Eine Regel für Erkennungsbenachrichtigungen erstellen

Veröffentlicht: 2025-02-04

Erstellen Sie eine Benachrichtigungsregel, wenn Sie eine Benachrichtigung über Entdeckungen erhalten möchten , die bestimmten Kriterien entsprechen.

Video: Sehen Sie sich die entsprechende Schulung an: Erkennungsbenachrichtigungen konfigurieren

Wenn eine Erkennung generiert wird, die Ihren Kriterien entspricht, wird eine Benachrichtigung mit Informationen von Erkennungskarte.

Sie können das System so konfigurieren, dass es eine E-Mail an eine Empfängerliste sendet oder einen bestimmten Webhook aufruft. RevealX 360-Benutzer können eine Benachrichtigungsregel erstellen, die einen Webhook aufruft, um Erkennungsdaten an einen zu exportieren konfigurierte Integration.

Hinweis: (Nur RevealX 360) Wenn Sie eine Benachrichtigungsregel erstellen, um Erkennungsdaten in eine SIEM-Integration zu exportieren, erstellen Sie die Benachrichtigung direkt aus dem Integrationen Seite in den Verwaltungseinstellungen , um Felder für Benachrichtigungsregeln vorab auszufüllen.

Bevor Sie beginnen

- Benutzern muss der Zugriff auf das NDR- oder NPM-Modul gewährt werden und sie müssen über vollständige Schreibberechtigungen verfügen. Privilegien oder höher, um die Aufgaben in diesem Handbuch abzuschließen.
- RevealX 360 benötigt eine Verbindung zu ExtraHop Cloud Services um Benachrichtigungen per E-Mail und Webhooks zu senden. RevealX Enterprise benötigt eine Verbindung zu ExtraHop Cloud Services, um Benachrichtigungen per E-Mail zu senden, kann aber auch ohne Verbindung eine Benachrichtigung über einen Webhook senden.
- Webhooks werden über TCP 443 (HTTPS) gesendet.
- E-Mail-Benachrichtigungen werden über ExtraHop Cloud Services gesendet und können identifizierbare Informationen wie IP-Adressen, Benutzernamen, Hostnamen, Domainnamen, Gerätenamen oder Dateinamen enthalten. RevealX Enterprise-Benutzer, deren behördliche Anforderungen externe Verbindungen verbieten, können Benachrichtigungen mit Webhook-Aufrufen so konfigurieren, dass Benachrichtigungen ohne externe Verbindung gesendet werden.
- E-Mail-Benachrichtigungen werden von no-reply@notify.extrahop.com gesendet. Stellen Sie sicher, dass Sie diese Adresse zu Ihrer Liste der zulässigen Absender hinzufügen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Regeln für Benachrichtigungen**.
3. Klicken Sie **Erstellen**.
4. Klicken Sie auf eine der folgenden Optionen:
   - Wählen Sie für NDR-Module **Sicherheitserkennung**.
   - Wählen Sie für NPM-Module **Leistungserkennung**.
5. In der Name Feld, geben Sie einen eindeutigen Namen für die Benachrichtigungsregel ein.
6. In der Beschreibung Feld, fügen Sie Informationen zur Benachrichtigungsregel hinzu.
7. In der Kriterien Abschnitt, klicken **Kriterien hinzufügen** um Kriterien anzugeben, die eine Benachrichtigung generieren.
   - **Für Triage empfohlen**
   - **Mindestrisikobewertung**

- **Typ**
- **Kategorie**
- **MITRE-Technik** (nur NDR)
- **Täter**
- **Opfer**
- **Rolle des Geräts**
- **Teilnehmer**
- **Standort**

Die Kriterienoptionen entsprechen den Filteroptionen auf der Seite „Erkennungen“.

8. In der Ziel Wählen Sie im Abschnitt aus den folgenden Optionen aus, wie die Benachrichtigung gesendet werden soll:

Option	Description
E-Mail senden	Senden Sie E-Mail-Benachrichtigungen an eine Verteilerliste.
Benutzerdefinierter Webhook	Senden Sie eine JSON-Nutzlast an eine Webhook-URL.
Integration	Exportieren Sie Erkennungsdaten in eine konfigurierte Integration. Für Integrationen empfehlen wir, dass ExtraHop-Administratoren Regeln für Erkennungsbenachrichtigungen aus dem Integrationen Seite.

