statement checks if a value is available for the victim variable:

```
{% if victims %}
```

In the following example, the IF statement checks if an offender name is available. If there is no value for the offender name, the value for the offender IP address variable is returned instead.

```
{% if offender.name %}{{offender.name}}{%else%}{{offender.ipaddr}}
{% endif %}
```

FOR loops

A FOR loop can enable the notification to display an array of objects.

```
{% for <array-object-variable> in <array-variable> %}
```

In the following example, a list of offender names from the offenders array are displayed in the notification. An IF statement checks for more items in the array (`{% if not loop.last %}`) and adds a line break

before printing the next value (\n). If an offender name is empty, the default filter returns "Unknown Name" for the value.

```
{% for offender in offenders %}
  {{offender.name | default ("Unknown Name")}}
  {% if not loop.last %}\n
  {% endif %}
{% endfor %}
```

Available detection variables
The following variables are available for webhook notifications about detections.

title: ***String***
The title of the detection.

detection: ***String***
A description of the detection.

type: ***String***
The type of detection.

id: ***Number***
The unique identifier for the detection.

url: ***String***
The URL for the detection in the ExtraHop system.

risk_score: ***Number***
The risk score of the detection.

site: ***String***
The site where the detection occurred.

start_time_text: ***String***
The time that the detection started.

end_time_text: ***String***
The time that the detection ended.

categories_array: ***Array of Strings***
An array of categories that the detection belongs to.

categories_string: ***String***
A string that lists the categories that the detection belongs to.

mitre_tactics: ***Array of Strings***
An array of MITRE tactic IDs associated with the detection.

mitre_tactics_string: ***String***
A string that lists the MITRE tactic IDs associated with the detection.

mitre_techniques: ***Array of Strings***
An array of MITRE technique IDs associated with the detection.

mitre_techniques_string: ***String***
A string that lists the MITRE technique IDs associated with the detection.

offender_primary: ***Object***
An object that identifies the primary offender and contains the following properties:

external: ***Boolean***
The value is `true` if the primary offender IP address is external to your network.

ipaddr: ***String***
The IP address of the primary offender.

name: ***String***

The name of the primary offender.

offenders: ***Array of Objects***

An array of offender objects associated with the detection. Each object contains the following properties:

external: ***Boolean***

The value is `true` if the offender IP address is external to your network.

ipaddr: ***String***

The IP address of the offender. Applies to detections with multiple offenders.

name: ***String***

The name of the offender. Applies to detections with multiple offenders.

victim_primary: ***Object***

An object that identifies the primary victim and contains the following properties:

external: ***Boolean***

The value is `true` if the primary victim IP address is external to your network.

ipaddr: ***String***

The IP address of the primary victim.

name: ***String***

The name of the primary victim.

victims: ***Array of Objects***

An array of victim objects associated with the detection. Each object contains the following properties:

external: ***Boolean***

The value is `true` if the victim IP address is external to your network.

ipaddr: ***String***

The IP address of the victim. Applies to detections with multiple victims.

name: ***String***

The name of the victim. Applies to detections with multiple victims.

api: ***Object***

An object that contains all fields returned by the `GET /detections/{id}operation`. For more information, see the Introduction to the ExtraHop REST API.

Webhook Examples

The following sections provide JSON templates for common webhook targets.

Slack

After you create a Slack app and enable incoming webhooks for the app, you can create an incoming webhook. When you create an incoming webhook, Slack will generate the URL for you to enter in the Payload URL field in your notification rule.

The following example shows the JSON payload for a Slack webhook:

```
{
    "blocks": [
        {
            "type": "header",
            "text": {
                "type": "plain_text",
                "text": "Detection: {{ title }}"
```

```
            }
        },
        {
            "type": "section",
            "text": {
                "type": "mrkdwn",
                "text": "• *Risk Score:* {{ risk_score }}\n • *Category:*
 {{ categories_string }}\n • *Site:* {{ site }}\n • *Primary Offender:*
 {{ offender_primary.name}} ({{ offender_primary.ipaddr}})\n • *Primary
 Victim:* {{ victim_primary.name }} ({{ victim_primary.ipaddr }})\n"
            }
        },
        {
            "type": "section",
            "text": {
                "type": "plain_text",
                "text": "Detection ID: {{ id }}"
            },
            "text": {
                "type": "mrkdwn",
                "text": "<{{ url }}|View Detection Details>"
            }
        }
    ]
}
```

Microsoft Teams

You can add an incoming webhook to a Teams channel as a connector. After you configure an incoming webhook, Teams will generate the URL for you to enter in the Payload URL field in your notification rule.

