Section Introduction, Splunk

This section of the SIEM domain will cover how analysts use SIEM platforms to identify and respond to security events, and how security events are analyzed and responded to.

After general setup, configuring rules and alerts is key to being efficient with your SIEM. As a security practitioner, you'll need to constantly refine your SIEM to provide you with the important security events happening on your network. A common problem with SIEM tools is that they produce too many un-prioritized alerts, more than the security team can take the time to investigate. That's why it's important to continuously tune new and existing rules to effectively find only the relevant threat actions.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Setup your own local version of Splunk SIEM using Boss of the SOC v3 dataset.
- Learn how security analysts analyze and investigate security events within Splunk.
- Practically analyze and investigate a number of simulated security events.