SEC541: **Cloud Security Monitoring and Threat Detection**

1 Day Course	6 CPEs	Laptop Required

You Will Be Able To

- Understand the threats against AWS cloud infrastructure
- Deep dive into AWS core logging services.
- Research, detect, and investigate threats
- Incorporate scripting and automation to make threat hunters more efficient
- Understand how good architecture improves threat hunting

Who Should Attend

- Security analysts
- Security architects
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- System administrators
- Cloud administrators

Exercises

- Identify Cloud Service Discovery Attacks with CloudTrail
- Identify Brute Force Attacks with VPC Flow Logs
- Identify Web App Attacks through CloudWatch Logs
- Leverage GuardDuty as a Threat Detection Service

Topics

- Analyzing the AWS management plane with CloudTrail
- Collecting network traffic
- Analyzing custom logging through CloudWatch
- Leveraging GuardDuty
- Investigate Security Hub

Attackers can run but not hide. Our radar sees all threats.

Cloud infrastructure provides organizations with new and exciting services to better meet the demands of their customers. However, these services bring with them new challenges, particularly the need to effectively hunt down and identify threats attacking your infrastructure. Securely operating cloud infrastructure requires new tools and approaches.

This course is a deep dive into the native services available within Amazon Web Services (AWS) to gather, analyze, and detect threats. You will learn about common attack techniques used against cloud infrastructure, and then investigate how to detect those threats in AWS. SEC541 is all about gaining the hands-on experience that gives you the skills and confidence to seek out threats in your own environment. We'll also discuss architectural design patterns that can make detection easier and attacks harder, as well as ways to automate tasks wherever possible.

Lab Information

These labs in this courseare hands-on, deep dives into the AWS service. Each lab will start by researching a particular threat, and the data needed to detect it. Then, the student will use native services within AWS to extract, transform, and analyze the threat. The course lecture coupled with the labs will give students a full picture of how those services within AWS services work, the data they produces, and common ways to analyze those data.

Do not expect to spend the labs clicking on screens. The labs are focused almost entirely on using the AWS command line interface (CLI), which is the best way to really understand the native services within AWS. The use of the CLI will also facilitate scripting and automation.

Author Statement

"Cloud service providers are giving us new tools faster than we can learn how to use them. As with any new and complex tool, when need to get past the surface level "how-to" in order to radically reshape our infrastructure. This course is a deep dive into elements of AWS that we may have used before but and are ready to truly explore. At the end of the class, you can be confident in knowing you will be able to start looking for the threats, and can start building a true Threat Hunting program in AWS."

—Shaun McCullough