Getting data into ES

One of the fundamentals of using Splunk Enterprise Security is to have all your security data sent into a Splunk deployment to be indexed. Once it's there, you can correlate events from disparate data sources across time, and identify complex behavior that could be malicious. Correlation is facilitated by the Splunk Common Information Model (CIM) which normalizes field names needed for correlation. It also puts the data into data models that accelerate searches. Because of this, Splunk Enterprise Security requires that all data sources comply with CIM.

The document Data source planning for Splunk Enterprise Security has detailed configuration information for add-ons and other data input components.

The terms "Add-on" and "TA" are often used interchangeably. The term "App" has a different meaning that implies that it has views on dashboards, all of which are available on Splunkbase.

You can easily download the TAs needed to send data into a Splunk deployment to drive your use cases. Common examples include: The Splunk Add-on for Microsoft Windows, Palo Alto Networks Add-on for Splunk, Splunk Add-on for Check Point Log Exporter and many others that support security products from Cisco, McAfee, CrowdStrike, Z-Scaler, and many others. There are currently over 1400 security-related apps and add-ons on Splunkbase.

The use of the TAs provides you with CIM-compliant data going into a Splunk deployment. In the event you need to validate or troubleshoot, see the manual for the CIM add-on. This add-on is normally in place as part of the Splunk Enterprise Security installation.

Syslog is a technology frequently employed, and considered a best practice, when collecting data from security devices such as firewalls and security appliances. You can set up a syslog server to collect data from its sources, and then forward it from the syslog server to a Splunk deployment. Further considerations with syslog are documented in the Splunk validated architecture whitepaper.

Here are more resources that can help you to get data in:

- Docs: Getting data in to Splunk Cloud
- Docs: Getting data in to Splunk Enterprise
- Docs: Data source planning for ES
- Docs: Use apps to get data in
- Docs: Use CIM to validate your data
- Tech Talk: Splunk Connect for Syslog: Ingest security data
- .Conf session: Data onboarding: Where do I begin?
- .Conf session: Taming GDI: The wild world of ‘Getting Data Into’ Splunk