9. Wenn Sie E-Mail senden als Ziel ausgewählt haben, führen Sie die folgenden Schritte aus:
   a) Geben Sie einzelne E-Mail-Adressen an, getrennt durch ein Komma.
   b) Klicken Sie **Speichern**.
10. Wenn Sie Benutzerdefinierter Webhook als Ziel ausgewählt haben, führen Sie die folgenden Schritte aus:
    a) In der Nutzlast-URL Feld, geben Sie die URL des Webhooks ein.
    b) Klicken Sie **Erweiterte Verbindungsoptionen anzeigen** um Folgendes zu konfigurieren:
       - In der Benutzerdefinierte Header Abschnitt, klicken Sie **Header hinzufügen** um benutzerdefinierte Schlüssel:Wert-Paare anzugeben.

         Benutzerdefinierte Header werden dem Header der Webhook-HTTP-POST-Anforderung hinzugefügt.
       - Wählen Sie einen Authentifizierungstyp aus.
         - Keine Authentifizierung
         - Standardauthentifizierung

           Geben Sie den Benutzernamen und das Passwort für die Zielanwendung ein.
         - Inhaber-Token

           Geben Sie das Zugriffstoken für die Zielanwendung ein.
       - Konfigurieren Sie die Verbindungsmethode.
         - Direkte Verbindung
           - Wählen Sie diese Option, um den Webhook über einen konfigurierten globalen Proxy zu leiten. (Nur RevealX Enterprise.)
           - Wählen Sie, um die Serverzertifikatsüberprüfung zu überspringen.
         - Proxy über einen angeschlossenen Sensor
           - Wählen Sie den Proxysensor aus.

- Wählen Sie, um die Serverzertifikatsüberprüfung zu überspringen.
- Wählen Sie diese Option, um den Webhook über einen Globy-Proxy zu leiten, der für den ausgewählten Sensor konfiguriert ist.

c) Unter Verhalten bei Benachrichtigungen, wählen Sie aus, wann das ExtraHop-System Benachrichtigungen bei einer Erkennung sendet.

- **Für jedes Erkennungsupdate senden**

  Erhalten Sie jedes Mal eine Benachrichtigung, wenn die Erkennung aktualisiert wird.

  Diese Auswahl wird empfohlen, wenn Sie Erkennungsdaten in ein SIEM exportieren und einen umfassenden Überblick über die Erkennungsaktivitäten wünschen.
- **Einmal pro Erkennung senden**

  Erhalten Sie eine einzige Benachrichtigung, wenn eine Erkennung erstellt wird.

  Diese Auswahl ist optimal, um eine Gruppe zu benachrichtigen, wenn eine Erkennung auftritt, ohne die Gruppe mit nachfolgenden Aktualisierungen zu überfordern.

d) Unter Payload-Optionen, wählen Sie aus, ob Sie die senden möchten Standard-Nutzlast oder geben Sie eine benutzerdefinierte JSON-Nutzlast ein.

Wenn Sie unter Benachrichtigungsverhalten ausgewählt haben, dass Benachrichtigungen einmal pro Erkennung gesendet werden sollen, müssen Sie eine benutzerdefinierte Nutzlast senden.

- **Standard-Nutzlast**

  Füllen Sie die Webhook-Nutzlast mit einem Kernsatz von Erkennungsfeldern.

  Im Dropdownmenü Payload-Felder hinzufügen können Sie auf zusätzliche Felder klicken, die Sie in die Payload aufnehmen möchten.
- **Benutzerdefinierte Nutzlast**

  Füllen Sie die Webhook-Nutzlast mit benutzerdefiniertem JSON auf.

  Sie können die vorgeschlagene benutzerdefinierte Nutzlast in der **Nutzlast bearbeiten** Fenster.

e) Klicken Sie **Speichern**.

f) Klicken Sie **Verbindung testen**.

Eine Nachricht mit dem Titel Testbenachrichtigung wird an die Payload-URL gesendet, um die Verbindung zu bestätigen.

