Integrate ExtraHop with Splunk

Published: 2019-07-15

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.

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

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.

Although there are many ways to export ExtraHop data to Splunk, we recommend that you install the ExtraHop Add-On for Splunk and the ExtraHop App for Splunk. The ExtraHop Add-On exports ExtraHop wire data metrics as Splunk events through the ExtraHop REST API, and the ExtraHop App adds important information to the exported data, such as device IP addresses.

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 Discover or Command appliance. After the Splunk platform indexes the events, you can analyze the data through the dashboards in the ExtraHop App for Splunk or by creating your own visualizations.

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 specifications:

- ExtraHop firmware version 7.1.2 or later
- Spunk Enterprise version 7.0 or later

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 appliance 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 appliance to retrieve wire data metrics.

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

   Note: 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.

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 Command or Discover appliance.

Configure a data input in Splunk

Detection data can be sent from a Command or Discover appliance 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 appliance to send detections data to Splunk.

Install and configure the ExtraHop App for Splunk

The ExtraHop App for Splunk adds information to the data that the ExtraHop Add-On for Splunk collects, including the IP addresses, MAC addresses, and hostnames of devices discovered by the ExtraHop system. The app also creates default inputs to collect metrics about HTTP, DNS, and storage activity and then builds dashboards to display that information.

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

- ExtraHop firmware version 7.1.2 or later
- Spunk Enterprise version 7.0 or later
- ExtraHop Add-On for Splunk 1.1.1 or later

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

1. Download the ExtraHop App for Splunk from the SplunkBase site.
2. Install the app according to the Splunk Add-Ons documentation.
3. Optional: Add pre-configured inputs and dashboards.

   After you install the ExtraHop App for Splunk, you can add pre-configured Splunk dashboards and inputs for HTTP, DNS, and storage activity. Note that the saved searches included in the app do not require you to create the dashboards and inputs; the saved searches will run automatically after the app is installed.

   a) On the Splunk Web home screen, click the ExtraHop App for Splunk icon in the navigation bar to launch the app.
   b) Click **Configuration** > **Setup**.

      Note: If the ExtraHop Add-On for Splunk is disabled or uninstalled, you will be prompted to enable or install the add-on before continuing.

   c) Specify the hostname or IP address of the ExtraHop Discover or Command appliance that you are collecting metrics from.
   d) Specify a valid ExtraHop REST API key for the appliance.

e) Click **Submit**.
f) After the app verifies connectivity to the ExtraHop appliance, specify a prefix for the app's inputs.

   For example, if you specify `extrahop`, the app will create four ExtraHop inputs named `extrahop_dns`, `extrahop_http`, `extrahop_nas`, and `extrahop_nas_fileinfo`.
g) Click **Create Defaults**.

The data inputs created by this process are configured with an interval of 300 seconds and an index of "main". These settings can be changed by editing the data inputs through the ExtraHop Add-On for Splunk or by manually editing the `inputs.conf` files.

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. Additionally, the ExtraHop App for Splunk includes a saved search that retrieves this information from an ExtraHop appliance and adds the information to Splunk in case that information was not already cached.

The search is scheduled to run every six hours. You can also run the search manually at any time by following these steps:

1. On the Splunk Web home screen, click **Settings** > **Knowledge** > **Searches, reports, and alerts**.
2. From the App drop-down menu, select **ExtraHop App for Splunk**.
3. Click **Run** next to the saved search named Retrieve Device Information.