Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Upload a custom CSV file of threat intelligence in Splunk Enterprise Security

Generated: 5/17/2022 10:15 pm

Upload a custom CSV file of threat intelligence in Splunk Enterprise Security

You can add a custom file of threat intelligence to Splunk Enterprise Security.

Prerequisite

Format the custom CSV file by adding headers for each type of intelligence in the file. The custom file can contain multiple types of intelligence, but you must include headers for each column in the CSV file. See Supported types of threat intelligence in Splunk Enterprise Security for the headers relevant for each type of threat intelligence.

Add the custom file to Splunk Enterprise Security.

1. On the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Type a file name for the file you want to upload. The file name you type becomes the name of the file saved to `$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/lookups`. The file name cannot include spaces or special characters and is saved in `$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/lookups` to ensure that all the search heads in a cluster are synchronized.
3. Upload the CSV-formatted file.
4. Type a **Weight** for the threat list. The weight of a threat file increases the risk score of objects associated with threat intelligence on this list.
5. (Optional) Select the **Overwrite** check box. If you have previously uploaded a file with the same file name, select this check box to overwrite the previous version of the file.
6. (Optional) In the **Advanced** tab, select the **Sinkhole** check box. This deletes the file after the intelligence from the file is processed.
7. 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.