splunk> turn data into doing

Splunk Attack Analyzer
Workshop

Overview

Tired of working across multiple tools and data sources to formulate threat analysis insights? Get hands-on with the Splunk Attack Analyzer workshop to see firsthand how quick and easy it is to gain consistent, high-quality, streamlined analysis of malware and credential phishing threats with Splunk® Attack Analyzer. Participants will walk through the Splunk Attack Analyzer UI and job analysis results, review the integration with Splunk® SOAR and utilize the out-of-the-box playbooks for phishing investigation and response.

Splunk Attack Analyzer

This workshop is led by SEs, Security SMEs, CSMs and Specialists to expose customers and prospects on how to utilize Splunk Attack Analyzer and Splunk SOAR to introduce how they can integrate to provide fully automated threat analysis.

The workshop agenda is approximately 2 hours and includes:

- **Overview of the Splunk Attack Analyzer platform**
  - **Hands-on exercises using the UI**
- **Overview of the Splunk App for Splunk Attack Analyzer**
  - **Hands-on exercise to review the data and app**
- **Introduction to SOAR Integration and OOTB Content**
  - **Hands-on exercise to explore and use the content**

Customers Who Will Benefit

The workshop is designed for personas on a Security Operations team that are responsible for content creation, specifically correlation searches. The workshop has three goals:

1. Develop a greater understanding of the integrations that exist between Splunk Attack Analyzer and Splunk security products.
2. Demonstrate the ability to automate the phishing response process with content that already exists.
3. Provide a series of exercises that allow users to see first hand how the products work together.

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 seen in the threat landscape, the data collected showcases common security attacks that you may encounter on a daily basis.
- **Hands-on Time:** Participants will have time during the workshop to interact with Splunk and the data set to gain a better understanding on how to answer security questions using Splunk.

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.