Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Add threat intelligence to Splunk Enterprise Security

Generated: 4/21/2022 10:11 pm

Add threat intelligence to Splunk Enterprise Security

As an ES administrator, you can correlate indicators of suspicious activity, known threats, or potential threats with your events by adding threat intelligence to Splunk Enterprise Security. Adding threat intelligence enhances your analysts' security monitoring capabilities and adds context to their investigations.

Splunk Enterprise Security includes a selection of threat intelligence sources. Splunk Enterprise Security also supports multiple types of threat intelligence so that you can add your own threat intelligence.

ES administrators can add threat intelligence to Splunk Enterprise Security by downloading a feed from the Internet, uploading a structured file, or inserting the threat intelligence directly from events in Splunk Enterprise Security.

Prerequisite

Review the types of threat intelligence that Splunk Enterprise Security supports. See Supported types of threat intelligence in Splunk Enterprise Security.

Steps

1. Configure the threat intelligence sources included with Splunk Enterprise Security.
2. For each additional threat intelligence source not already included with Splunk Enterprise Security, follow the procedure to add threat intelligence that matches the source and format of the intelligence that you want to add.
    - Upload a STIX or OpenIOC structured threat intelligence file
    - Upload a custom CSV file of threat intelligence
    - Add threat intelligence from Splunk events in Splunk Enterprise Security
    - Add and maintain threat intelligence locally in Splunk Enterprise Security
    - Add threat intelligence with a custom lookup file in Splunk Enterprise Security
    - Upload threat intelligence using REST API
3. Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

See also

Change existing threat intelligence in Splunk Enterprise Security

Add threat intelligence with an adaptive response action.

Threat Intelligence API reference in *REST API Reference*.

Threat Intelligence framework in Splunk ES on the Splunk developer portal