Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security

Generated: 4/05/2022 7:23 am

Upload a STIX or OpenIOC structured threat intelligence file in Splunk Enterprise Security

Upload threat intelligence in a STIX or OpenIOC file to Splunk Enterprise Security using one of the following methods:

- Upload a STIX or OpenIOC file using the Splunk Enterprise Security interface
- Add STIX or OpenIOC files using the REST API
- Add STIX or OpenIOC files using the file system

Upload a STIX or OpenIOC file using the Splunk Enterprise Security interface

Splunk Enterprise Security supports adding the following file types directly in the Splunk Enterprise Security interface:

- OpenIOC 1.0 and 1.1
- STIX 1.0, 2.0, and 2.1
- CSV

Parsing STIX documents of version 2.0 and version 2.1 parses STIX observable objects such as `type: "observed-data"` from the threat intelligence document as outlined in the `collections.conf` configuration file. The STIX pattern syntax used in STIX "indicator" objects and elsewhere is not currently supported.

To add a file in the Splunk Enterprise Security interface, complete the following steps:

1. On the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Click **New**.
3. Select **IOC/STIX/STIX 2** from the drop down menu.
   This opens the **Add Intelligence Document** dialog.
4. Type the information for the threat intelligence document that you want to upload.
5. Click on the **General** tab and type a **Weight** for the threat intelligence file. The weight of a threat intelligence file increases the risk score of objects associated with threat intelligence on this list.
6. Select the **Threat intelligence** checkbox if you want to classify the intelligence document as threat intelligence. Classifying an intelligence document as threat intelligence triggers specific workloads. For more information on how to configure intelligence documents, see Configure intelligence documents.

   > Use the tooltips provided in the UI to populate the remaining fields based on the intelligence document that you plan to upload.
7. (Optional) Click the **Advanced** tab and select the **Sinkhole** check box. This deletes the file after the intelligence from the file is processed.
8. Click **Save**.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add STIX or OpenIOC files using the REST API

The Splunk Enterprise Security REST API supports uploading threat intelligence files in OpenIOC, STIX, or CSV format. See Threat Intelligence API reference.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.