Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Add threat intelligence with a custom lookup file in Splunk Enterprise Security

Generated: 6/13/2022 9:46 am

Add threat intelligence with a custom lookup file in Splunk Enterprise Security

You can add threat intelligence to Splunk Enterprise Security as a custom lookup file. Add a custom lookup file in this way if you want to edit the lookup file in Splunk Enterprise Security. If you want to add a lookup file to have the intelligence in it extracted once, upload the CSV file instead. See Upload a custom CSV file of threat intelligence in Splunk Enterprise Security.

A lookup-based threat source can add data to any of the supported threat intelligence types, such as file or IP intelligence. See Supported types of threat intelligence in Splunk Enterprise Security.

Prerequisite

Create the custom CSV 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.

Steps

First, add the lookup to Splunk Enterprise Security.

1. Select **Configure > Content > Content Management**.
2. Select **Create New Content > Managed Lookup**.
3. Click **Create New**.
4. Select the lookup file to upload.
5. Select an **App** of **SA-ThreatIntelligence**.
6. (Optional) Modify the file name. For example, type `threatindicatorszerodayattack.csv`.
7. (Optional) Modify the definition name. For example, `zero_day_attack_threat_indicators_list`.
8. Leave the default lookup type of **Manual editing**.
9. Type a label for the lookup. The label appears as the name for the lookup on the Content Management page. For example, Zero Day Threat Indicators.
10. Type a description for the lookup. For example, File-based threat indicators from zero day malware.
11. Save.

Next, add a threat source input stanza that corresponds to the lookup file so that ES can parse the threat intelligence.

1. Select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Click **New**.
3. Type a **Name**. The name cannot include spaces. For example, zero_day_attack_threat_indicators.
4. Type a **Type**. For example, zero_day_IOCs.
5. Type a **Description**. For example, File-based threat indicators from zero day malware.
6. Type a **URL** that references the lookup definition you created. For example, `lookup://zero_day_attack_threat_indicators_list`
7. (Optional) Change the default **Weight** for the threat data.
8. (Optional) Change the default **Retry interval** for the lookup.
9. If your lookup contains multiple types of threat intelligence, type the headers in the **Fields** section.
10. 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.