Création d'une règle de notification de détection

Publié: 2024-01-31

Créez une règle de notification si vous souhaitez recevoir une notification concernant les détections correspondant à des critères spécifiques.

Vidéos Consultez la formation associée : Configurer les notifications de détection

Lorsqu'une détection correspondant à vos critères est générée, une notification est envoyée avec des informations provenant du carte de détection.

Vous pouvez configurer le système pour envoyer un e-mail à une liste de destinataires ou appeler un webhook spécifique.

Avant de commencer

- Les utilisateurs doivent disposer d'un accès au module NDR ou NPM et disposer d'une écriture complète privilèges ou une version supérieure pour effectuer les tâches décrites dans ce guide.
- Reveal (x) 360 nécessite connexion aux services cloud ExtraHop pour envoyer des notifications par e-mail et via des webhooks. Reveal (x) Enterprise nécessite une connexion à ExtraHop Cloud Services pour envoyer des notifications par e-mail, mais peut envoyer une notification via un webhook sans connexion.
- Les notifications par e-mail sont envoyées via les services cloud ExtraHop et peuvent contenir des informations identifiables telles que des adresses IP, des noms d'utilisateur, des noms d'hôtes, des noms de domaine , des noms d'équipements ou des noms de fichiers. Les utilisateurs de Reveal (x) Enterprise dont les exigences réglementaires interdisent les connexions externes peuvent configurer des notifications avec des appels Webhook pour envoyer des notifications sans connexion externe.
- Reveal (x) 360 ne peut pas envoyer d'appels Webhook aux terminaux de votre réseau interne. Les cibles Webhook doivent être ouvertes au trafic externe.
- Les cibles Webhook doivent disposer d'un certificat signé par une autorité de certification (CA) du programme de certificats Mozilla CA. Voir https://wiki.mozilla.org/CA/Included_Certificates pour les certificats émis par des autorités de certification publiques fiables.
- Reveal (x) Enterprise doit se connecter directement aux points de terminaison du webhook pour envoyer des notifications.
- Les notifications par e-mail sont envoyées depuis no-reply@notify.extrahop.com. Assurez-vous d'ajouter cette adresse à votre liste d'expéditeurs autorisés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles de notification**.
3. Cliquez **Créez**.
4. Dans le Nom champ, saisissez un nom unique pour la règle de notification.
5. Dans le Descriptif champ, ajoutez des informations sur la règle de notification.
6. Dans le Type d'événementsection, sélectionnez **Détection de sécurité** ou **Détection des performances**.
7. Dans le Critères section, cliquez sur **Ajouter des critères** pour spécifier les critères qui généreront une notification.
    - **Score de risque minimum**
    - **Tapez**
    - **Catégorie**
    - **Technique**
    - **Délinquant**
    - **Victime**
    - **Rôle de l'appareil**

- **Source**
- **Site**

Les options de critères correspondent à options de filtrage sur la page Détections.

8. Dans la section Actions, cliquez sur **Ajouter une action** pour spécifier la manière dont la notification sera envoyée.
   - Cliquez **Envoyer un e-mail** et spécifiez les adresses e-mail individuelles, en les séparant par une virgule.
   - Cliquez **Appelez Webhook** et définissez les paramètres suivants :
     1. Dans le URL de la charge utile dans ce champ, saisissez l'URL du webhook.
     2. Dans le Charge utile (JSON) dans le champ, saisissez la charge utile JSON qui sera envoyée à l'URL de la charge utile.

        Consultez les Référence de notification Webhook par exemple des charges utiles.
     3. (Facultatif) Dans la section En-têtes personnalisés, cliquez sur **Ajouter un en-tête** pour spécifier des paires clé:valeur personnalisées.

        Des en-têtes personnalisés sont ajoutés à l'en-tête de la requête HTTP POST du webhook.
     4. Cliquez **Enregistrer**.
     5. Cliquez **Connexion de test**.

        Un message intitulé Notification de test sera envoyé à l'URL de la charge utile pour confirmer la connexion.