Hinweis Bestätigen Sie nach dem Testen der Verbindung, dass Sie die Benachrichtigung in der Zielanwendung erhalten haben. RevealX Enterprise zeigt eine Fehlermeldung an, wenn die Testbenachrichtigung nicht erfolgreich war.

11. In der Optionen Abschnitt, der **Benachrichtigungsregel aktivieren** Das Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Benachrichtigungsregel zu deaktivieren.

Wenn eine Erkennung den Kriterien entspricht, wird eine Benachrichtigung gesendet.

Referenz zur Webhook-Benachrichtigung

Dieses Handbuch enthält Informationen zum Schreiben benutzerdefinierter Payloads für Sicherheits- oder Leistungserkennungsbenachrichtigungen mit benutzerdefinierten Webhook- oder Integrationszielen. Das Handbuch enthält einen Überblick über die Payload (JSON) -Schnittstelle, die Standardnutzlast für Webhook-Ziele, eine Liste von Payload-Feldern, die Sie der Standard-Payload hinzufügen können, und Beispiele für die JSON-Struktur für gängige Webhook-Ziele wie Slack, Microsoft Teams und Google Chat.

Hier sind einige Überlegungen zu Webhook-Benachrichtigungen:

- RevealX 360 kann keine Webhook-Aufrufe an Endpunkte in Ihrem internen Netzwerk senden. Webhook-Ziele müssen für externen Verkehr geöffnet sein.
- RevealX Enterprise muss eine direkte Verbindung zu Webhook-Endpunkten herstellen, um Benachrichtigungen zu senden.
- Webhook-Ziele müssen über ein Zertifikat verfügen, das von einer Zertifizierungsstelle (CA) des Mozilla CA Certificate Program signiert wurde. siehe https://wiki.mozilla.org/CA/Included_Certificates für Zertifikate von vertrauenswürdigen öffentlichen CAs.

Weitere Informationen zu Benachrichtigungsregeln finden Sie unter Eine Regel für Erkennungsbenachrichtigungen erstellen.

Nutzlast JSON

ExtraHop-Webhooks sind in JSON formatiert und werden unterstützt von Jinja2-Template-Engine. Wenn Sie eine Regel für Benachrichtigungen zur Sicherheits- oder Leistungserkennung erstellen und einen benutzerdefinierten Webhook oder eine benutzerdefinierte Integration als Ziel auswählen, haben Sie die Möglichkeit, eine Standardnutzlast auszuwählen oder Ihre eigene benutzerdefinierte Nutzlast zu schreiben.

Standard-Nutzlast
Die Standard-Payload-Option ist verfügbar, wenn Sie als Benachrichtigungsverhalten für den Webhook auswählen, dass für jedes Erkennungsupdate eine Benachrichtigung gesendet wird. Die Standardnutzlast enthält den folgenden Basissatz an Informationen zu einer Erkennung.

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "src": {
        "type": "{{ src.type }}",
        "hostname": "{{ src.hostname }}",
        "ipaddr": "{{ src.ipaddr }}",
        "role": "{{ src.role }}",
        "endpoint": "{{ src.endpoint }}",
        "username": "{{ src.username }}",
        "device": {
            "oid": {{ src.device.oid }},
            "name": "{{ src.device.name }}",
            "ipaddrs": {{ src.device.ipaddrs | safe }},
            "macaddr": "{{ src.device.macaddr }}"
        }
    },
    "dst": {
        "type": "{{ dst.type }}",
        "hostname": "{{ dst.hostname }}",
        "ipaddr": "{{ dst.ipaddr }}",
        "role": "{{ dst.role }}",
        "endpoint": "{{ dst.endpoint }}",
        "username": "{{ dst.username }}",
        "device": {
            "oid": {{ dst.device.oid }},
            "name": "{{ dst.device.name }}",
            "ipaddrs": {{ dst.device.ipaddrs | safe }},
            "macaddr": "{{ dst.device.macaddr }}"
        }
    },
    "additional_participants": {{ additional_participants | safe }},
    "properties": {{ properties }},
    "description": "{{ description }}",
    "categories_ids": {{ categories_ids | safe }},
    "mitre_techniques": {{ mitre_techniques | safe }},
    "recommended": "{{ recommended }}",
    "recommended_factors": {{ recommended_factors | safe }},
```

