Création d'une règle de notification de détection

Publié: 2024-10-26

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. Les utilisateurs de RevealX 360 peuvent créer une règle de notification qui appelle un webhook pour exporter les données de détection vers un intégration configurée.

Note: (RevealX 360 uniquement) Si vous créez une règle de notification pour exporter les données de détection vers une intégration SIEM , créez la notification directement depuis Intégrations page dans les paramètres d'administration pour pré-remplir les champs des règles de notification.

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.
- RevealX Enterprise nécessite un connexion aux services cloud ExtraHop pour envoyer des notifications par e-mail, mais vous pouvez 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 RevealX Enterprise qui ont des exigences réglementaires interdisant les connexions externes peuvent configurer des notifications avec des appels Webhook pour envoyer des notifications sans connexion externe.
- 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. Cliquez sur l'une des options suivantes :
   - Pour les modules NDR, sélectionnez Security Detection.
   - Pour les modules NPM, sélectionnez Performance Detection.
5. Dans le Nom champ, saisissez un nom unique pour la règle de notification.
6. Dans le Descriptif champ, ajoutez des informations sur la règle de notification.
7. Dans le Critères section, cliquez sur **Ajouter des critères** pour spécifier les critères qui généreront une notification.
   - **Recommandé pour le triage**
   - **Score de risque minimum**
   - **Tapez**
   - **Catégorie**
   - **Technique MITRE** (NDR uniquement)
   - **Délinquant**
   - **Victime**

- **Rôle de l'appareil**
- **Participant**
- **Site**

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

8. Dans la section Cible, sélectionnez le mode d'envoi de la notification parmi les options suivantes :

Option	Description
Envoyer un e-mail	Envoyez des notifications par e-mail à une liste de distribution.
Webhook personnalisé	Envoyez une charge utile JSON à l'URL d'un webhook.
Intégration	Exportez les données de détection vers une intégration configurée. Pour les intégrations, nous recommandons aux administrateurs d'ExtraHop de créer des règles de notification de détection à partir du Intégrations page.

9. Si vous avez sélectionné Envoyer un e-mail comme cible, procédez comme suit :
   a) Spécifiez les adresses e-mail individuelles, en les séparant par une virgule.
   b) Cliquez **Enregistrer**.
10. Si vous avez sélectionné Custom Webhook comme cible, procédez comme suit :
    a) Dans le champ URL de la charge utile, saisissez l'URL du webhook.
    b) Cliquez **Afficher les options de connexion avancées** pour configurer les éléments suivants :
       - 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.
       - 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.
    c) Dans Comportement des notifications, sélectionnez le moment où le système ExtraHop enverra des notifications pour une détection.
       - **Envoyer pour chaque mise à jour de détection**

         Recevez une notification chaque fois que la détection est mise à jour.

         Cette sélection est recommandée si vous exportez des données de détection vers un SIEM et que vous souhaitez une visibilité complète de l'activité de détection.
       - **Envoyer une fois par détection**

         Recevez une seule notification lorsqu'une détection est créée.

         Cette sélection est optimale pour avertir un groupe lorsqu'une détection se produit sans surcharger le groupe de mises à jour ultérieures.
    d) Dans Options de charge utile, sélectionnez si vous souhaitez envoyer le charge utile par défaut ou saisissez une charge utile JSON personnalisée.
       - **Charge utile par défaut**

Remplissez la charge utile du webhook avec un ensemble de champs de détection de base.

Dans la liste déroulante Ajouter des champs de charge utile, vous pouvez cliquer sur les champs supplémentaires que vous souhaitez inclure dans la charge utile.

- **Charge utile personnalisée**

  Tapez votre propre charge utile directement dans la fenêtre Aperçu de la charge utile (JSON).

  Conseil: Pour personnaliser une charge utile par défaut, copiez-la depuis la fenêtre d'aperçu, puis passez à **Charge utile personnalisée**, puis collez la charge utile dans la fenêtre d'aperçu pour la modifier.

  Vous pouvez également copier-coller des exemples de charges utiles à partir du Référence de notification du Webhook.

e) Cliquez **Enregistrer**.

f) 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. RevealX Enterprise affiche un message d'erreur si la notification de test n'a pas abouti.

11. Dans le Options section, la **Activer la règle de notification** La case à cocher est activée par défaut. Décochez la case pour désactiver la règle de notification.

Lorsqu'une détection correspond aux critères, une notification est envoyée.

Référence de notification du Webhook

Ce guide fournit des informations sur la rédaction de charges utiles personnalisées pour les notifications de sécurité ou de détection des performances avec des webhooks personnalisés ou des cibles d'intégration. Le guide contient une présentation de l'interface Payload (JSON), la charge utile par défaut pour les cibles de webhook, une liste de champs de charge utile que vous pouvez ajouter à la charge utile par défaut et des exemples de structure JSON pour les cibles de webhook courantes, telles que Slack, Microsoft Teams et Google Chat.

Voici quelques points à prendre en compte à propos des notifications de webhook :

- RevealX 360 ne peut pas envoyer d'appels Webhook aux terminaux de votre réseau interne. Les cibles Webhook doivent être ouvertes au trafic externe.
- RevealX Enterprise doit se connecter directement aux points de terminaison du webhook pour envoyer des notifications.
- 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.

