SEC541: **Cloud Security Threat Detection**

GCTD
Cloud Threat Detection
giac.org/gctd

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Understand how identities can be abused in cloud environments
- Monitor threat actors using cloud-native logging tools
- Define and understand compute resources such as virtual machines (VMs) and containers
- Detect and address attacker pivots within your cloud infrastructure
- Implement effective detection strategies using cloud provider tools
- Investigate and analyze instances in your compute resources for suspicious activities
- Perform detailed analysis and detection of threats in Microsoft 365 and Azure environments
- Pivot between different log sources to uncover the full narrative of an attack
- Build automation workflows to reduce repetitive security tasks
- Centralize and normalize data from various sources to enhance analysis and threat detection

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.

It's undeniable that cloud environments offer unparalleled benefits, however, poorly trained personnel can expose your organization to an ever-expanding list of dynamic threats. SEC541: Cloud Security Threat Detection is designed to address these challenges by equipping professionals with the skills to identify, detect, and respond to threats in cloud infrastructures. This comprehensive course delves into cloud-native logging, threat models, intrusion detection, and continuous monitoring, ensuring that your organization can maintain a robust security posture in AWS, Azure, and Microsoft 365 environments.

SEC541 immerses students in real-world scenarios, teaching them to navigate cloud-specific logs, build effective threat detection systems, and understand the unique aspects of cloud architecture. By mastering these skills, your team can significantly reduce detection and response times, enhance visibility into the cloud threat landscape, and effectively defend against sophisticated attacks.

SEC541 boosts the proficiency of cloud security analysts and empowers teams to operate more efficiently and effectively, maximizing your organization's security capabilities. Equip your workforce with the latest knowledge in cloud security threat detection and ensure your organization is prepared to tackle the complexities of modern cloud security challenges.

Business Takeaways

- **Reduce Detection and Response Time—**Quickly identify and respond to critical cloud threats.
- **Enhance Visibility—**Gain comprehensive insights into your cloud environment.
- **Improve Security Posture—**Implement effective cloud-specific threat detection strategies.
- **Proactive Threat Management—**Address threats early, aiding in swift incident resolution.
- **Efficiency and Automation—**Increase efficiency with automated detection and response workflows.
- **Cost Savings—**Avoid financial fallout by proactively securing your cloud environment.
- **Upskill Workforce—**Equip your team with the latest cloud security knowledge and techniques to defend against sophisticated cloud threats.

Hands-on Training

The hands-on portion of SEC541 is designed to provide students with practical, real-world experience in cloud security threat detection. Each student receives access to their own AWS and Azure accounts, where they can explore and interact with live cloud environments. The labs cover a wide range of topics, from analyzing cloud-native logs to detecting and responding to threats in AWS, Azure, and Microsoft 365. Students will perform attacks against their own accounts, generating the data needed for thorough analysis and investigation.

A key component of SEC541 is the 21 interactive labs, making up about 40% of the course time, split evenly between AWS and Azure environments. These labs are essential for applying the lecture's lessons by allowing students to practice and hone their skills in a controlled environment. By engaging in these hands-on activities, students gain a deeper understanding of cloud-specific threats and the tools and techniques needed to detect and respond to them effectively. This immersive approach ensures that participants leave the course with the confidence and capability to secure their own cloud environments.

Section Descriptions

SECTION 1: Management Plane and Network Attacks

SEC541 starts with detecting adversarial activity in your cloud environment through management plane and network logging and analysis.

TOPICS: Code Spaces Case Study; MITRE ATT&CK and Definitions; API Logging; Parsing JSON; Cloud-Native Logging Services; Network Flow Logging; Capturing Raw Network Traffic

SECTION 2: Compute and Application Attacks

In Section 2, we will dig deeper into your applications, serverless deployments and compute systems running within the cloud environment.

TOPICS: Telsa Case Study; Host Visibility; Application Component Logging; Managed Container Services; Operational logging Techniques; Identifying Data Exfiltration

SECTION 3: Security Services and Data Discovery

In Section 3, we will leverage cloud provider's security services to detect activity and investigate resources, identify data compromises, vulnerability systems, and pivot through many different telemetry types.

TOPICS: Capital One Case Study; Metadata Service and GuardDuty; Function Attack Surface; Investigating Resources; Investigating Data; Vulnerability Analysis Services; Artifical Intelligence (AI) in the Cloud; Tracking Across Logs

SECTION 4: Microsoft Ecosystem

In Section 4, we will deep dive into Azure's ecosystem and the unique threats that can occur.

TOPICS: Malware Bytes Case Study; Detection Services; Microsoft 365; Entra ID; Command and Control; Storage Monitoring; Network Enrichment and Analytics

SECTION 5: Data Shipping, Automation, and CloudWars

In Section 3, we will learn how to cross pull logs across multiple clouds, automate response actions, and put your new skills to the test in a Capture-the-Flag event.

TOPICS: Data Shipping, Enrichment and Export; Automating Detection and Response Actions; CloudWars

"I would recommend SEC541 to any cloud security stakeholder that wants to empower all the security tools companies have in order to improve detection, understand protection, and overall increase their security level."

—Veronique Dupont, Cloud Cyber Security Architect, **Airbus**

"Inputting the malicious commands makes the labs much more interesting. Learning what to look for from both sides of the keyboard in one course is refreshing."

—Scott H., **U.S. Government**

"I really like the labs and the fact that we play the attacks before watching the logs, that's pretty cool."

—Damien Glomon, **ANSSI**

Who Should Attend

- Cloud security analysts
- Threat detection engineers
- Security Operations Center (SOC) operators
- Security incident responders
- Cloud security architects
- Penetration testers
- SOC managers
- Blue Team members
- Forensic analysts
- Offensive security professionals looking to understand defensive techniques
- IT professionals transitioning to cloud security roles
- Anyone responsible for securing cloud environments in any industry

NICE Framework Work Roles

- Security Architect (OPM 652)
- Systems Security Analyst (OPM 461)
- Information Systems Security Manager (OPM 722)

GCTD

Cloud Threat Detection
giac.org/gctd

GIAC Cloud Threat Detection

The GIAC Cloud Threat Detection (GCTD) certification validates a practitioner's ability to detect and investigate suspicious activity in cloud infrastructure. GCTD-certified professionals are experienced in cyber threat intelligence, secure cloud configuration, and other practices needed to defend cloud solutions and services.

- Detecting attacks in the cloud
- Cloud investigations and cyber threat intelligence
- Assessments and automation in AWS and Azure