Configuring and optimizing Enterprise Security

Adding asset and identity data to Splunk Enterprise Security is a best practice and is required for effective use of Splunk Enterprise Security. This process will have been started for you by Professional Services if they did your installation and configuration.

You might feel that you do not have a good list of assets and identities. While this may be true, it is critical to start collecting and configuring this information so that the urgency of alerts are correctly evaluated and so you can get important context for investigations. This document contains guidance on how to collect and what add-ons can help with the process.

Threat Intelligence (TI) is another important asset for data enrichment that speeds up incident response. TI is information that has been collected, analyzed and evaluated for reliability by people with deep security expertise. It contains information that helps consumers of the TI to conduct faster incident investigations and response. The TI is packaged for easy integration with security analytics tools such as Splunk Enterprise Security, and with orchestration tools such as SOAR.

Splunk has a Threat Intelligence Platform (TIP) that helps with the acquisition of TI from Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs). The TIP also allows the creation and sharing of site-specific TI to be shared back and participate in the intelligence cycle. Splunk’s TIP can be integrated with ES by using the TruStar Unified App for Splunk Enterprise and Enterprise Security.

While there are many items in Splunk Enterprise Security that can and should be configured and adjusted, here are some common configuration and tuning tasks.

Configure users and roles

Splunk Enterprise Security adds three roles to the default roles provided by Splunk platform. The new roles allow a Splunk administrator to assign access to specific functions in Splunk Enterprise Security based on a user’s access requirements. The Splunk platform administrator can assign groups of users to the roles that best fit the tasks the users will perform and manage in Splunk Enterprise Security.

Enrich data

Enriching data involves using assets, identities, and threat intelligence.

- Docs: Add asset and identity data to Splunk Enterprise Security
- Docs: Configure users and roles
- Docs: Add threat intelligence to Splunk Enterprise Security
- .Conf session: Integrating a threat intelligence platform
Configure correlation searches

A correlation search is a type of scheduled search that scans multiple data sources, which can then be used to detect suspicious events and patterns in your data. You can configure a correlation search to generate an adaptive response, such as creating a notable event when search results meet specific conditions. You can then investigate notable events using the Incident Review dashboard in Splunk Enterprise Security. It is in this dashboard where the conditions discovered by the search are presented. The urgency of the event and other contextual information are also shown so you can determine next steps as quickly as possible.

Correlation searches are often synonymous with use cases. Security-focused use cases often involve searching for an indicator of compromise, and when found, raising it as an event for investigation or remediation. Many repetitive tasks involved in investigation and remediation should be automated with a SOAR product like Splunk SOAR.

To configure a correlation search:

1. Access the Configure drop-down menu from the app.
2. Select Content Management, and set the type to Correlation Search.
3. You can then enable and disable searches, update the settings that dictate how they run, change the search logic, and throttle their adaptive response actions. This configuration page is where much tuning and development will take place.

Noting what to search, filter or adjust is as varied as cyber security is itself. If you need direct help, use On Demand Services early and often to access experts available on request. You can also access a catalog of some of the services available to you.

It is best to enable correlation searches one at a time, understand how that search works, and validate it provides valuable information - not just noise. Enabling too many searches at once risks your SOC being flooded with alerts which may be hard to fix. It's best to start small, as the speed of enablement, validation and tuning will get faster with practice. No SIEM is a set and forget endeavor - it requires a practice of continuous improvement, because the nature of security is itself dynamic.

The beauty of Splunk Enterprise Security is that it is so expressive in its ability to be improved and pivot in different directions as an investigation or hunt unfolds. This does make your learning curve steeper, but is well worth the effort because once you have a working knowledge of how to use Splunk, your ability to detect, respond and act on security incidents will be robust and fast.
Getting data in is a big topic. If you'd like to go deeper, here is some more useful content to read:

- Docs: Correlation search overview for Splunk ES
- Docs: Configure correlation searches in Splunk ES
- Blog: Upping the auditing game for correlation searches within Enterprise Security — Part 1: The basics
- .Conf Session: On the fence about Enterprise Security? Can it add value to your SOC/company?