SEC510: **Cloud Security Engineering and Controls™**

GPCS
Public Cloud Security
giac.org/gpcs

5 Day Course | 38 CPEs | Laptop Required

You Will Be Able To

- Make informed choices across AWS, Azure, and GCP with deep dives into PaaS and IaaS
- Learn from real-world attack case studies
- 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 GenAI 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

"Labs are amazing, they cover all the content we review over the lecture."

—Enrique Gamboa, **ALG**

Prevent real attacks with controls that matter.

Protecting multicloud environments is both tough and essential. Default controls often fall short, and what works in one CSP may fail in another. SEC510: Cloud Security Engineering and Controls™ delivers advanced training on building preventive, attack-driven defenses across AWS, Azure, and GCP. Students gain practical skills to secure modern environments from encryption and ransomware protection to defending GenAI workloads through controls that reduce risk and safeguard critical assets at scale.

SEC510 helps professionals move beyond compliance checklists and CSP defaults by teaching how to engineer guardrails that prevent misconfigurations and shrink the cloud attack surface. Instead of relying on vendor documentation, students test and validate how controls work in practice, uncovering incorrect or incomplete implementations across providers.

The course also explores how to mitigate flaws in applications and cloud services, including zero-day risks, by enforcing secure-by-design configurations. While frameworks such as MITRE ATT&CK, the CIS Cloud Provider Benchmarks, and the Cyber Defense Matrix provide useful guidance, SEC510 goes further, showing how to engineer defenses that protect what matters most.

"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

What Are Cloud Security Controls?

Cloud security controls are options provided by cloud service providers to limit exposure of cloud assets. Each CSP provides default controls that are often insecure, failing to consider the business case and needs of each customer. For secure cloud configuration that truly prevents real risk, the cloud security controls must be implemented based on business strategy, goals, and requirements by a professional who understands the nuances of various CSPs.

Hands-On Training

SEC510: Cloud Security Engineering and Controls training reinforces all the concepts discussed in the lectures through hands-on labs in real cloud environments. Each lab includes a step-by-step guide as well as a "no hints" option for students who want to test their skills without assistance. This allows students to choose the level of difficulty that is best for them and fall back to the step-by-step guide as needed. With 19+ Terraform-powered labs, students leave with reusable code, proven practices, and the confidence to secure multicloud environments at scale. This course also provides many *optional* bonus challenges. One module in these bonus challenges requires an Oracle Cloud Infrastructure (OCI) account. *This is not provided by SANS.*

Section Descriptions

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

SEC510 begins with cloud breach trends, showing why multicloud makes security harder and why standardization or agnosticism alone can't solve the problem. Students apply frameworks like MITRE ATT&CK, CIS Benchmarks, and the Cyber Defense Matrix while deploying a modern web app across AWS, Azure, and GCP. The section then builds a foundation in Identity and Access Management (IAM)—covering human and machine identities, access controls, and common risks like metadata exposure. Students explore Broken Access Control and privilege escalation, using native tools and guardrails to detect improper access, enforce least privilege, and prevent attackers from exploiting default permissions.

TOPICS: Introduction; Cloud Identity and IAM; Cloud Managed Identity and Metadata Services; Broken Access Control and Policy Analysis; IAM Privilege Escalation

SECTION 2: Cloud Private Networks and Endpoints

Section 2 covers how to lock down infrastructure within a virtual private network. As the public cloud IP address blocks are well known and default network security is often lax, millions of sensitive assets are unnecessarily accessible to the public Internet. This section will ensure that none of these assets belong to your organization. It begins by demonstrating how ingress and egress traffic can be restricted within each provider. The next module covers cloud-based network analysis capabilities to address malicious traffic on network channels that cannot be blocked. With our infrastructure locked down, we pivot to controlling network access to PaaS using Private Endpoints. This section concludes with techniques for securely granting organization members access to assets in private cloud networks. These techniques allow an organization to work effectively while keeping internal systems off the public internet.

TOPICS: Cloud Virtual Networks; Protecting Public Virtual Machines; Private Endpoint Security; Private Endpoint Abuse; Enabling Traffic Monitoring

SECTION 3: Cloud Data Security and GenAI Controls

Cloud data security is critical, with many breaches tied to weak or missing controls. This section examines encryption, secure storage, ransomware defense, access control, and data loss detection across AWS, Azure, and GCP.

Module 1: Encryption
Covers cryptographic key management and in-transit encryption, showing how providers implement layered protection for data at rest and in motion.

Module 2: Cloud Storage Security
Focuses on disabling public access, applying advanced controls like ransomware mitigation, file versioning, and retention, and detecting sensitive data exposure.

Second Half: GenAI Security
Explores how Generative AI can affect cloud security, teaching students to secure GenAI infrastructure by addressing RAG risks, common implementation flaws, and real-world case studies such as Azure's AI Foundry.

TOPICS: Cryptographic Key Management; Encryption with Cloud Services; Cloud Storage Platforms; Signed URLs; GenAI-Driven Mitigations; Securing Cloud GenAI Infrastructure

SECTION 4: Serverless Workloads and End-User Security

This section teaches students how to secure the infrastructure powering their cloud-based applications and how to protect the users of those applications. It begins with App Services, platforms that simplify the process of running and scaling cloud applications. This leads into a computing paradigm taking the industry by storm: serverless Functions as a-Service (FaaS). The next module covers how Customer Identity and Access Management (CIAM) can help track and authenticate the users of an organization's applications. The Google Cloud Platform obtained their CIAM services through their acquisition of a company named Firebase. The section concludes with a detailed breakdown of this CIAM and its interplay with Firebase's flagship product, the Realtime Database. This highly popular but rarely reviewed service is a serverless database with many access control considerations and security implications for Google Cloud projects.

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 course concludes with practical guidance on how to securely operate across multiple cloud providers. Students first examine how multicloud integration impacts Identity and Access Management (IAM), including the risks of long-lived credentials that attackers value far more than short-lived ones. They then explore Workload Identity Federation as a safer way to authenticate between clouds and to integrate with third-party Cloud Security Posture Management (CSPM) services. Finally, students learn how third-party integrations, including CSPMs, can introduce new risks. Using Microsoft Defender for Cloud as a case study, they analyze a critical vulnerability that exposed linked AWS accounts and implement mitigations to minimize vendor trust and prevent similar exploits.

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 GPCS certification validates a practitioner's ability to secure the cloud in both public cloud and multi cloud environments. GPCS-certified professionals are familiar with the nuances of AWS, Azure, and GCP and have the skills needed to defend each of these platforms.

- Evaluation and comparison of public cloud service providers
- Auditing, hardening, and securing public cloud environments
- Introduction to multi-cloud compliance and integration