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 de sécurité ou de détection des performances et que vous sélectionnez un webhook ou une intégration personnalisé comme cible, vous avez la possibilité de sélectionner une charge utile par défaut ou d'écrire votre propre charge utile personnalisée .

Charge utile par défaut
Le JSON de charge utile par défaut pour un webhook contient l'ensemble d'informations de base suivant concernant une détection.

```
{
   "title": {{title}},
   "type": {{type}},
   "src": {
       "type": {{src.type}},
       "hostname": "{{src.hostname}}",
       "ipaddr": {{src.ipaddr}},
       "role": {{src.role}},
       "endpoint": {{src.endpoint}}, // sender|receiver|client|server
       "device": {
           "oid": {{src.device.oid}},
           "name": {{src.device.name}},
           "ipaddrs": {{src.device.ipaddrs}},
           "macaddr": {{src.device.macaddr}}
       },
   },
   "dst": {
       "type": {{dst.type}},
       "hostname": {{dst.hostname}},
       "ipaddr": {{dst.ipaddr}},
       "role": {{dst.role}},
       "endpoint": {{dst.endpoint}},
       "device": {
           "oid": {{dst.device.oid}},
           "name": {{dst.device.name}},
           "ipaddrs": {{dst.device.ipaddrs}},
           "macaddr": {{dst.device.macaddr}}
       },
   },
   "properties": {{properties}},
   "description": {{description}},
"categories_ids": {{categories_ids}},
   "mitre_techniques": {{mitre_techniques}}, // array of objects
   "recommended": {{recommended}},
 "recommended_factors: {{recommended_factors}},
   "url": {{url}},
   "risk_score": {{risk_score}},
   "time": {{time}},
  "id": {{detection_id or id}}
  }
```

Vous pouvez modifier la charge utile par défaut en sélectionnant des champs dans la liste déroulante Ajouter des champs de charge utile. Pour apporter des modifications personnalisées, vous pouvez copier la charge utile par défaut, modifier votre option de charge utile en Charge utile personnalisée, puis coller la charge utile par défaut dans le champ de charge utile pour apporter vos modifications.

Charge utile personnalisée
Sélectionnez l'option de charge utile personnalisée pour écrire votre propre JSON pour un webhook de règles de notification. Le champ Charge utile (JSON) affiche un ensemble vide de crochets dans lesquels vous pouvez ajouter le JSON à votre charge utile personnalisée.

Conseil Avant de prendre le temps de saisir une longue charge utile personnalisée, nous vous recommandons de tester votre connexion à l'URL du webhook. De cette façon, vous pouvez être sûr que les problèmes ne sont pas dus à une erreur de connexion.

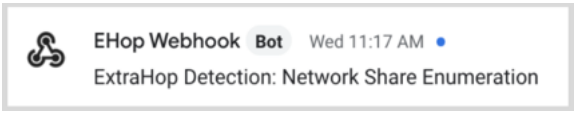
Tapez une simple ligne de JSON pour tester la connexion. Par exemple, la figure ci-dessous montre une variable de texte de base que vous pouvez copier pour tester votre connexion.

Validation de syntaxe
L'éditeur de webhook permet de valider les syntaxes JSON et Jinja2. Si vous tapez une ligne qui inclut une syntaxe JSON ou Jinja2 incorrecte, une erreur apparaît dans le champ Charge utile avec 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 des webhooks concernant les détections.

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

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

type : ***Corde***
Type de détection.

identifiant : ***Numéro***
L'identifiant unique pour la détection.

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

point_de risque : ***Numéro***
L'indice de risque de la détection.

site : ***Corde***
Le site où la détection a eu lieu.

texte_date_début : ***Corde***
Heure à laquelle la détection a commencé.

texte_de_fin : ***Corde***
Heure à laquelle la détection s'est terminée.

tableau_catégories : ***Tableau de cordes***
Tableau de catégories auxquelles appartient la détection.

chaîne_catégories : ***Corde***
Chaîne répertoriant les catégories auxquelles appartient la détection.

mitre_tactics : ***Tableau de cordes***
Tableau d'identifiants tactiques MITRE associés à la détection.

mitre_tactics_string : ***Corde***
Chaîne répertoriant les ID de tactiques MITRE associés à la détection.

mitre_techniques : *Tableau de cordes*

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

mitre_techniques_string : *Corde*

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

délinquant principal : *Objet*

(Obsolète) 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.

délinquants : *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 contrevenant 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*

(Obsolète) Objet qui identifie la victime principale et contient les propriétés suivantes :

externe : *Booléen*

La valeur est `true` si l' adresse IP de la victime principale 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 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 la 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 une chaîne Teams en tant que connecteur. Après avoir configuré un webhook entrant, Teams génère l'URL que vous pouvez saisir dans le champ URL de la charge utile de votre règle de notification.

L'exemple suivant montre la charge utile JSON pour 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 RevealX",
                              "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

Depuis un salon de discussion Google, vous pouvez cliquer sur la liste déroulante à côté du nom du salon et sélectionner Gérer les webhooks. Une fois que vous avez ajouté un webhook et que vous l'avez nommé, Google Chat génère l'URL que vous pouvez saisir dans le champ URL de la 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}}"
                                                }
                                            }
                                        }
                                    }
                                ]
                            }
                        ]
                    }
                ]
            }
        ]
}
```