Export ExtraHop metrics to Splunk

Published: 2021-12-31

The ExtraHop system monitors network and application performance by gathering data passively on the network. It offers deep and customizable analytics of wire data in real time.

The Splunk big-data platform offers storage and correlation of a variety of data sources. Splunk collects and indexes data generated by applications, servers, and other devices.

Integrating ExtraHop with Splunk enables long-term storage of wire data and correlation of wire data with other sources, such as machine data from logs.

The ExtraHop Add-On exports ExtraHop wire data metrics as Splunk events through the ExtraHop REST API.

Note: For a deeper integration with Splunk, you can configure the ExtraHop system to send transaction-level records to a Splunk server for long-term storage. Learn more about enabling Splunk as your recordstore.

Install and configure the ExtraHop Add-On for Splunk

The ExtraHop Add-On for Splunk enables you to export ExtraHop wire data metrics as Splunk events. You can export metrics about any activity group, device group, or application from an ExtraHop system.

The ExtraHop Add-On for Splunk collects 30-second metrics through the ExtraHop REST API. Dataset metrics are collected for 5th, 25th, 50th, 75th, and 95th percentiles. All detections collected by the ExtraHop Add-On for Splunk are assigned the extrahop-detection source type.

Before you begin
The ExtraHop Add-On for Splunk requires the following software:

- ExtraHop firmware version 7.1.2 or later
- Splunk Enterprise version 7.3 or earlier

Note: Because this add-on runs on Splunk Enterprise, all Splunk Enterprise system requirements apply.

1. Download the ExtraHop Add-On for Splunk from the SplunkBase site.
2. Install the add-on according to the Splunk Add-Ons documentation.
3. Optional: Configure proxy settings.

   If you want to connect the add-on to your ExtraHop system over a proxy, you must configure proxy settings.

   a) On the Splunk Web home screen, click the ExtraHop Add-On for Splunk icon in the navigation bar to launch the add-on.
   b) Click **Configuration**.
   c) On the Proxy tab, configure proxy settings.

Create the metric inputs

You must create data inputs that collect information from an ExtraHop system to retrieve wire data metrics.

You can create metric inputs for any information that is available through the ExtraHop REST API. Each input can only collect metrics for a single metric category. If you want to collect metrics for multiple categories, you must create multiple inputs. Find the REST API parameters you need, such as Metric Category and Metric Name, in the Metric Catalog.

1. On the Splunk Web home screen, click the ExtraHop Add-On for Splunk icon in the navigation bar to launch the add-on.
2. Click **Inputs**.
3. Click **Create New Input**.
4. In the Add ExtraHop Add-On for Splunk window, specify settings for the input
5. Click **Add**.

Create a data input for detections

The ExtraHop Add-On for Splunk contains a sourcetype for ExtraHop detections. In order to receive detections in Splunk, you must configure a data input for ExtraHop detections and configure the ExtraHop Detection SIEM Connector on your ExtraHop system.

Configure a data input in Splunk

Detection data can be sent from a ExtraHop system to Splunk through the syslog protocol. Complete the procedure in the Splunk documentation to get data from a TCP or UDP port. You must set the source type value to `extrahop-detection`.

Configure the ExtraHop Detection SIEM Connector

Follow the instructions on the ExtraHop Detection SIEM Connector bundle page to configure your ExtraHop system to send detections data to Splunk.

Troubleshoot the ExtraHop Add-On for Splunk

It might take some time for the data to be indexed initially by Splunk. To troubleshoot any errors that might occur with the add-on, view the `splunk.log` and `ta_extrahop_addon_extrahop.log` log files.

IP addresses, MAC addresses, and hostnames might not appear in Splunk when this data is missing from the “extrahop_deviceoid_lookup” KV store lookup table. In ExtraHop Add-On for Splunk v1.1.1 and later, IP addresses, MAC addresses, and hostnames are saved to the KV Store at the time of data ingest.