splunk> turn data into doing

Investigating with Splunk
Workshop

Overview

Investigating with Splunk is a modular, hands-on workshop designed to familiarize participants with how to investigate incidents using Splunk and open source. This workshop provides users a way to gain experience searching in Splunk to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations. The workshop leverages the popular Boss of the SOC (BOTS) dataset in a question and answer format. Users will leave with a better understanding of how Splunk can be used to investigate in their enterprise.

Investigating with Splunk

This workshop is led by SEs, Security SMEs, CSMs and Specialists to expose you to real-world scenarios that an analyst might encounter on a daily basis. This workshop presents questions that would be asked as an investigation unfolds and users will use Splunk to answer those questions.

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

- **An investigation primer**
- **Advanced Persistent Threat scenario**
- **Ransomware Scenario**

Workshop Data

The workshop data is sourced from the BOTS v1 2016 data set, focusing on network and host data including:

- Suricata
- Fortinet NGFW
- Splunk for Stream (wire data)
- Windows Event Logs
- Microsoft Sysmon

Customers Who Will Benefit

The workshop is designed for all personas on a Security Operations teams responsible for security monitoring and incident response. The workshop has three goals:

1. Understand the types of questions that need to be asked during an investigation
2. Identify the data required to find the answer to these questions in Splunk
3. Develop searches in Splunk that provide answers to the questions in order to advance your investigation

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.