splunk> turn data into doing

Enterprise Security Hands-On
Workshop

Overview

Enterprise Security Hands-On is a modular, hands-on workshop designed to familiarize participants with how to investigate incidents using Splunk Enterprise and Splunk Enterprise Security. This workshop provides users an opportunity to walk through multiple scenarios and see first-hand how Enterprise Security can be used from the creation of a notable event to investigate all the way to the raw event that identifies the adversary's action. The workshop leverages the popular Boss of the SOC (BOTS) dataset and is laid out in an interactive format. Users will leave with a better understanding of how Splunk and Enterprise Security can be used to generate notable events and investigate them as they occur in the enterprise.

Enterprise Security Hands-On

This workshop is led by SEs, Security SMEs.and Specialists to expose you to three real-world scenarios that an analyst might face during the day. This workshop walks users through these incidents from notable event all the way to accessing the raw logs, all in a single pane of glass.

The workshop agenda is approximately 3-4 hours and includes:

- **A brief overview of Enterprise Security (previous knowledge of Splunk ES is expected)**
- **Perform investigations and response in Enterprise Security**
  - **Enterprise Security Frameworks**
  - **SA Investigator**
  - **RBA (Risk Based Alerting)**
- **Detection Content, Coverage, & Validation**
  - **Splunk Security Content (SURGe, ESCU, SSE)**
  - **MITRE ATT&CK coverage**

Workshop Data

The workshop data is sourced from the BOTS v5 2019 data set, focusing on network and host data including:

- PaloAlto Networks NGFW
- Splunk for Stream (wire data)
- Windows Event Logs
- Microsoft Sysmon

Customers Who Will Benefit

The workshop is designed for personas with Splunk experience on a Security Operations team responsible for security monitoring and incident response. The workshop has three goals:

1. Understand the kinds of notable events that Enterprise Security can provide
2. Learn more about how the power the analyst has to drill deeper into the underlying events that triggered these events
3. Demonstrate how Splunk Enterprise Security can provide analysts with access to all of their security data in a single interface to answer questions generally asked of the SOC.

Benefits

- **Expert guidance from Splunk security subject matter experts**: Learn from Splunkers who have years of experience, not only in Splunk but also in security.
- **Real World Data:** Based on attack scenarios from Splunk's Boss of the SOC, the data collected showcases common security attacks that you may encounter on a daily basis.
- **Hands-on Time:** Participants will interact with Splunk and the data set to gain a better understanding on how to investigate using Splunk Enterprise Security.

Workshop Logistics

This workshop is hands-on, and each user will need access to a modern web browser with internet connectivity. Splunk will provide a cloud environment where the Splunk software and data will reside.

Splunk Security Specialists

We are here to help customers get the most out of their Splunk deployments. Our services are backed by Splunk experts who provide consistent and quality service delivery, architecture guidance, training, and ongoing support.

Take your Splunk environment to the next level and achieve continual optimization, enhanced processes, and active collaboration. If you are interested in learning more about our workshops as well as BOTS, please contact your Splunk Sales Representative.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.