Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Configure intelligence documents in Splunk Enterprise Security

Generated: 6/13/2022 9:46 am

Configure intelligence documents in Splunk Enterprise Security

Use the Splunk Enterprise Security app UI to configure intelligence documents and select specific workloads and actions that you want to trigger after the document is downloaded or uploaded.

Specific type of workloads are triggered based on whether an intelligence document is defined as threat intelligence or not. If an intelligence document is also a threat document, a workload is automatically triggered for processing the threat document. If the intelligence document is not defined as a threat document, you can select the workload actions (For example: user defined saved searches) that you want to trigger after the intelligence document is downloaded or uploaded.

Therefore, workloads allow you to streamline the parsing and processing of intelligence documents and help to improve the extensibility and performance of the threat intelligence framework.

> You may configure a customized workload for your intelligence document only if it is not labeled as threat intelligence.

Configuring the workloads in the UI automatically populates the workload settings in the `[threatlist]` stanza for the intelligence document in the `inputs.conf`configuration file. The workload actions run synchronously, one after the other, in the order in which they appear in the workload settings of the `[threatlist]` stanza.

(Optional) Configure workloads for intelligence documents

Configure the workload settings for intelligence documents only if they are not defined as threat intelligence.

Prerequisite
The intelligence document is not defined as threat intelligence. You may verify this in the corresponding `[threatlist]` stanza of the `inputs.conf` configuration file by checking if `is_threatintel = 0`.

Steps

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management > Sources**.
   This displays the list of intelligence documents in the app that are sorted by Interval, Type, URL, Weight, and Status.
   To edit a `[threatlist]` stanza setting that is unavailable in the Threat Management Intelligence UI for version 6.4.0 or higher, click on the **Advanced Edit** tab next to the intelligence document. This opens the **Intelligence Download Settings** dialog that you may use to edit the configuration settings. However, you must refresh the UI for the edits made in the **Intelligence Download Settings** dialog to be visible.
2. Click on the name of the intelligence document for which you want to configure a customizable workload.
   This displays the **Add Intelligence Document** form. The form displays only fields that are relevant for the selected document **Type** and helps to streamline the editing process.
3. Click on the **General** tab in the **Add Intelligence Document** form.
4. Scroll down to deselect **Threat Intelligence**.
   This action removes the document from threat intelligence along with its implicit workload. Instead, it now enables you to add a custom workload to the document.

   > If the '"Threat Intelligence"' field is enabled, the document is automatically added to threat intelligence based on the file parser settings or type of document.

5. Click on the **Advanced** tab in the **Add Intelligence Document** form.
6. From the **Workloads** drop down menu, select the workloads or actions that you want to add to your document.

Splunk Enterprise Security only supports adding saved searches as workloads for the intelligence document.