SEC541: Cloud Security Monitoring and Threat Detection

3 Day Course	18 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

Authors' 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, we need to get past the surface-level 1how-to in order to radically reshape our infrastructure. This course is an overview of the elements of AWS and Azure that we may have used before but are ready to truly explore. By the end of the class, you ll be confident knowing that you have the skills to start looking for the threats and building a true threat detection program in AWS and Azure."

—Shaun McCullough and Ryan Nicholson

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.

In SEC541, we start by walking through a real world attack campaign against a cloud infrastructure. We will break down how it happened, what made it successful, and what could have been done to catch them in the act. We spend the day dissecting the attacks, learning how to leverage cloud native and cloud integrated capabilities to detect, hunt, or investigate similar attacks in a real environment, and build our arsenol of analytics, detections and best practices for you to bring back to work on Monday.

Notice to Students

This course was formerly 1-Day. Additional content around AWS as well as Azure, and more labs have been added to this content.

Lab Information

The labs in this course are hands-on explorations into AWS logging and monitoring services. 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 work, the data they produce, and common ways to analyze those data.

Day 1 and 2 labs will center around your own infrastructure you will build in class, perform your own attacks, and gather those logs. Day 3, the class will open up to a larger shared AWS environment leverage managed security services.

Section Descriptions

SECTION 1: Management Plane and Network Logging

Section 1 will look at how attackers took over the infrastructure from the company CodeSpaces, and investigate how the AWS and Azure management plane and network logging can be used to detect similar techniques.

TOPICS: Debrief: Codespaces; Detecting T1526 with API Logging; Log Parsing with JQ; Detecting T1499, T1078.004 with Cloud-Native Logging Services; Detecting T1048.001 with Network Flow Logging

SECTION 2: Compute and Cloud Services Logging

Section 2 of the course will investigate how bitcoin miners snuck into Tesla s Kubernetes infrastructure, and will investigate ways to use cloud native services, application logs, managed container telemetry, and operating system logs to gather together data from across your organization to analyze for attack behavior.

TOPICS: Debrief Tesla Attack; Operating System Logs with Network Flow Logging; Application Logs; Log Agents; Container Logs; Cloud Services Logs

SECTION 3: Cloud Service and Data Discovery in AWS

In Section 3, we will investigate the Capital One attack, how the attacker gained access and extracted over 100 million customer s information, and investigate how AWS and Azure s inventory services, managed security products, and active vulnerability services can be leveraged to identify potential vulnerabilities and threats in your cloud infrastructure.

TOPICS: Debrief: Capital One; Detecting T1530 with Cloud Inventory; Detecting T1105 with Data Discovery; Detecting T1190 with Vulnerability Analysis Services; Data Centralization