Splunk SOAR Hands-On
Workshop

Overview

The Splunk SOAR Hands-On workshop is designed to familiarize participants with how to respond to incidents, manage cases and artifacts, as well as automate their incident response and standard operating procedures.

This workshop provides users with an opportunity to walk through a real-world scenario and see first-hand how Splunk SOAR can be used from the creation of a notable event to enriching alerts by automatically gathering data, all the way to managing and resolving the incident.

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 SOAR can be used to decrease the amount of time needed to triage and respond to alerts and they will also build their own basic investigative playbook.

SOAR Hands-On

This workshop is led by Splunk SEs and Security SMEs and is designed to give participants hands on experience in using SOAR for investigation and triage of a realistic security incident. This workshop walks participants through the basic use of automation through to creation of advanced playbooks to streamline the investigation process.

Workshop Agenda

The workshop agenda is approximately 4 hours and includes:

- **A brief overview of SOAR**
- **SOAR Apps & Assets**
- **Incident investigation and automation with actions**
- **Workbooks (Case Templates) and Case Management**
- **Playbook development for automation of investigation and response**
- **Automation and orchestration best practices**

SOAR Apps

During this workshop we will be integrating with various 3rd party technologies including:

- VirusTotal
- MaxMind
- BlueCoat Proxy
- ThreatMiner
- Whois

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. Provide an introduction to the SOAR platform and its capabilities.
2. Learn how to use the powerful playbook editor by developing and testing your own automation playbooks.
3. Demonstrate how SOAR can be used as your central Incident Management platform: handle cases, reference indicators, add notes, resolve incidents, collaborate and more.

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 and assets used:** Based on attack scenarios from Splunk's Boss of the SOC, the data used includes common security attacks that you may encounter on a daily basis. You will use services like Virus Total and ThreatMiner to investigate, triage and enrich this data and associated security incidents.
- **Hands-on Time:** Participants will interact with Splunk SOAR and the data set to gain a better understanding on how to investigate and automate using Splunk SOAR.

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.