Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Add threat intelligence from Splunk events in Splunk Enterprise Security

Generated: 6/13/2022 9:46 am

Add threat intelligence from Splunk events in Splunk Enterprise Security

You can add threat intelligence from Splunk events to the local threat intelligence lookups.

1. Write a search that produces threat indicators.
2. Add `| outputlookup local_<threat intelligence type>_intel append=t` to the end of the search.

For example, write a search that produces a list of IP addresses that are testing a web server for vulnerabilities and add them to the `local_ip_intel` lookup to be processed by the modular input and added to the `ip_intel` KV Store collection.

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.