Collect L7 records with a trigger

Published: 2024-04-02

L7 protocols can be committed (collected and stored) as a record through a global trigger function. L7 records include messages, transactions, and sessions sent over common L7 protocols such as DNS, HTTP, and SSL.

In the following steps, you will learn how to collect records for any device that sends or receives an HTTP response.

Learn more about ExtraHop Records.

First, we will write a trigger to collect information from the built-in HTTP record type with the commitRecord() method, which is available on all protocol classes. The basic trigger syntax is `<protocol>.commitRecord()`. Then, we will assign the trigger to a web server. Finally, we will verify that the records are being sent to the recordstore.

Before you begin

- You must have a configured recordstore, such as an ExtraHop recordstore, Splunk, or Google BigQuery
- These instructions assume some familiarity with ExtraHop Triggers, which require experience with JavaScript. Alternatively, you can configure L7 record collection through the ExtraHop system.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon, and then click **Triggers**.
3. Click **Create**.
4. In the Create Trigger pane, complete your information, similar to the following example:
   - **Name:** `HTTP Responses`
   - **Description:** `This trigger collects HTTP responses.`
5. Select the checkbox next to **enable debug log**.
6. From the Events drop-down list, select **HTTP_RESPONSE**.
7. In the **Assignments** text box, search for an active web server that you want to collect records for and select the server.
8. In the right pane, type the following example code:

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

   This code generates records for the HTTP record type when the `HTTP_RESPONSE` event occurs and corresponds to the built-in record format for HTTP.
9. Click **Save**.

Next steps

Wait a few minutes for records to be collected, and then verify that your records are being collected in the next step by clicking **Records** from the top menu, and then clicking **View Records** to start a query.

If you do not see any HTTP records after 5 minutes, click the **Debug Log** tab at the bottom of the page in the Trigger Editor to see if there are any errors you can resolve. If the trigger is running, the message "committing HTTP responses" is displayed. If records do not appear after the trigger is running, contact ExtraHop Support.