        Note: Après avoir testé la connexion, confirmez que vous avez reçu la notification dans l'application cible. Reveal (x) Enterprise affiche un message d'erreur si la notification de test n'a pas abouti.
     6. Sélectionnez un type d'authentification.
        - **Aucune authentification**
        - **Authentification de base**

          Entrez le nom d'utilisateur et le mot de passe de l' application cible.
        - **Jeton Bearer**

          Entrez le jeton d'accès pour l'application cible.
9. Dans le Options section, sélectionnez **Activer la règle de notification** case à cocher pour activer la notification.

Lorsqu'une détection correspond aux critères, une notification est envoyée. Une seule détection ne générera jamais plus d'une notification par règle de notification.

Référence de notification Webhook

Ce guide fournit des informations de référence pour vous aider à écrire la charge utile JSON pour les notifications basées sur des webhooks. Le guide contient une présentation de l'interface Payload (JSON), une liste des variables de détection disponibles pour les webhooks et des exemples de structure JSON pour les cibles de webhooks courantes, telles que Slack, Microsoft Teams et Google Chat.

Pour plus d'informations sur les règles de notification, voir Création d'une règle de notification de détection.

Charge utile JSON

Les webhooks ExtraHop sont formatés en JSON, alimentés par Moteur de création de modèles Jinja2. Lorsque vous créez une règle de notification et que vous sélectionnez l'option webhook, l'éditeur de webhook s'ouvre sur la droite et vous pouvez modifier la charge utile.

Vous pouvez modifier la charge utile par défaut à l'aide de propriétés personnalisées ou copier un modèle JSON pour Slack, Microsoft Teams ou Google Chat à partir du Exemples section.

Par défaut, la charge utile contient un échantillon `text` propriété. L'exemple de code JSON présenté dans la figure ci-dessous envoie une notification avec le texte « ExtraHop Detection » suivi du titre de détection qui remplace la variable.

Nous vous recommandons de tester votre connexion à l'URL du webhook avant de modifier la charge utile. Ainsi, vous pouvez être sûr que les problèmes ne sont pas dus à une erreur de connexion.

Validation de syntaxe

L'éditeur de webhook fournit une validation syntaxique JSON et Jinja2. Si vous tapez une ligne dont la syntaxe JSON ou Jinja2 est incorrecte, une erreur s'affiche sous le champ Payload contenant l'erreur.

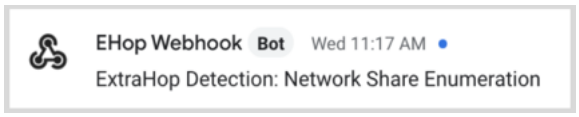
Variables

Les variables de détection sont ajoutées à la charge utile en insérant le nom de la variable entre deux ensembles d'accolades ({{et}}).

Par exemple, l'échantillon de la charge utile inclut une variable pour le titre de détection :

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

Lorsqu'une détection correspond à une règle de notification et à la variable, celle-ci est remplacée par le titre de la détection. Par exemple, si la règle de notification correspond à la détection pour Network Share Enumeration, la variable est remplacée par le titre de la notification, comme dans la figure suivante :



Consultez la liste des variables de détection.

Filtres

Les filtres vous permettent de modifier une variable.

Transmission de JSON

Si la variable renvoie une valeur formatée en JSON, la valeur est automatiquement échappée et traduite en chaîne. Si vous souhaitez transmettre un code JSON valide à votre cible de webhook, vous devez spécifier `safe` filtre :

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

Dans l'exemple suivant, la variable renvoie des données de détection au format JSON concernant les participants directement à la cible du webhook :

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

Déclarations IF
Une instruction IF permet de vérifier si une valeur est disponible pour la variable. Si la variable est vide, vous pouvez spécifier une variable alternative.

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

Dans l'exemple suivant, l'instruction IF vérifie si une valeur est disponible pour la variable victim :

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

Dans l'exemple suivant, l'instruction IF vérifie si le nom du délinquant est disponible. S'il n'y a aucune valeur pour le nom du délinquant, la valeur de la variable d'adresse IP du délinquant est renvoyée à la place.

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

Boucles FOR
Une boucle FOR peut permettre à la notification d'afficher un tableau d'objets.

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

Dans l'exemple suivant, une liste des noms de délinquants du tableau des délinquants est affichée dans la notification. Une instruction IF vérifie la présence d'autres éléments dans le tableau (`{% if not loop.last %}`) et ajoute un saut de ligne avant d'imprimer la valeur suivante (\n). Si le nom du délinquant est vide, le filtre par défaut renvoie « Nom inconnu » pour la valeur.

