# Sammeln Sie L7-Datensätze mit einem Auslöser

Veröffentlicht: 2023-09-13

L7-Protokolle können über eine globale Triggerfunktion als Datensatz festgeschrieben (gesammelt und gespeichert) werden. L7-Datensätze umfassen Nachrichten, Transaktionen und Sitzungen, die über gängige L7-Protokolle wie DNS, HTTP und SSL gesendet werden.

In den folgenden Schritten erfahren Sie, wie Sie Datensätze für jedes Gerät sammeln, das eine HTTP-Antwort sendet oder empfängt.

Erfahre mehr über ExtraHop Records.

Zunächst schreiben wir einen Auslöser, um Informationen aus dem integrierten HTTP-Datensatztyp mit der Methode commitRecord () zu sammeln, die für alle verfügbar ist Protokollklassen. Die grundlegende Trigger-Syntax lautet `<protocol>.commitRecord()`. Dann weisen wir den Auslöser einem Server zu. Schließlich werden wir überprüfen, ob die Aufzeichnungen an den Recordstore gesendet werden.

**Bevor Sie beginnen**

- Sie müssen über einen konfigurierten Recordstore verfügen, z. B. ExtraHop Recordstore, Splunk, oder Google BigQuery
- Diese Anweisungen setzen eine gewisse Vertrautheit voraus mit ExtraHop-Trigger, für die Erfahrung mit JavaScript erforderlich ist. Alternativ können Sie L7-Datensatzsammlung konfigurieren durch das ExtraHop-System.

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 **Auslöser**.
3. klicken **Erstellen**.
4. In der Trigger erstellen Fenster, vervollständigen Sie Ihre Informationen, ähnlich dem folgenden Beispiel:
   - **Name:** `HTTP-Antworten`
   - **Beschreibung:** `Dieser Auslöser sammelt HTTP-Antworten.`
5. Markieren Sie das Kästchen neben **Debug-Log aktivieren**.
6. Wählen Sie in der Dropdownliste Ereignisse **HTTP_RESPONSE**.
7. In der **Zuweisungen** Textfeld, suchen Sie nach einem aktiven Webserver, für den Sie Datensätze sammeln möchten, und wählen Sie den Server aus.
8. Geben Sie im rechten Bereich den folgenden Beispielcode ein:

```
HTTP.commitRecord();
debug ("committing HTTP responses");
```

   Dieser Code generiert Datensätze für den HTTP-Datensatztyp, wenn `HTTP_RESPONSE` Ereignis tritt ein und entspricht dem integrierten Datensatzformat für HTTP.
9. klicken **Speichern**.

**Nächste Schritte**
Warten Sie einige Minuten, bis die Datensätze erfasst wurden, und überprüfen Sie dann im nächsten Schritt, ob Ihre Datensätze erfasst werden, indem Sie auf **Rekorde** aus dem oberen Menü und dann klicken **Aufzeichnungen ansehen** um eine Abfrage zu starten.

Wenn Sie nach 5 Minuten keine HTTP-Einträge sehen, klicken Sie auf **Debug-Protokoll** Klicken Sie unten auf der Seite im Trigger-Editor auf einen Tab, um zu sehen, ob es Fehler gibt, die Sie beheben können. Wenn der Auslöser ausgeführt wird, wird die Meldung „HTTP-Antworten übergeben“ angezeigt. Wenn

nach der Ausführung des Auslöser keine Datensätze angezeigt werden, wenden Sie sich an ExtraHop-Unterstützung.