SEC510: **Public Cloud Security: AWS, Azure, and GCP**

5 Day Course	30 CPEs	Laptop Required

You Will Be Able To

- Understand the inner workings of cloud services and Platform as a Service (PaaS) offerings in order to make more informed decisions in the cloud
- Understand the design philosophies that undergird each provider and how these have influenced their services in order to properly prescribe security solutions for them
- Discover the unfortunate truth that many cloud services are adopted before their security controls are fully fleshed out
- Understand Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) in depth.
- Understand the intricacies of Identity and Access Management, one of the most fundamental concepts in the cloud and yet one of the last understood
- Understand cloud networking and how locking it down is a critical aspect of defense-in-depth in the cloud
- Analyze how each provider handles encryption at rest and in transit in order to prevent sensitive data loss
- Explore the service offering landscape to discover what is driving the adoption of multiple cloud platforms and to assess the security of services at the bleeding edge
- Understand the complex connections between cloud accounts, providers, and on-premise systems and the cloud
- Perform secure data migration to and from the cloud
- Understand Terraform Infrastructure-as-Code well enough to share it with your engineering team as a starting point for implementing the controls discussed in the course

Multiple Clouds Require Multiple Solutions

SEC510: Public Cloud Security: AWS, Azure, and GCP teaches you how the major cloud providers work and how to securely configure and use their services and Platform as a Service (PaaS) offerings.

Organizations in every sector are increasingly adopting cloud offerings to build their online presence. However, although cloud providers are responsible for the security of the cloud, their customers are responsible for what they do in the cloud. Unfortunately, the providers have made the customer's job difficult by offering many services that are insecure by default. Worse yet, with each provider offering hundreds of different services and with many organizations opting to use multiple providers, security teams need a deep understanding of the underlying details of the different services in order to lock them down. As the landscape rapidly evolves and development teams eagerly adopt the next big thing, security is constantly playing catch-up in order to avert disaster.

SEC510 provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services.

The Big 3 cloud providers alone provide more services than any one company can consume. As security professionals, it can be tempting to limit what the developers use to the tried-and-true solutions of yesteryear. Unfortunately, this approach will inevitably fail as the product development organization sidelines a security entity that is unwilling to change. Functionality drives adoption, not security, and if a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. SEC510 gives you the ability to provide relevant and modern guidance and guardrails to these teams to enable them to move both quickly and safely.

Course Authors' Statement

"The move to leveraging multiple public cloud providers introduces new challenges and opportunities for security and compliance professionals. As the service offering landscape is constantly evolving, it is far too easy to prescribe security solutions that are not accurate in all cases. While it is tempting to dismiss the multicloud movement or block it at the enterprise level, this will only make the problem harder to control.

"Why do teams adopt additional cloud solutions in the first place? To make their jobs easier or more enjoyable. Developers are creating products that make money for the business, not for the central security team. If a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. Security should embrace the inevitability of the multicloud movement and take on the hard work of implementing guardrails that enable the organization to move quickly and safely.

"The multicloud storm is coming, whether you like it or not."

— Brandon Evans and Eric Johnson

Section Descriptions

SECTION 1: Cloud Credential Management

SEC510 starts with a brief overview of the Big 3 cloud providers. We will examine the factors driving adoption of multiple cloud providers and the rise in popularity of Azure and GCP, which historically have lagged far behind AWS. 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 the intricacies of Identity and Access Management (IAM), one of the most fundamental and misunderstood concepts in cloud security. Playing the role of an attacker in their lab environment, students will compromise real IAM credentials using application vulnerabilities and then use them to access sensitive data. The remainder of this section will focus on how to leverage well-written IAM policies to minimize the damage caused by such attacks. Although the ultimate solution is to fix the bug in the application, these strategies can prevent a minor incident from becoming front-page news.

TOPICS: The Multicloud Movement; Multicloud Security Assessment; Identity and Access Management; Cloud Credentials Management; Application Vulnerability Overviews

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. The section begins by demonstrating how ingress and egress traffic can be restricted within each provider. Students will analyze the damage that can be done without these controls by accessing a public-facing database and creating a reverse shell session in each environment. We will then eliminate both attack vectors with secure cloud configuration. In addition to introducing additional network defense-in-depth mechanisms, we will discuss cloud-based intrusion detection capabilities to address the network-based attacks we cannot eliminate. Students will analyze cloud traffic and search for indicators of compromise.

TOPICS: Cloud Virtual Networks; Network Traffic Analysis; Private Endpoints; Advanced Remote Access; Command and Control Servers

SECTION 3: Encryption, Storage, and Logging

The first half of Section 3 covers all topics related to encryption in the cloud. Students will learn about each provider's cryptographic key solution and how it can be used to encrypt data at rest. Students will also learn how end-to-end, in-transit encryption is performed in the cloud, such as the encryption between clients, load balancers, applications, and database servers. Proper encryption is not only critical for security; it is also an important legal and compliance consideration. This section will ensure that your organization has all of the information at its disposal to send the auditors packing. The second half of Section 3 covers storing data in the cloud, defense-in-depth mechanisms, access logging, filesystem persistence, and more.

TOPICS: Cloud Key Management; Encryption with Cloud Services; Cloud Storage Platforms

SECTION 4: Serverless Platforms

This course section tackles the ever-changing trends in technology by providing in-depth coverage of a paradigm taking the industry by storm: Serverless. It balances the discussion of the challenges serverless introduces with the advantages it provides to secure product development and security operations. The first half of the section covers serverless cloud functions in AWS Lambda, Microsoft Azure, and Google Cloud Functions. After introspecting the serverless runtime environments using Serverless Prey (a popular open-source tool written by the course authors), students will examine and harden practical serverless functions in a real environment. The second half of the course section covers App Services, which often interplay with cloud functions. The section concludes with a detailed analysis of Firebase, an application platform with serverless offerings that has been loosely integrated with the Google Cloud Platform since its acquisition by Google in 2014.

TOPICS: Cloud Serverless Functions; Application Platforms

SECTION 5: Cross-Account and Cross-Cloud Assessment

The course concludes with practical guidance on how to operate an organization across multiple cloud accounts and providers. Many of the topics discussed in the earlier course sections are significantly complicated when moving from a single account to multiple accounts, as well as when the providers are integrated with each other. We will cover these complications, look at automatic security benchmarking utilities, and safely tear down the lab environment.

TOPICS: Cross-Account Management; Cross-Cloud Integrations; Automated Benchmarking; Summary; Additional Resources

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

"It highlighted the 3 main cloud platforms with their advantages and disadvantages of each other. The course taught us how to create users, hack in the systems with vulnerabilities, and then taught how to harden them."

— Almami Kassama, **Ahold**