splunk> turn data into doing

User Behavior Analytics (UBA) Hands-On Workshop

Overview

UBA Hands-On is a modular, hands-on workshop designed to familiarize participants with how to investigate threats and hunt anomalies using Splunk UBA. This workshop provides users an opportunity to walk through multiple scenarios and see how UBA can be used to dig deeper into threats identified by UBA as well as uncover additional indicators by pivoting through anomalies uncovered by UBA's machine learning models. 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 Splunk UBA can be used to investigate previously unknown threats and anomalies as they occur in the enterprise.

User Behavior Analytics Hands-On

This workshop is led by SEs, Security SMEs, CSMs and Specialists to expose customers and prospects how UBA can be used to investigate threats and hunt against anomalies by using hands-on exercises to investigate an pivot between apps, users, network addresses and other associated metadata found using machine learning.

The workshop agenda is approximately 2 hours and includes:

- **A brief overview of UBA**
- **Threat Detection with UBA**
- **Hunting in Anomalies in UBA**
- **Exercises throughout the workshop to investigate in UBA**

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

1. Understand how UBA can be used to uncover previously unknown threats and anomalies

2. Learn how threats detected by UBA can be investigated to broaden an investigation.

3. Demonstrate how anomalies created by UBA can be used to hunt for additional suspicious indicators that can extend your hunt further.

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.

splunk> BOSS of the SOC

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.

splunk>