Sammle L7-Datensätze mit einem Auslöser

Veröffentlicht: 2025-02-04

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

Zuerst schreiben wir einen Auslöser, um Informationen aus dem eingebauten HTTP-Recordtyp mit der commitRecord () -Methode zu sammeln, die auf allen 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 einen konfigurierten Recordstore haben, z. B. ExtraHop Recordstore, Splunk, oder Google BigQuery
- Diese Anweisungen setzen eine gewisse Vertrautheit mit ExtraHop-Auslöser, die Erfahrung mit JavaScript erfordern. 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 auf **Trigger**.
3. Klicken Sie **Erstellen**.
4. In der Trigger erstellen Bereich, vervollständigen Sie Ihre Informationen, ähnlich wie im folgenden Beispiel:
   - **Name:** `HTTP-Antworten`
   - **Beschreibung:** `Dieser Auslöser sammelt HTTP-Antworten.`
5. Markieren Sie das Kästchen neben **Debug-Log aktivieren**.
6. Wählen Sie im Drop-down-Menü 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 Sie **Speichern**.

Nächste Schritte

Warten Sie einige Minuten, bis die Datensätze erfasst sind, und überprüfen Sie dann im nächsten Schritt, ob Ihre Aufzeichnungen erfasst werden, indem Sie auf **Aufzeichnungen** aus dem Hauptmenü und dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

Wenn Sie nach 5 Minuten keine HTTP-Einträge sehen, klicken Sie auf **Debug-Protokoll** Tabulatortaste unten auf der Seite im Trigger-Editor, um zu sehen, ob es Fehler gibt, die Sie beheben können. Wenn der Auslöser läuft, wird die Meldung „Committing HTTP Responses“ angezeigt. Wenn nach dem Ausführen des Auslöser keine Datensätze angezeigt werden, wenden Sie sich an ExtraHop-Unterstützung.