splunk> turn data into doing

# AWS Hands-On Workshop

## Overview

This workshop is designed to extend your knowledge into the AWS suite of solutions beyond EC2 and S3. During the workshop, hands-on investigations leveraging CloudTrail and CloudWatch data, as well as VPC Flow data, are provided. Data sets created by AWS security solutions, like GuardDuty and Security Hub, will be introduced as well. The workshop concludes with detections from ESCU and SSE to highlight the integration of AWS data sources into Enterprise Security. The workshop leverages the Boss of the SOC (BOTS) dataset with hands-on exercises throughout. Users will come away with a better understanding of the logging available to them from AWS and which events are important to collect to gain visibility into adversary actions in the environment.

## AWS2 Hands-On

This workshop is led by SEs, Security SMEs, CSMs and Specialists to expose customers and prospects on how to use AWS data to respond to security incidents and troubleshoot issues in an AWS environment.

The workshop agenda is approximately 4 hours and includes:

- **Introduction to AWS Shared Responsibility model**
- **Incident Response with VPC Flow logs**
- **Introduction to Security Hub and GuardDuty**
- **Adversary studies with CloudTrail**
- **Exercises throughout the workshop providing opportunities to investigate and learn AWS data sources**

### Workshop Data

The workshop data is sourced from the BOTS v5 data set, focusing on AWS telemetry including:

- CloudTrail
- CloudWatch
- Security Hub
- GuardDuty
- VPC Flow logs
- S3 Log Access
- AWS Config

### Customers Who Will Benefit

The workshop is designed for personas on a Security Operations team that are responsible for monitoring and securing their own AWS environments. The workshop has three goals:

1. Develop a greater understanding of AWS data in Splunk.
2. Demonstrate the ability to investigate incidents that have occurred in AWS using Splunk Enterprise, Splunk Enterprise Security, and Splunk Security Essentials.
3. Provide a series of exercises that allow users to practice incident investigation with AWS data in a safe environment.

## 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.

## 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.

splunk>