Trigger

Veröffentlicht: 2024-09-26

Trigger bestehen aus benutzerdefiniertem Code, der bei Systemereignissen automatisch über die ExtraHop Trigger API ausgeführt wird. Sie können über die Trigger-API einen Trigger, bei dem es sich um einen JavaScript-Block handelt, schreiben, 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:

- Erstellen Sie 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 User-Agent-Daten, die von einem generiert wurden HTTP Anfrage ist keine in das ExtraHop-System integrierte Metrik. Die ExtraHop Auslöser API bietet jedoch eine User-Agent-HTTP-Eigenschaft , mit der Sie einen Trigger schreiben können, der User-Agent-Daten als benutzerdefinierte Metrik sammelt.
- Generieren Aufzeichnungen und schreiben Sie sie zur langfristigen Speicherung und zum Abrufen in einen Datenspeicher.
- 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-Payloads zuzugreifen und diese von nicht unterstützten 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 klicken Sie dann **Trigger**. Auf der Seite „Auslöser“ können Sie einen Auslöser erstellen oder wählen Sie das Häkchen neben einem Auslöser, um Bearbeiten Sie die Triggerkonfiguration oder modifizieren Sie das Trigger-Skript.

Einen Auslöser planen

Das Schreiben eines Auslöser zur Erfassung benutzerdefinierter Metriken ist eine leistungsstarke Methode, um Ihre Anwendungs - und Netzwerkleistung zu überwachen. Trigger verbrauchen jedoch Systemressourcen und können die Systemleistung beeinträchtigen, und ein schlecht geschriebener Auslöser kann zu unnötiger Systemlast führen. Bevor Sie einen Auslöser erstellen, evaluieren Sie, was Ihr Auslöser erreichen soll, ermitteln Sie, welche Ereignisse und Geräte erforderlich sind, um die benötigten Daten zu extrahieren, 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 TLS-Zertifikate ab?
  - Erhält mein Netzwerk Verbindungen über nicht autorisierte Ports?
  - Wie viele langsame Transaktionen hat 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 vorhanden ist, 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 TLS-Verbindungen ausgeführt werden. Eine vollständige Liste der Systemereignisse finden Sie in der 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 gehen, überprüfen Sie die Referenz, um sicherzustellen, dass die Eigenschaft, die Sie extrahieren möchten, verfügbar ist, oder um herauszufinden, welche Eigenschaften in einem Standard-SMB-Datensatz erfasst sind.
- Legen Sie fest, wie Sie die vom Auslöser gesammelten Daten visualisieren oder speichern möchten. Zum Beispiel können Sie Metriken auf einem Dashboard oder von Protokoll, Sie können Datensätze an den Recordstore senden.
- Stellen Sie fest, ob bereits ein Auslöser existiert, der Ihren Anforderungen entspricht oder leicht geändert werden kann. Beginnen Sie nach Möglichkeit immer mit einem bereits vorhandenen Auslöser. Suchen Sie in den folgenden Ressourcen nach einem vorhandenen Auslöser:
  - Bestehende Trigger auf der Seite „Trigger“
  - Die ExtraHop Community-Foren

Trigger bauen

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

- Konfiguriere den Auslöser um Details wie den Triggernamen 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 Triggerereignis.
- Schreiben Sie das Trigger-Skript, das die Anweisungen angibt, die der Auslöser ausführt, wenn ein für den Auslöser konfiguriertes Systemereignis eintritt. Das Trigger-Skript kann Anweisungen für eine einfache Aufgabe wie das Erstellen einer benutzerdefinierten Metrik zur Geräteanzahl namens „slow_rsp“ oder für komplexere Aufgaben wie die Überwachung und Erfassung von Statistiken über die Cloud-Anwendungen bereitstellen, auf die in Ihrer Umgebung zugegriffen wird.

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.
- Überprüfe die Diagramme zum Systemstatus für Trigger-Ausnahmen, Ausfälle aus der Trigger-Warteschlange und unerwartete Aktivitäten.
- Prüfen Sie, ob das Trigger-Skript den Leitfaden zu bewährten Methoden für Triggers.

Navigiere durch Trigger

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 Debugging aktiviert ist. Wenn das Debuggen aktiviert ist, werden die Ausgaben von Debug-Anweisungen im Triggerskript im Debug-Log-Ausgabe.

Ereignisse

Die Systemereignisse, die zur Ausführung des Auslöser führen, wie `HTTP_RESPONSE`.

Geändert

Das letzte Mal, dass der Auslöser geändert wurde.