splunk> turn data into doing

Building Correlation Searches with Splunk Enterprise Security

Overview

Building Correlation Searches with Splunk Enterprise Security is a modular, hands-on workshop designed to familiarize participants with how to leverage Splunk to develop their own correlation searches. This workshop provides users a way to gain familiarity with building correlation searches in Splunk, as well as introducing data models and the tstats command that can provide a user a method to further optimize their correlation searches. The workshop leverages the popular Boss of the SOC (BOTS) dataset with hands-on exercises that build on one another. Users will come away with a better understanding of how to build their own correlation searches in Splunk as well as how to customize their associated notable events to provide more immediate insights to their analysts.

Building Correlation Searches

This workshop is led by SEs, Security SMEs, CSMs and Specialists to expose customers and prospects on how to build correlation searches in Splunk Enterprise Security as well as introduce how their associated notable events can be customized to help analysts gain further insight into their security event data.

The workshop agenda is approximately 8 hours and includes:

- **Common Information Model and Data Models**
- **tstats command**
- **Building a Correlation Search**
- **Configuring Notable Events**
- **Customizing Notable Events for Greater Context**
- **Exercises throughout the workshop providing opportunities to write your correlation searches!**

Workshop Data

The workshop data is sourced from the BOTS v4 2019 data set, focusing on network and host data including:

- Zeek
- Fortinet NGFW
- Splunk for Stream (wire data)
- Windows Event Logs
- Microsoft Sysmon
- Microsoft Cloud Services

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 data models and accelerated searches in Splunk
2. Demonstrate the ability to extend and customize correlation searches and their associated notable events to place more context in front of the analyst.
3. Provide a series of exercises that allow users to create a variety of correlation searches that can be utilized within their environment.

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 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.

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.