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

Variables de détection disponibles
Les variables suivantes sont disponibles pour les notifications du webhook concernant les détections.

titre : ***Corde***
Titre de la détection.

détection : ***Corde***
Description de la détection.

type : ***Corde***
Type de détection.

identifiant : ***Numéro***
Identifiant unique pour la détection.

URL : ***Corde***
URL de détection dans le système ExtraHop.

score de risque : ***Numéro***
L'indice de risque associé à la détection.

site : ***Corde***
Le site sur lequel la détection a eu lieu.

time_de_début du texte : ***Corde***
Heure à laquelle la détection a commencé.

texte_heure_fin : ***Corde***
Heure à laquelle la détection a pris fin.

tableau de catégories : ***Tableau de chaînes***

Un ensemble de catégories auxquelles appartient la détection.

catégories_chaîne : ***Corde***

Chaîne répertoriant les catégories auxquelles appartient la détection.

mitre_tactics : ***Tableau de chaînes***

Un ensemble d'identifiants tactiques MITRE associés à la détection.

mitre_tactics_string : ***Corde***

Chaîne répertoriant les identifiants tactiques MITRE associés à la détection.

techniques de mitre : ***Tableau de chaînes***

Un ensemble d'identifiants de techniques MITRE associés à la détection.

mitre_techniques_string : ***Corde***

Chaîne répertoriant les identifiants de technique MITRE associés à la détection.

délinquant principal : ***Objet***

Un objet qui identifie le délinquant principal et qui contient les propriétés suivantes :

externe : ***Booléen***

La valeur est `true` si l' adresse IP du délinquant principal est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP du délinquant principal.

nom : ***Corde***

Le nom du délinquant principal.

contrevenants : ***Tableau d'objets***

Un ensemble d'objets du délinquant associés à la détection. Chaque objet contient les propriétés suivantes :

externe : ***Booléen***

La valeur est `true` si l'adresse IP du délinquant est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP du délinquant. S'applique aux détections impliquant plusieurs délinquants.

nom : ***Corde***

Le nom du délinquant. S'applique aux détections impliquant plusieurs délinquants.

victime_principale : ***Objet***

Un objet qui identifie la victime principale et contient les propriétés suivantes :

externe : ***Booléen***

La valeur est `true` si l' adresse IP principale de la victime est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP de la victime principale.

nom : ***Corde***

Le nom de la victime principale.

victimes : ***Tableau d'objets***

Un ensemble d'objets victimes associés à la détection. Chaque objet contient les propriétés suivantes :

externe : ***Booléen***

La valeur est `true` si l'adresse IP de la victime est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP de la victime. S'applique aux détections impliquant plusieurs victimes.

nom : ***Corde***

Le nom de la victime. S'applique aux détections impliquant plusieurs victimes.

API : ***Objet***

Un objet qui contient tous les champs renvoyés par `GET /detections/{id}operation`. Pour plus d'informations, consultez le Présentation de l'API REST ExtraHop.

Exemples de webhooks

Les sections suivantes fournissent des modèles JSON pour les cibles de webhook courantes.

Slack

Après avoir créé une application Slack et activé les webhooks entrants pour l'application, vous pouvez créer un webhook entrant. Lorsque vous créez un webhook entrant, Slack génère l' URL que vous devez saisir dans le champ URL de charge utile de votre règle de notification.

L'exemple suivant montre la charge utile JSON d'un webhook Slack :

```
{
    "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

Vous pouvez ajouter un webhook entrant à un canal Teams en tant que connecteur. Après avoir configuré un webhook entrant, Teams génère l'URL que vous devez saisir dans le champ URL de charge utile de votre règle de notification.

L'exemple suivant montre la charge utile JSON d'un webhook Microsoft Teams :

```
{
   "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

Dans un salon de discussion Google, vous pouvez cliquer sur le menu déroulant à côté du nom du salon et sélectionner Gérer les webhooks. Après avoir ajouté un webhook et lui avoir donné un nom, Google Chat génère l'URL que vous devez saisir dans le champ URL de charge utile de votre règle de notification .

L'exemple suivant montre la charge utile JSON d'un webhook Google Chat :

```
{
    "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}}"
                                            }
                                        }
                                    }
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```