SEC510: Cloud Security Controls and Mitigations

GPCS Public Cloud Security
giac.org/gpcs

5 Day Course	38 CPEs	Laptop Required

You Will Be Able To

- Make informed decisions in the Big 3 cloud service providers by understanding the inner workings of each of their Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings
- Implement secure Identity and Access Management (IAM) with multiple layers of defense-in-depth
- Build and secure multi cloud networks with segmentation and access control
- Encrypt data at rest and in-transit throughout each cloud
- Control the confidentiality, integrity, and availability of data in each cloud storage service
- Support non-traditional computing platforms like Application Services and serverless Functions as a Service (FaaS)
- Integrate each cloud provider with one another without the use of long-lived credentials
- Automate security and compliance checks using cloud-native platforms
- Guide engineering teams in enforcing security controls using Terraform and Infrastructure-as-Code (IaC)

Business Takeaways

- Reduce the attack surface of your organization's cloud environments
- Prevent incidents from becoming breaches through defense in-depth
- 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 environment
- Resolve all unintentional access to business 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 hard. Default controls are insecure more often than not. A security control that works in one of the Big 3 CSPs may not work the same in another. Many cloud security controls are focused on compliance rather being derived from real attack case studies. Attack-driven controls are necessary to protect an organization's most important cloud-based assets.

Accepting the inevitability of application flaws, whether the application is developed in-house or by a third-party, is fundamental for successful cloud security controls. Not many cybersecurity professionals can fix vulnerable application code. Thankfully, it is typically easier to apply secure cloud configuration to mitigate the impact of these vulnerabilities. Relying on the CSP's security defaults and documentation is insufficient. SEC510 exposes many examples of incorrect, incomplete, or contradictory CSP controls. Additionally, if there is a zero-day vulnerability in a cloud service used by your organization, you must brace for that impact by controlling what you can.

SEC510 leverages standards and frameworks where useful, such as the MITRE ATT&CK Cloud Matrix, the Center for Internet Security (CIS) Cloud Provider Benchmarks, and the Cyber Defense Matrix. These tools have limits, and SEC510 goes beyond them to teach the techniques needed to protect what matters to the organization. Mitigate the risk of common cloud mistakes with cloud security controls that matter and reduce your attack surface by eliminating misconfigurations.

"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

Hands-On Training

SEC510: Cloud Security Controls and Mitigations 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. Students can continue to use the lab instructions, application code, and IaC after the course concludes. With this, they can repeat every lab exercise in their own cloud environments as many times as they like.

SEC510 also offers students an opportunity to participate in Bonus Challenges each day in a gamified environment, while also providing more hands-on experience with the Big 3 CSPs and relevant utilities. Can you win the SEC510 Challenge Coin?

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.

Section Descriptions

SECTION 1: Cloud Identity and Access Management

SEC510 starts with a brief overview cloud breach trends, exploring why the vast majority of breaches are now happening in the cloud. We will explore how multicloud makes security harder, why organizations are going multicloud, and how both standardization and cloud agnosticism cannot solve the problem alone. We introduce three of the frameworks we will use throughout the course to implement attack-driven controls and mitigations: the MITRE ATT&CK Cloud Matrix, the Center for Internet Security (CIS) Cloud Foundational Benchmarks, and the Cyber Defense. Students will then initialize their lab environment and deploy a modern web application to each of the Big 3 providers. This leads into an analysis of one of the most fundamental and misunderstood concepts in cloud security: Identity and Access Management. The remainder of this section will focus on how to harden the IMDS and leverage well-written IAM policies to minimize the harm caused by such attacks. These strategies are critical to prevent a minor vulnerability from becoming front-page news.

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

SECTION 2: Cloud Virtual Networks

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

Data security is as important, if not more important, in the cloud than it is on-premises. There are countless cloud data leaks that could have been prevented with the appropriate controls. This section examines the cloud services that enable data encryption, secure storage, access control, data loss detection, policy enforcement, and more. The first half of Section 3 covers all you need to know about encryption in the cloud. Students will learn about each provider's cryptographic key management solution and how it can be used to apply multiple layers of encryption at rest. The second half of Section 3 is primarily focused on cloud storage services. After briefly discussing the most basic storage security technique, turning off public access, it will cover more advanced controls like organization-wide access control, file versioning, data retention, secure transit, and more. It concludes with a discussion of additional data exfiltration paths and how to automatically detect sensitive data storage.

TOPICS: Cryptographic Key Management; Encryption with Cloud Services; Cloud Storage Platforms; Sensitive Data Exfiltration; Sensitive Data Detection

SECTION 4: Cloud Application Services and 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 and Cloud Security Posture Management

The course concludes with practical guidance on how to operate an organization across multiple cloud providers. Many of the topics discussed in the sections become more complicated if an organization's cloud providers are integrated with one another. We begin by discussing multicloud integration impacts Identity and Access Management (IAM). The next module covers the cloud-native Cloud Security Posture Management (CSPM) services. Students will use these services to automate security checks for the CIS Benchmarks covered throughout the course. With these capabilities, an organization can take the lessons learned in SEC510 and apply them at scale. The final module, Multicloud CSPM, ties these two topics together. Most organizations would prefer to use a single platform to assess the security posture of all their clouds. After learning about the third-party multicloud CSPM services, students will leverage Workload Identity such that Microsoft Defender for Cloud to analyze the security posture of all three cloud providers. If implemented properly, this capability will be invaluable to security organizations. If done wrong, this integration can decrease the security of the organization's AWS accounts and Google Cloud projects. This module will highlight these pitfalls to ensure that students engineer this correctly from the start.

TOPICS: Multicloud Access Management; Cloud Security Posture Management; Vendor Integration and Multicloud Security Posture Management; 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
  - Identity and Access Management
  - Managing a cloud-based virtual network
  - Secure configuration management

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