```
    "url": "{{ url }}",
    "risk_score": {{ risk_score }},
    "time": {{ time }},
    "id": {{ detection_id or id }}
}
```

Sie können die Standard-Payload ändern, indem Sie Felder aus dem Dropdownmenü Payload-Felder hinzufügen auswählen. Um benutzerdefinierte Änderungen vorzunehmen, können Sie Ihre Payload-Option in ändern **Benutzerdefinierte Nutzlast**, bearbeiten Sie dann die vorgeschlagene Nutzlast in der **Nutzlast bearbeiten** Fenster.

Benutzerdefinierte Nutzlast
Wählen Sie die benutzerdefinierte Payload-Option, um das vorgeschlagene JSON für einen Benachrichtigungsregel-Webhook zu bearbeiten.

Wenn Sie auswählen, dass für jedes Erkennungsupdate eine Benachrichtigung gesendet werden soll unter Verhalten bei Benachrichtigungen, die vorgeschlagene benutzerdefinierte Nutzlast enthält den folgenden JSON-Code:

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "src": {
        "type": "{{ src.type }}",
        "hostname": {{ src.hostname | safe }},
        "ipaddr": "{{ src.ipaddr }}",
        "role": "{{ src.role }}",
        "endpoint": "{{ src.endpoint }}",
        "username": "{{ src.username }}",
        "device": {
            "oid": {{ src.device.oid }},
            "name": {{ src.device.name | safe }},
            "ipaddrs": {{ src.device.ipaddrs | safe }},
            "macaddr": {{ src.device.macaddr | safe }}
        }
    },
    "dst": {
        "type": "{{ dst.type }}",
        "hostname": {{ dst.hostname | safe }},
        "ipaddr": "{{ dst.ipaddr }}",
        "role": "{{ dst.role }}",
        "endpoint": "{{ dst.endpoint }}",
        "username": "{{ dst.username }}",
        "device": {
            "oid": {{ dst.device.oid }},
            "name": {{ dst.device.name | safe }},
            "ipaddrs": {{ dst.device.ipaddrs | safe }},
            "macaddr": {{ dst.device.macaddr | safe }}
        }
    },
    "additional_participants": {{ additional_participants | safe }},
    "properties": {{ properties }},
    "description": "{{ description }}",
    "categories_ids": {{ categories_ids | safe }},
    "mitre_techniques": {{ mitre_techniques | safe }},
    "recommended": "{{ recommended }}",
    "recommended_factors": {{ recommended_factors | safe }},
    "url": "{{ url }}",
    "risk_score": {{ risk_score }},
    "time": {{ time }},
    "id": {{ detection_id or id }}
}
```

Wenn Sie auswählen, dass pro Erkennungsupdate eine Benachrichtigung gesendet werden soll unter Verhalten bei Benachrichtigungen, die vorgeschlagene benutzerdefinierte Nutzlast enthält den folgenden JSON-Code:

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "url": "{{ url }}",
    "description": "{{ description }}",
    "api": {{ api | safe }},
    "categories_string": "{{ categories_string }}",
    "categories_array": {{ categories_array | safe }},
    "victims": {{ victims | safe }},
    "offenders": {{ offenders | safe }},
    "description_format": "{{ description_format }}",
    "victim_primary": {{ victim_primary | safe }},
    "offender_primary": {{ offender_primary | safe }}
}
```

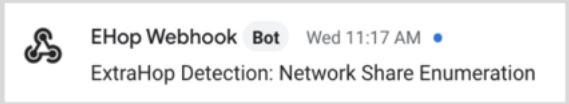
Hinweis: Bevor Sie sich die Zeit nehmen, eine lange benutzerdefinierte Nutzlast einzugeben, empfehlen wir Ihnen, Ihre Verbindung zur Webhook-URL zu testen. Auf diese Weise können Sie sicher sein, dass Probleme nicht auf einen Verbindungsfehler zurückzuführen sind.

Syntaxvalidierung
Der Webhook-Editor bietet JSON- und Jinja2-Syntaxvalidierung. Wenn Sie eine Zeile eingeben , die eine falsche JSON- oder Jinja2-Syntax enthält, wird unter dem Payload-Feld ein Fehler mit dem Fehler angezeigt.
Variablen
Erkennungsvariablen werden der Nutzlast hinzugefügt, indem der Variablenname zwischen doppelten Gruppen geschweifter Klammern ({{und}}) eingefügt wird.

Das Beispiel in der Payload enthält beispielsweise eine Variable für den Erkennungstitel:

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

Wenn eine Erkennung einer Benachrichtigungsregel mit der Variablen entspricht, wird die Variable durch den Erkennungstitel ersetzt. Wenn die Benachrichtigungsregel beispielsweise mit der Erkennung für Network Share Enumeration übereinstimmt, wird die Variable durch den Titel in der Benachrichtigung ersetzt, ähnlich der folgenden Abbildung:



Sehen Sie eine Liste von Erkennungsvariablen.

Filter
Filter ermöglichen es Ihnen, eine Variable zu ändern.

JSON übergeben

Wenn die Variable einen Wert zurückgibt, der in JSON formatiert ist, wird der Wert automatisch maskiert und in eine Zeichenfolge übersetzt. Wenn Sie gültiges JSON an Ihr Webhook-Ziel übergeben möchten, müssen Sie Folgendes angeben: `safe` filtern:

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

Im folgenden Beispiel gibt die Variable Erkennungsdaten über Teilnehmer im JSON-Format direkt an das Webhook-Ziel zurück:

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

IF-Kontoauszüge
Eine IF-Anweisung kann überprüfen, ob ein Wert für die Variable verfügbar ist. Wenn die Variable leer ist, können Sie eine alternative Variable angeben.

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

Im folgenden Beispiel prüft die IF-Anweisung, ob ein Wert für die Opfervariable verfügbar ist:

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

Im folgenden Beispiel prüft die IF-Anweisung, ob ein Täternname verfügbar ist. Wenn es keinen Wert für den Namen des Täters gibt, wird stattdessen der Wert für die Variable IP-Adresse des Täters zurückgegeben.

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

FÜR Schleifen
Eine FOR-Schleife kann es der Benachrichtigung ermöglichen, ein Array von Objekten anzuzeigen.

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

Im folgenden Beispiel wird eine Liste mit Täternamen aus dem Täter-Array in der Benachrichtigung angezeigt. Eine IF-Anweisung sucht nach weiteren Elementen im Array (`{% if not loop.last %}`) und fügt einen Zeilenumbruch hinzu, bevor der nächste Wert gedruckt wird (`\n`). Wenn ein Tätername leer ist, gibt der Standardfilter „Unbekannter Name“ für den Wert zurück.

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

Verfügbare Erkennungsvariablen
Die folgenden Variablen sind für Webhook-Benachrichtigungen über Erkennungen verfügbar.

titel: ***Schnur***

Der Titel der Erkennung.

Beschreibung: ***Schnur***

Eine Beschreibung der Erkennung.

typ: ***Schnur***

Die Art der Erkennung.

ID: ***Zahl***

Die eindeutige Kennung für die Erkennung.

url: ***Schnur***

