

Auslöser

Veröffentlicht: 2024-04-13

Trigger bestehen aus benutzerdefiniertem Code, der automatisch bei Systemereignissen über die ExtraHop Trigger API ausgeführt wird. Sie können über die Trigger-API einen Trigger schreiben, bei dem es sich um einen JavaScript-Block handelt, um benutzerdefinierte Wire-Data-Ereignisse und -Metriken zu extrahieren, zu speichern und zu visualisieren, die für Ihr Unternehmen, Ihre Infrastruktur, Ihr Netzwerk, Ihre Kunden und Geschäftsanwendungen spezifisch sind.

Zu den gängigsten Workflows, die Sie über Trigger ausführen können, gehören die folgenden Operationen:

- Erstelle eine [Anwendung](#) Container, in dem Metriken für bestimmte Geräte gesammelt werden. Anwendungscontainer erweitern die gerätebasierten Ansichten, die das ExtraHop-System standardmäßig erstellt.
- Erstellen [benutzerdefinierte Metriken](#) und speichern Sie sie im ExtraHop-Datenspeicher. Zum Beispiel Benutzeragent-Daten, die von einem HTTP Anfrage ist keine Metrik, die in das ExtraHop-System integriert ist. Die ExtraHop Auslöser API bietet jedoch eine HTTP-Eigenschaft für Benutzeragenten , mit der Sie einen Trigger schreiben können, der Benutzeragentendaten als benutzerdefinierte Metrik sammelt.
- Generieren [Aufzeichnungen](#) und schreiben Sie sie in einen Datenspeicher, um sie langfristig zu speichern und abzurufen.
- Senden Sie Daten an Syslog-Verbraucher wie Splunk oder an Datenbanken von Drittanbietern, wie MongoDB oder Kafka, durch eine [Datenstrom öffnen](#).
- Führen Sie eine Universal Payload Analysis (UPA) durch, um auf TCP- und UDP-Nutzlasten von nicht unterstützten Daten zuzugreifen und diese zu analysieren Protokolle.
- Initiieren Sie Paketerfassungen, um einzelne Datenflüsse auf der Grundlage benutzerdefinierter Kriterien Datensatz. Ihr ExtraHop-System muss für die PCAP lizenziert sein, um auf diese Funktion zugreifen zu können.

Um alle Auslöser anzuzeigen, klicken Sie auf **Systemeinstellungen** Symbol  und dann klicken **Auslöser**. Auf der Trigger-Seite können Sie [einen Auslöser erstellen](#) oder klicken Sie auf das Häkchen neben einem Auslöser, um [Bearbeiten Sie die Trigger-Konfiguration](#) oder [das Trigger-Skript ändern](#).

Einen Auslöser planen

Das Schreiben eines Auslöser zur Erfassung benutzerdefinierter Metriken ist eine leistungsstarke Methode zur Überwachung Ihrer Anwendung - und Netzwerkleistung. Trigger verbrauchen jedoch Systemressourcen und können die Systemleistung beeinträchtigen, und ein schlecht geschriebener Auslöser kann zu unnötiger Systemlast führen. Bevor Sie einen Auslöser erstellen, sollten Sie auswerten, was Ihr Auslöser bewirken soll, ermitteln, welche Ereignisse und Geräte zum Extrahieren der benötigten Daten erforderlich sind, und ermitteln Sie, ob bereits eine Lösung existiert.

- Identifizieren Sie die spezifischen Informationen, die Sie sammeln müssen, indem Sie die folgenden Arten von Fragen stellen:
 - Wann laufen meine SSL-Zertifikate ab?
 - Erhält mein Netzwerk Verbindungen über nicht autorisierte Ports?
 - Wie viele langsame Transaktionen verzeichnet mein Netzwerk?
 - Welche Daten möchte ich über einen offenen Datenstrom an Splunk senden?
- Überprüfen Sie die Metrischer Katalog um festzustellen, ob bereits eine integrierte Metrik existiert, die die benötigten Daten extrahiert. Integrierte Metriken belasten das System nicht zusätzlich.
- Identifizieren Sie, welches System Veranstaltungen produzieren Sie die Daten, die Sie sammeln möchten. Beispielsweise kann ein Auslöser, der die Aktivität von Cloud-Anwendungen in Ihrer Umgebung überwacht, bei HTTP-Antworten und beim Öffnen und Schließen von SSL-Verbindungen ausgeführt werden. Eine vollständige Liste der Systemereignisse finden Sie in [ExtraHop Trigger API-Referenz](#).

