SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC541:™ Cloud Security Threat Detection™

GCTD
Cloud Threat Detection
giac.org/gctd

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Build a detection engineering program for cloud environments
- Analyze API and cloud-native logs to uncover attacker activity
- Hunt threats across services, containers, and Microsoft 365
- Detect persistence, privilege escalation, and lateral movement in cloud
- Apply threat intelligence and AI tooling to detection workflows
- Automate security response using native and open-source tools

Business Takeaways

- Reduce cloud breach detection and response time
- Implement scalable detection strategies for multicloud environments
- Improve visibility and alert fidelity across AWS, Azure, and M365
- Align threat detection to real attacker behavior using MITRE ATT&CK
- Leverage automation and AI to reduce workload and response lag
- Enhance team proficiency in cloud forensics and investigation

Expose the invisible. Detect what others miss.

Modern attackers exploit gaps in visibility across cloud platforms, moving laterally between services and abusing native tools to stay undetected. SEC541: Cloud Security Threat Detection™ equips defenders with the skills to detect, investigate, and respond to these advanced threats across AWS, Azure, and Microsoft 365.

Through hands-on labs and real-world case studies, students build a cloud-native detection engineering process and develop practical skills in API monitoring, log analysis, threat hunting, and automation. The course emphasizes actionable techniques—delivered through 22 labs and scenario-driven exercises—that students can immediately apply to improve detection capabilities in production environments.

This advanced course teaches security professionals how to detect cloud-native threats using real-world case studies, detection engineering strategies, and deep telemetry analysis. Students learn to build detections, investigate abuse of identity and services, apply threat intelligence, and automate response workflows using native tools across cloud providers.

Hands-on Training

SEC541™ delivers 22 hands-on labs designed to reflect real cloud-attack scenarios. Students get access to live AWS and Azure environments, where they execute attacks, analyze telemetry, and build detections using production-grade tools.

Labs include:

- Cloud-native detection labs using CloudTrail, CloudWatch, GuardDuty, Sentinel, Defender, and more
- Telemetry correlation exercises leveraging KQL, ElasticSearch, and multi-source log analysis
- AI-powered detection workflows using Azure AI Foundry and automation pipelines
- CloudWars simulation, a CTF-style challenge applying course skills to complex threat scenarios

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

sans.org/sec541

- Watch a preview of this course
- Discover how to take this course: Online, In-Person

Section Descriptions

SECTION 1: Detection of Cloud API and Network Attacks

Section 1 introduces detection engineering with a real-world case study. Students monitor cloud APIs, analyze VPC flow logs, and deploy decoy networks.

TOPICS: Attack Analysis Methodology; Cloud Management API; Detection Engineering; Network Traffic Analysis; Detection Strategy

SECTION 3: Security Services and Investigations

Section 3 focuses on cloud-native detection tools and telemetry fusion. It includes cross-account persistence, data classification, and vulnerability analysis.

TOPICS: Resource Inventory and Detection; Vulnerability Analysis; Correlate Logs, Data Exposure and Resource Activity; Cross-Account Role Persistence

SECTION 5: Data Shipping, Automation, and CloudWars

In Section 5, students automate forensics and incident response across cloud platforms, culminating in the CloudWars challenge—an applied capstone capture the flag (CTF).

TOPICS: Cloud IR; Forensic Workflows, Detection Engineering; Multi-Cloud Security; Threat Hunting; CTF

SECTION 2: Compute and Application Attacks

Section 2 covers compute workloads including containers and serverless. Students investigate the Tesla Kubernetes breach and detect ransomware, hijacking, and metadata abuse.

TOPICS: Host Visibility; Metadata; App Component, VM and Container Logging; Data Exfiltration

SECTION 4: Microsoft Ecosystem

Section 4 dives into Azure Sentinel, Defender, KQL, and M365 threat detection. Students simulate Exchange attacks and build AI-assisted detection workflows.

TOPICS: Microsoft Sentinel, M365 Attack Analysis, Defender XDR; Entra ID; KQL: Storage Monitoring; AI Tooling

"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, **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

Ideal for technical defenders and security leaders responsible for cloud detection, investigation, and response:

- Cloud security analysts
- SOC analysts and managers
- Detection engineers and forensic analysts
- Blue Team members and incident responders
- Cloud security architects and DevSecOps engineers
- Penetration testers seeking defensive perspective
- Government, critical infrastructure, and regulated industry security teams

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