Die URL für die Erkennung im ExtraHop-System.

Risikobewertung: ***Zahl***

Die Risikoscore der Erkennung.

Standort: ***Schnur***

Der Standort, an dem die Erkennung stattgefunden hat.

Startzeit_Text: ***Schnur***

Die Uhrzeit, zu der die Erkennung gestartet wurde.

Endzeittext: ***Schnur***

Der Zeitpunkt, zu dem die Erkennung endete.

kategorien_array: ***Reihe von Zeichenketten***

Eine Reihe von Kategorien, zu denen die Erkennung gehört.

kategorien_string: ***Schnur***

Eine Zeichenfolge, die die Kategorien auflistet, zu denen die Erkennung gehört.

Eigenschaften: ***Schnur***

Eine Zeichenfolge, die die mit der Erkennung verknüpften Eigenschaften auflistet.

empfohlen: ***Boolesch***

Der Wert ist `true` wenn die Erkennung für die Triage empfohlen wurde.

empfohlene_Faktoren: ***Reihe von Zeichenketten***

Eine Reihe von Faktoren, die dazu geführt haben, dass die Erkennung für die Triage empfohlen wurde.

mitre_tactics: ***Reihe von Zeichenketten***

Eine Reihe von MITRE-Taktik-IDs, die mit der Erkennung verknüpft sind.

mitre_tactics_string: ***Schnur***

Eine Zeichenfolge, die die mit der Erkennung verknüpften MITRE-Taktik-IDs auflistet.

mitre_techniques: ***Reihe von Zeichenketten***

Eine Reihe von MITRE-Technik-IDs, die mit der Erkennung verknüpft sind.

mitre_techniques_string: ***Schnur***

Eine Zeichenfolge, die die MITRE-Technik-IDs auflistet, die mit der Erkennung verknüpft sind.

src:

Die Quelle, die an der Erkennung Teilnehmer war. Der Quellteilnehmer initiiert den mit der Erkennung verbundenen Verkehr. Jedes Quellteilnehmerobjekt enthält die folgenden Eigenschaften:

typ:

Der Objekttyp der Erkennungsquelle. Dieser Wert wird `Gerät`, `ipaddr`, oder `Anwendung`.

Hostname:

Der Hostname, der mit der Erkennungsquelle verknüpft ist.

ipaddr:

Die mit der Erkennungsquelle verknüpfte IP-Adresse. Dies ist die IP-Adresse, die während der Erkennung erkannt wurde.

Rolle:

Die Erkennungsfunktion der Quelle. Dieser Wert wird `Täter` oder `Opfer`.

Endpunkt:

Der Endpunkttyp der Quelle gemäß dem Protokoll. Dieser Wert wird `Client` oder `Absender`, abhängig vom Protokoll des Netzwerkverkehrs.

Nutzername:

Der mit der Erkennungsquelle verknüpfte Benutzername.

Gerät:

Das Quellgerät Gerät mit der Erkennung verknüpft ist. Dieses Objekt ist nur vorhanden, wenn der Quelltyp Gerät ist. Jedes Objekt enthält die folgenden Eigenschaften:

Deckel:

Die eindeutige ExtraHop-Objekt-ID des Quellgeräts.

Name:

Der Name des Quellgeräts.

iPads:

Die IP-Adressen, die dem Quellgerät zugeordnet sind. Diese IP-Adressen wurden bei der Erkennung nicht erkannt, waren aber zuvor dem Gerät zugeordnet.

Makaddr:

Die MAC-Adresse des Quellgeräts.

dst:

Der Zielteilnehmer an der Erkennung. Der Zielteilnehmer empfängt den anfänglichen Verkehr, der mit der Erkennung verbunden ist. Jedes Zielteilnehmerobjekt enthält die folgenden Eigenschaften:

typ:

Der Objekttyp des Erkennungsziels. Dieser Wert wird `Gerät`, `ipaddr`, oder `Anwendung`.

Hostname:

Der Hostname, der mit dem Erkennungsziel verknüpft ist.

ipaddr:

Die mit dem Erkennungsziel verknüpfte IP-Adresse. Dies ist die IP-Adresse, die während der Erkennung erkannt wurde.

Rolle:

Die Erkennungsfunktion des Ziels. Dieser Wert wird `Täter` oder `Opfer`.

Endpunkt:

Der Endpunkttyp des Ziels gemäß dem Protokoll. Dieser Wert wird `Server` oder `Empfänger`, abhängig vom Protokoll des Netzwerkverkehrs.

Nutzername:

Der mit dem Erkennungsziel verknüpfte Benutzername.

Gerät:

Das Zielgerät Gerät mit der Erkennung verknüpft ist. Dieses Objekt ist nur vorhanden, wenn der Quelltyp Gerät ist. Jedes Objekt enthält die folgenden Eigenschaften:

Deckel:

Die eindeutige ExtraHop-Objekt-ID des Zielgeräts.

Name:

Der Name des Zielgeräts.

iPads:

Die mit dem Zielgerät verknüpften IP-Adressen. Diese IP-Adressen wurden bei der Erkennung nicht erkannt, waren aber zuvor dem Gerät zugeordnet.

Makaddr:

