splunk> turn data into doing

PEAK Threat Hunting – Hands On
Workshop

Overview

Join us for an interactive workshop introducing SURGe's PEAK Threat Hunting Framework. This hands-on session will explore the framework and offer deep-dive instruction into each of the three hunt types (Hypothesis-Driven, Baseline, and Model-Assisted Threat Hunting). Attendees will perform actual threat hunts on realistic data, as well as engage with examples and demos drawn from real-life hunting scenarios. Whether you're looking to refine your threat hunting skills or integrate advanced methodologies into your team's arsenal, this workshop is an essential step forward.

PEAK Threat Hunting – Hands On

This workshop is led by SEs, Security SMEs, CSMs, and Specialists to expose customers and prospects to SURGe's PEAK Threat Hunting Framework. It will provide an overview of the entire framework, but the majority of the session will focus on practical threat hunting examples which the participants will perform against realistic data.

The workshop agenda is approximately 6 hours and includes:

- **PEAK framework overview**
- **Hypothesis-Driven Threat Hunting**
- **Baseline Threat Hunting**
- **Model-Assisted Threat Hunting (M-ATH) with Machine Learning and Data Science techniques**
- **Hands-on exercises and demos to reinforce the techniques with real-world hunting examples**

Workshop Data

The workshop data is sourced from the BOTS v4 2019 data set, focusing on network and host data, including:

- Windows process execution logs (Sysmon event code 1)
- Network flow data from Splunk Stream
- DNS domain data from query logs/passive DNS sources

Customers Who Will Benefit

The workshop is designed for members of Security Operations or Threat Hunting teams who are responsible for conducting threat hunting operations full- or part-time. The workshop has three goals:

1. Give the participants a working understanding of the PEAK framework and its application in real-world threat hunting scenarios
2. Learn how to perform each of the three types of threat hunts (Hypothesis-Driven, Baseline, and Model-Assisted).
3. Provide practical example hunts that the participants can adapt and apply to their own environments.

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 of 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 or 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.