splunk> turn data into doing

Insider Threat
Workshop

Overview

Insider Threat Detection with Splunk is a modular, hands-on workshop designed to provide a deeper dive into Insider Threats exposing participants to data sources and techniques that can be used to detect insider threat behavior. This workshop leverages Splunk Enterprise and introduces participants to indicators of Insider Threat and methods to detect them. This is the second Insider Threat workshop and introduces new and different data from the first. The workshop leverages the popular Boss of the SOC (BOTS) dataset with stand alone exercises. Users will leave with a better understanding of how Splunk can be used to hunt for insider threats within their enterprise.

Insider Threat

This workshop is led by Security SMEs to expose you to a deep dive into the Fraud and Insider Threat scenario in BOTSv6. This real-world scenario will provide an opportunity to go deeper into a number of data sources that can be utilized to identify insider activities while providing participants the opportunity to investigate based on indicators that are uncovered. The workshop is designed to expose users to different data sources that could be used to identify improper activity by insiders. These results can be anayzed in order to determine who may be an insider of interest and learn how Splunk can be used to operationalize these detections.

The workshop in total is approximately 4 hours, but can be delivered in a modular manner and includes:

- **Insider Threat background and challenges**
- **Insider threat program development**
- **Data sources to leverage**
- **Five insider threat scenarios using different data sources for a total of ten hands-on exercises using data sources like Salesforce and Check Point**

Workshop Data

The workshop data is sourced from the BOTS v6 2021 data set, focusing on insider threat data:

- Physical Security Badge data
- Customer Relationship Management
- Remote Access
- Endpoint
- Email

Customers Who Will Benefit

The workshop is designed for personas on Security Operations teams responsible for insider threats. The workshop has four goals:

1. Understand insider threat indicators
2. Understand why monitoring insider activities is needed within organizations
3. Use common data sources to identify insider threats
4. Provide ideas that can be used to develop and enhance insider threat investigation techniques and programs

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 scenarios from Splunk's Boss of the SOC, the data collected showcases common insider threat scenarios 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.

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.