Die MAC-Adresse des Zielgeräts.

primärer Täter: *Objekt*

(Veraltet) Ein Objekt, das den Haupttäter identifiziert und die folgenden Eigenschaften enthält:

extern: *Boolesch*

Der Wert ist `true` wenn die IP-Adresse des primären Täters außerhalb Ihres Netzwerk liegt.

ipaddr: *Schnur*

Die IP-Adresse des Haupttäters.

Name: *Schnur*

Der Name des Haupttäters.

Straftäter: ***Reihe von Objekten***

Eine Reihe von Täterobjekten, die mit der Erkennung verknüpft sind. Jedes Objekt enthält die folgenden Eigenschaften:

extern: ***Boolesch***

Der Wert ist `true` wenn die IP-Adresse des Täters außerhalb Ihres Netzwerk liegt.

ipaddr: ***Schnur***

Die IP-Adresse des Täters. Gilt für Feststellungen mit mehreren Tätern.

Name: ***Schnur***

Der Name des Täters. Gilt für Feststellungen mit mehreren Tätern.

primäres Opfer: ***Objekt***

(Veraltet) Ein Objekt, das das primäre Opfer identifiziert und die folgenden Eigenschaften enthält:

extern: ***Boolesch***

Der Wert ist `true` wenn die IP-Adresse des primären Opfers außerhalb Ihres Netzwerk liegt.

ipaddr: ***Schnur***

Die IP-Adresse des primären Opfers.

Name: ***Schnur***

Der Name des Hauptopfers.

Opfer: ***Reihe von Objekten***

Eine Reihe von Opferobjekten, die mit der Erkennung verknüpft sind. Jedes Objekt enthält die folgenden Eigenschaften:

extern: ***Boolesch***

Der Wert ist `true` wenn die IP-Adresse des Opfers außerhalb Ihres Netzwerk liegt.

ipaddr: ***Schnur***

Die IP-Adresse des Opfers. Gilt für Erkennungen mit mehreren Opfern.

Name: ***Schnur***

Der Name des Opfers. Gilt für Erkennungen mit mehreren Opfern.

api: ***Objekt***

Ein Objekt, das alle Felder enthält, die von `GET /detections/{id}operation`. Weitere Informationen finden Sie in der Einführung in die ExtraHop REST API.

Webhook-Beispiele

Die folgenden Abschnitte enthalten JSON-Vorlagen für gängige Webhook-Ziele.

Slack

Nachdem du eine Slack-App erstellt und eingehende Webhooks für die App aktiviert hast, kannst du einen eingehenden Webhook erstellen. Wenn du einen eingehenden Webhook erstellst, generiert Slack die URL, die du in das Feld Payload-URL in deiner Benachrichtigungsregel eingibst.

Das folgende Beispiel zeigt die JSON-Nutzlast für einen 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

Du kannst einem Teams-Kanal einen eingehenden Webhook als Connector hinzufügen. Nachdem Sie einen eingehenden Webhook konfiguriert haben, generiert Teams die URL, die Sie in das Feld Payload-URL in Ihrer Benachrichtigungsregel eingeben müssen.

Das folgende Beispiel zeigt die JSON-Nutzlast für einen 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 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 }}"
                }
            ]
        }
    ]
  }
]
}
```

Microsoft Teams mit adaptiven Karten

Sie können einen Webhook für den Versand adaptiver Karten konfigurieren, sodass Sie das Aussehen Ihres eingehenden Webhooks in Teams anpassen können.

Beachten Sie jedoch, dass wir die Adaptive Card nicht für die Anzeige in der mobilen Teams-App empfehlen, da Ihre Inhalte möglicherweise nicht wie erwartet gerendert werden.

Das folgende Beispiel zeigt die JSON-Nutzlast für einen Microsoft Teams-Webhook mit einer Adaptive Card:

```
{
   "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

In einem Google-Chatroom können Sie auf das Drop-down-Menü neben dem Raumnamen klicken und Webhooks verwalten auswählen. Nachdem Sie einen Webhook hinzugefügt und ihm einen Namen gegeben haben, generiert Google Chat die URL, die Sie in das Feld Payload-URL in Ihrer Benachrichtigungsregel eingeben müssen.

Das folgende Beispiel zeigt die JSON-Nutzlast für einen 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}}"
                                            }
                                        }
                                    }
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ]
}
```