Getting started with ES

This guide is designed to help you get started with Splunk Enterprise Security or to make improvements on your configuration to ensure you receive maximum value from the platform.

1. Start sending your security-related data to Splunk using Common Information Model (CIM) compatible Technology Add-ons (TAs).
2. Use Splunkbase for add-ons to get data in.
3. Validate data using the Common Information Model validation app.
4. Start to configure assets and identities.
5. Enable notable events to drive the use case (start with 2-3 high-impact use cases and get them understood and tuned).

This Splunk Enterprise Security app is highly configurable, which helps you be effective in the fast-changing domain of Cyber Security. Because of that, it is highly recommended that installation and initial configuration is handled by Professional Services. If you are a cloud customer the installation is automated, but Professional Services are still recommended to assist with the configuration, including getting data in.