SEC510: Cloud Security Engineering and Controls™

GPCS
Public Cloud Security
giac.org/gpcs

5	30	Laptop
Day Course	CPEs	Required

You Will Be Able To

- Make informed choices across AWS, Azure, and GCP with deep dives into PaaS and IaaS
- Leverage AI to effectively and enforce controls at scale
- Test and validate security controls instead of relying on vendor documentation
- Build layered IAM and integrate identity into network security
- Automate encryption and compliance checks
- Prevent, mitigate, and recover from ransomware
- Secure FaaS, multicloud, IaC deployments, and GenAI workloads

Business Takeaways

- Prevent incidents from becoming breaches with attack-driven, preventive controls—including defenses for emerging AI workloads
- Reduce the attack surface of your organization's cloud environments
- Control the confidentiality, integrity, and availability of data in the Big 3 CSPs
- Increase use of secure automation to keep up with the speed of today's business
- Resolve unintentional access to sensitive cloud assets
- Reduce the risk of ransomware impacting your organization's cloud data

Prevent real attacks with controls that matter.

Build the skills to engineer cloud security controls across AWS, Azure, and GCP. SEC510 prepares practitioners to secure multicloud environments, reduce attack surface, and apply practical defenses across identity, network, data, serverless, third-party integrations, and GenAI workloads.

Through hands-on labs and real-world cloud attack scenarios, students learn how to move beyond CSP defaults, validate controls in practice, and design guardrails that limit the impact of misconfigurations, vulnerable applications, and cloud service risks.

SEC510 also supports preparation for the GIAC Public Cloud Security (GPCS) certification.

What Are Cloud Security Controls?

Cloud security controls are techniques and settings provided by cloud service providers (CSPs) that help protect cloud-based assets from unauthorized access, data breaches, and other cyber threats. While each CSP offers default controls, those defaults are often too generic to account for an organization's specific risks, goals, and operating needs.

Effective cloud security requires tuning controls such as access restrictions, encryption, and network segmentation to real-world threats across each provider. In complex multicloud environments, these controls help reduce risk and protect sensitive data. AI can help manage that complexity, but only when guided by practitioners who understand multicloud engineering.

Hands-On Training

SEC510 reinforces the course concepts through hands-on labs in real cloud environments across AWS, Azure, and Google Cloud. Students use Terraform Infrastructure as Code to deploy and configure services, work through practical cloud security engineering tasks, and apply controls they can adapt for their own environments. In total, there are 52 hands-on labs, including AI techniques, with optional Agentic AI instruction paths that show how tools such as OpenAI Codex can help perform cloud security engineering tasks more efficiently.

"The course provided so much information and details about common security misconfigurations and mistakes in the cloud that one would not believe fit into the week. Very comprehensive, but the scary thing is that it feels like it is barely scratching the surface! Awesome job by the course authors."

—Petr Sidopulos

Section Descriptions

SECTION 1: Cloud Engineering and Identity Access Management (IAM)

SEC510 begins with cloud breach trends and the challenges of multicloud. Students explore IAM and machine identity risks, practice real-world attacks, and use tools like IAM analyzers to detect Broken Access Control. The section ends with strategies to prevent privilege escalation.

TOPICS:

- Introduction
- Cloud Identity and IAM
- Cloud Managed Identity and Metadata Services
- Broken Access Control and Policy Analysis
- IAM Privilege Escalation

SECTION 2: Private Networks, Endpoints, and Encryption

Section 2 focuses on networking and encryption controls. Students will learn to secure VMs, use private endpoints for PaaS, prevent Remote Code Execution (RCE) with data exfiltration, analyze flow logs to detect malicious activity, and manage cryptographic keys across all three major clouds.

TOPICS:

- Protect Public VMs
- Private Endpoint Security
- Private Endpoint Abuse
- Enabling Traffic Monitoring
- Cryptographic Key Management
- Encryption with Cloud Services

SECTION 3: Cloud Data Security and AI Controls

Section 3 focuses on cloud data security and AI controls. Students explore secure storage, ransomware defense, Vector Databases, leveraging Generative AI (GenAI)/Agentic AI to implement cloud security controls, and how to secure Retrieval Augmented Generation (RAG) infrastructure in the cloud.

TOPICS:

- Cloud Storage Platforms
- Signed URLs
- Vector Database
- AI-Driven Mitigations
- Securing Cloud AI Infrastructure

SECTION 4: Serverless Workloads and End-User Security

Section 4 covers securing cloud app infrastructure and users, starting with serverless FaaS benefits and risks. Students harden real serverless functions, explore Customer Identity and Access Management (CIAM) threats like account takeover via Amazon Cognito, and protect the most critical services in Google Cloud's Firebase platform.

TOPICS:

- Cloud Serverless Functions
- Cloud Customer Identity and Access Management
- Firebase Databases and Google Cloud Implications

SECTION 5: Multicloud, CSPM, and Third-Party Integrations

The final section covers multicloud operations, focusing on IAM risks, safe credential use, and Workload Identity Federation. Students automate security checks with CSPM tools, explore trust issues with third-party platforms, and study how to mitigate a real cloud security vendor vulnerability using Microsoft Defender as a case study.

TOPICS:

- Multicloud Access Management
- Workload Identity
- Cloud Security Posture Management
- Vendor Integrations
- Summary
- Additional Resources

"Yes, I would definitely recommend this course. I consider the security topics covered to be critical knowledge for companies that are hosting in the cloud. The course content has been very well put together, well researched, and is very applicable."

—Dan Van Wingerden, **Radiology Partners**

Who Should Attend

- Security analysts
- Security engineers
- Security researchers
- Cloud engineers
- DevOps engineers
- Security auditors
- System administrators
- Operations personnel
- Anyone who is responsible for:
  - Evaluating and adopting new cloud offerings
  - Researching new vulnerabilities and developments in cloud security
  - Handling identity and access management
  - Managing a cloud-based virtual network
  - Secure configuration management
  - Generative AI (GenAI) infrastructure

NICE Framework Work Roles

- Systems Security Analyst (OPM Code 461)
- Security Architect (SP-ARC-002)
- Secure Software Assessor (SP-DEV-002)
- Security Control Assessor (SP-RSK-002)
- Information Systems Security Developer (SP-SYS-001)

GPCS
Public Cloud Security
giac.org/gpcs

GIAC Public Cloud Security

The GIAC Public Cloud Security (GPCS) certification validates a practitioner's preparedness to secure the cloud in both public and multicloud environments. GPCS certification holders understand the nuances of AWS, Azure, and Google Cloud Platform, and are equipped to defend these platforms effectively.