The following example shows the JSON payload for a Microsoft teams webhook:

```
{
   "type":"message",
   "attachments":[
      {
         "contentType":"application/vnd.microsoft.card.adaptive",
         "contentUrl":null,
         "content":{
            "$schema":"https://adaptivecards.io/schemas/adaptive-card.json",
            "type":"AdaptiveCard",
            "body":[
               {
                  "type":"ColumnSet",
                  "columns":[
                     {
                        "type": "Column",
                        "width":"16px",
                        "items":[
                           {
                              "type":"Image",
                              "horizontalAlignment":"center",
                              "url":"https://assets.extrahop.com/
favicon.ico",
                              "altText":"ExtraHop Logo"
                           }
                        ]
                     },
                     {
                        "type": "Column",
                        "width":"stretch",
                        "items":[
```

```
                           {
                              "type":"TextBlock",
                              "text":"ExtraHop Reveal(x)",
                              "weight": "bolder"
                           }
                        ]
                     }
                  ]
               },
               {
                  "type":"TextBlock",
                  "text":"**{{ title }}**"
               },
               {
                  "type":"TextBlock",
                  "spacing":"small",
                  "isSubtle":true,
                  "wrap":true,
                  "text":"{{ description }}"
               },
               {
                  "type":"FactSet",
                  "facts":[
                     {
                        "title":"Risk Score:",
                        "value":"{{ risk_score }}"
                     },
                     {
                        "title":"Category:",
                        "value":"{{ categories_string }}"
                     },
                     {
                        "title":"Site:",
                        "value":"{{ site }}"
                     },
                     {
                        "title":"Primary Offender:",
                        "value":"{{ offender_primary.name }}
 ({{ offender_primary.ipaddr }})"
                     },
                     {
                        "title":"Primary Victim:",
                        "value":"{{ victim_primary.name }}
 ({{ victim_primary.ipaddr }})"
                     }
                  ]
               },
               {
                  "type":"ActionSet",
                  "actions":[
                     {
                        "type":"Action.OpenUrl",
                        "title":"View Detection Details",
                        "url":"{{ url }}"
                     }
                  ]
               }
            ]
         }
      }
   ]
}
```

Google Chat

From a Google chat room, you can click the dropdown next to the room name and select Manage webhooks. After you add a webhook and name it, Google Chat will generate the URL for you to enter in the Payload URL field in your notification rule.

The following example shows the JSON payload for a Google Chat webhook:

```
{
    "cards": [
        {
            "header": {
                "title": "{{title}}"
            },
            "sections": [
                {
                    "widgets": [
                        {
                            "keyValue": {
                                "topLabel": "Risk score",
                                "content": "{{risk_score}}"
                            }
                        },
                        {
                            "keyValue": {
                                "topLabel": "Categories",
                                "content": "{{categories_string}}"
                            }
                        }
                        {% if offenders %}
                       ,{
                            "keyValue": {
                                "topLabel": "Offenders",
                                "contentMultiline": "true",
                                "content": "{% for offender in offenders %}
{% if offender.name %}{{offender.name}}{% else %}{{offender.ipaddr}}{% endif
 %}{% if not loop.last %}\n{% endif %}{% endfor %}"
                            }
                        }
                        {% endif %}
                        {% if victims %}
                       ,{
                            "keyValue": {
                                "topLabel": "Victims",
                                "contentMultiline": "true",
                                "content": "{% for victim in victims %}{%
 if victim.name %}{{victim.name}}{% else %}{{victim.ipaddr}}{% endif %}{% if
 not loop.last %}\n{% endif %}{% endfor %}"
                            }
                        }
                        {% endif %}
                    ]
                },
                {
                    "widgets": [
                        {
                            "buttons": [
                                {
                                    "textButton": {
                                        "text": "VIEW DETECTION DETAILS",
                                        "onClick": {
                                            "openLink": {
                                                "url": "{{url}}"
                                            }
```

```
                                        }
                                    }
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```