- Machen Sie sich mit den API-Methoden und -Eigenschaften vertraut, die in der [ExtraHop Trigger API-Referenz](#). Bevor Sie beispielsweise mit der Planung Ihres Auslöser zu weit kommen, überprüfen Sie die Referenz, um sicherzustellen, dass die Eigenschaft, die Sie extrahieren möchten, verfügbar ist, oder um herauszufinden, welche Eigenschaften in einem Standard-CIFS-Datensatz gesammelt werden.
- Legen Sie fest, wie Sie die vom Auslöser gesammelten Daten visualisieren oder speichern möchten. Sie können beispielsweise Metriken auf einem anzeigen Dashboard oder von Protokoll, Sie können Aufzeichnungen an den Recordstore senden.
- Stellen Sie fest, ob bereits ein Auslöser existiert, der Ihren Anforderungen entspricht oder leicht geändert werden könnte. Beginnen Sie immer mit einem bereits vorhandenen Auslöser, wann immer dies möglich ist. Suchen Sie in den folgenden Ressourcen nach einem vorhandenen Auslöser:
 - [Bestehende Trigger auf der Trigger-Seite](#)
 - [Die ExtraHop Community-Foren](#)

Auslöser bauen

Wenn Sie feststellen, dass Sie einen neuen Auslöser erstellen müssen, machen Sie sich mit den folgenden Aufgaben vertraut, die abgeschlossen werden müssen:

- [Den Auslöser konfigurieren](#) um Details wie den Namen des Auslöser und ob das Debuggen aktiviert ist, bereitzustellen. Geben Sie vor allem an, bei welchen Systemereignissen der Auslöser ausgeführt wird. Wenn Sie beispielsweise möchten, dass Ihr Auslöser jedes Mal ausgeführt wird, wenn eine SSH-Verbindung geöffnet wird, geben Sie an `SSH_OPEN` als auslösendes Ereignis.
- [Schreiben Sie das Trigger-Skript](#), das die Anweisungen angibt, die der Auslöser ausführt, wenn ein für den Auslöser konfiguriertes Systemereignis eintritt. Das Triggerskript kann Anweisungen für einfache Aufgaben wie die Erstellung einer benutzerdefinierten Gerätezählmetrik namens „slow_rsp“ oder für komplexere Aufgaben wie die Überwachung und Erfassung von Statistiken über die Cloud-Anwendungen, auf die in Ihrer Umgebung zugegriffen wird, bereitstellen.

Nachdem der Auslöser abgeschlossen ist und ausgeführt wird, ist es wichtig zu überprüfen, ob der Auslöser erwartungsgemäß funktioniert.

- [Das Debug-Log anzeigen](#) für die erwartete Ausgabe von Debug-Anweisungen im Trigger-Skript. Das Protokoll zeigt auch alle Laufzeitfehler und Ausnahmen an, die Sie beheben müssen.
- [Überwachen Sie die Leistungskosten](#) indem die Anzahl der vom Auslöser verbrauchten Zyklen verfolgt wird.
- [Überprüfen Sie die Diagramme zur Systemintegrität](#) für Trigger-Ausnahmen, Drops aus der Trigger-Warteschlange und unerwartete Aktivitäten.
- Vergewissern Sie sich, dass das Trigger-Skript dem entspricht [Leitfaden mit bewährten Methoden für Trigger](#).

In Auslösern navigieren

Die Seite Trigger enthält eine Liste der aktuellen Trigger mit den folgenden Informationen:

Name

Der benutzerdefinierte Name des Auslöser.

Autor

Der Name des Benutzers, der den Auslöser geschrieben hat. Standard-Trigger zeigen ExtraHop für dieses Feld an.

Beschreibung

Die benutzerdefinierte Beschreibung des Auslöser.

Zuweisungen

Die Geräte oder Gerätegruppen, denen der Auslöser zugewiesen ist.

Status

Ob der Auslöser aktiviert ist. Wenn der Auslöser aktiviert ist, wird auch die Anzahl der Gerätezuweisungen angezeigt.

Debug-Protokoll

Ob das Debuggen aktiviert ist. Wenn das Debuggen aktiviert ist, werden die Ausgaben von Debug-Anweisungen im Trigger-Skript protokolliert [Debug-Log-Ausgabe](#).

Ereignisse

Die Systemereignisse, die dazu führen, dass der Auslöser ausgeführt wird, wie HTTP_RESPONSE.

Geändert

Das letzte Mal, dass der Auslöser geändert wurde.

Triggers

<input type="checkbox"/>	Name ↑	Author	Description	Assignments	Status	Debug Log	Events	Modified
<input type="checkbox"/>	Active Direct...	ExtraHop	Custom metrics for Active Direct...	0	■ ENABLED	■ DISABLED	CIFS_RESPONSE, ...	2017-11-2
<input type="checkbox"/>	AD: DNS Ser...	ExtraHop	DNS service (SRV) resource reco...	0	■ DISABLED	■ DISABLED	DNS_REQUEST, D...	2018-08-2
<input type="checkbox"/>	AD: Group Po...	ExtraHop	Group Policy custom metrics for ...	0	■ DISABLED	■ DISABLED	CIFS_RESPONSE	2018-08-2