Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Change existing intelligence in Splunk Enterprise Security

Generated: 4/15/2022 7:25 pm

Change existing intelligence in Splunk Enterprise Security

After you add intelligence to Splunk Enterprise Security, you can make changes to the settings to make sure the intelligence you correlate with events is useful.

Disable an intelligence source

Disable an intelligence source to stop downloading information from the source. This also prevents new threat indicators from the disabled source from being added to the threat intelligence collections.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Find the intelligence source.
3. Under **Status**, click **Disable**.

Disable individual threat artifacts

To prevent individual threat artifacts on a threat list from creating notable events if they match events in your environment, disable individual threat artifacts. If you have command line access to the Enterprise Security search head, you can disable individual threat artifacts using the REST API. See Threat Intelligence API reference in Splunk Enterprise Security *REST API Reference*.

Edit an intelligence source

Change information about an existing intelligence source, such as the retention period or the download interval for the source.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Click the name of the intelligence source you want to edit.
3. Make changes to the fields as needed.
4. Save your changes.

By default, only administrators can edit intelligence sources. To allow non-admin users to edit intelligence sources, see Adding capabilities to a role in the *Installation and Upgrade Manual*.

Configure threat source retention

Remove threat intelligence from the KV Store collections in Splunk Enterprise Security based on the date that the threat intelligence was added to Enterprise Security.

The default maximum age is `-30d` for 30 days of retention in the KV Store. To remove the data more often, use a smaller number such as `-7d` for one week of retention. The maximum age field cannot be left black because storing the collection indefinitely can impact performance.

Define the maximum age of the threat intelligence.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Select an intelligence source.

3. Change the **Maximum age** setting using a relative time specifier.

Review the logic for retention

Threat intelligence entries are removed when you meet the following conditions:

- The entry is no longer in the source threat list
- The threat list is processed
- The time that the threat list was last seen and processed is earlier than the `max_age` time setting
- The threat retention input runs every 24 hours by default

As of Enterprise Security 6.4.0, threat collection data is no longer deleted from the KV Store based only on the `max_age` time setting defined in the `inputs.conf` file compared to the `time` field in each threat intelligence collection.

The `time` field in the threat collection is updated when any of the following items are true:

- The `[threatlist]` stanza has been updated.
- Non-TAXII document's hash value has changed.
- TAXII document's mod-time has changed.

Additional fields are now included in the `[threat_group_intel]` stanza called `last_seen` and `last_processed`. The delete processing logic follows:

Last processed
: When the threat intelligence document is processed, the last_processed field is updated. It is processed based on the interval in Threat Intelligence Management.

Time
: When threat intelligence data is inserted after processing, the time field is updated. This happens when the data is new or when the data contains changes.

Last seen
: Whether or not anything is inserted or revised after processing, the last_seen field is updated.

If threat intelligence has not been processed but it has been seen within the maximum age time frame, the data is not deleted. The `time` field isn't taken at face value because the data has not been processed, therefore the contents of the document are unknown. After the document has been processed, only then can it be determined which items to remove. For example, the process time falls within the max age time.

Otherwise, data gets deleted if the `time` field exceeds the `max_age` field.

Configure threat intelligence file retention

Configure how long files are stored by Splunk Enterprise Security after processing. You can modify the settings to manage global file retention for intelligence sources, or modify individual settings for each download or upload to more granularly control file retention.

Modular inputs managed on the Threat Intelligence Management page handle file parsing of intelligence sources. The parsing process includes analyzing the downloaded file, extracting relevant values, saving it into a lookup, and storing matching data into an index. You have the option to parse the file and delete it, also called sinkhole, or parse the file and keep it as a reference.

Splunk Enterprise Security does not sinkhole an uploaded file (file:// threat intel types) or lookup files (lookup:// threat intel types). Otherwise, if sinkhole is set to True, Splunk Enterprise Security deletes the intelligence file after processing.

Remove files associated with a specific download

Use the sinkhole check box to remove files associated with a threat intelligence download.

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Locate the threat intelligence download.
3. Click on the **Advanced** tab.
4. Select the **Sinkhole** check box.
5. Save your changes.