splunk> turn data into doing

Advanced APT Hunting
Workshop

Overview

Advanced APT Hunting with Splunk is a modular, hands-on workshop designed to provide a deeper dive into an Advanced Persistent Threat while providing an opportunity for participants to develop hypotheses and hunt. This workshop leverages Splunk and Enterprise Security and introduces how models like the Lockheed Martin Kill Chain, MITRE ATT&CK and Diamond Model can be used to contextualize their hunts. The workshop leverages the popular Boss of the SOC (BOTS) dataset in a multi-hunt format. Users will leave with a better understanding of how Splunk can be used to hunt for threats within their enterprise.

Advanced APT Hunting

This workshop is led by Security SMEs to expose you to an APT hunt based on Splunk's BOTSv5 data set. This real-world scenario will provide you an opportunity to go deeper into adversary actions as well as give participants the chance to hunt for indicators of compromise by focusing on developing hypotheses and then hunting to confirm the hypothesis. This workshop contains a series of pivots from the intial hypothesis to allow threat hunters to go deeper into the data and uncover additional activity occurring to develop a more complete picture of the attack as well as learn how Splunk can help achieve this.

The workshop in total is approximately six hours, but can be delivered in a modular manner and includes:

- **Hunting basics**
- **Models to leverage as you hunt**
- **Contextualizing your hunt using asset and identity information**
- **Threat Hunts across our BOTS v5 APT Scenario**

Workshop Data

The workshop data is sourced from the BOTS v5 2020 data set, focusing on network and host data including:

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

Customers Who Will Benefit

The workshop is designed for personas on a Security Operations teams responsible for threat hunting and incident response. The workshop has four goals:

1. Understand why threat hunting is needed within organizations
2. Develop hypotheses to guide your hunt
3. Identify the data that is needed to confirm your hypotheses is in Splunk
4. Create searches and pivot in Splunk to confirm your hypotheses during your hunts

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 hunt 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 Strategists

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.

splunk>