SEC549: **Enterprise Cloud Security Architecture**

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Enable business through secure cloud architectural patterns
- Connect the dots between architectural patterns and real-life infrastructure
- Build a secure, scalable identity foundation in the cloud
- Centralize your organization's workforce identity to prevent sprawl
- Build micro-segmented networks using hub and spoke patterns
- Configure centralized network firewalls for inspecting north-south and east-west traffic
- Learn how to incorporate both network-based and identity-based controls
- Ability to create data perimeters for cloud-hosted data repositories
- Centralize and share Key Management Service (KMS) resources across an organization
- Enable Security Operations to respond in the Cloud
- Understand the telemetry and logging available across service models (IaaS, PaaS and SaaS)
- Design recovery processes leveraging break-glass accounts
- Strategically approach a phased cloud migration

"I would recommend this course. It hits many core aspects of secure design. Additionally, lack of Cloud Security Architecture and Strategy, and Insecure Design have been highlighted as a top risk by organizations like Cloud Security Alliance and OWASP. Cloud security architecture topics need to have more attention and focus in general."

—Greg Lewis, **SAP**

Design it Right from the Start

Without a mental model for threats in the cloud, architects attempt to strong-arm design patterns intended for the on-premise world onto cloud systems, hindering the speed of cloud adoption and modernization. Worse yet, failure to identify trust boundaries in the cloud results in missing security controls at the identity or network-planes and poor security outcomes. SEC549 introduces students to security architecture as it applies to the cloud. Students take away from this course a clear mental model of the cloud and the controls available to them, allowing students to shift their threat models to this new, vastly different world with distributed perimeters and unfamiliar trust boundaries.

It's inevitable that even the most mature organizations will have their security posture challenged, therefore in this course we dive deep into architectures which enable Security Operation Centers to monitor, detect, respond and recover from incidents in the cloud. Students learn how to effectively support business goals with robust logging of cloud telemetry and centralization of events and insights gathered at the edge. This course empowers the Architect to ensure adequate logging is configured in cloud environments and develop recovery strategies emphasizing the need to design for availability.

SEC549 is constructed around the cloud migration journey of a fictional company and the challenges they encounter along the way. Students are tasked with phasing in a centralized identity plan, building large scale micro-networks, and designing big data services for cloud-hosted applications. Both network-layer and identity-layer controls are covered in-depth as complementary mechanisms for securing access to distributed resources. The importance of centralizing identity is a core take-away of this course as showcased through the discussion of fragmented identity and its perils, especially with the rise of the Cloud and the adoption of multiple cloud service providers. Students are taught the foundational concepts used when designing for phased identity consolidation so they can confidently tackle similar challenges on the job.

Business Takeaways:

- Mitigate the risk posed by nascent cloud technologies and their rapid adoption
- Decrease the risk of cloud migrations by planning for phased approach
- Help your organization prevent identity sprawl and tech debt through centralization
- Enable business growth by creating high-level guardrails
- Prevent costly anti-patterns from becoming entrenched
- Move your organization towards a Zero-Trust posture through the uplifting of existing access patterns

Hands-On Training:

The hands-on portion of the course is unique and especially suited to the student who wants to architect for the cloud. Each lab is performed by observing and correcting an anti-pattern presented as an architectural diagram. The "correct" version of each diagram is implemented as live infrastructure in AWS and made available to the student to explore the configurations. In this course, the students have access to an enterprise-scale AWS Organization and can observe all details discussed in the labs and throughout the course.

Each of the sections of the course discusses security design considerations for all three major clouds, however there is an emphasis on working with AWS and labs are structured around concepts in AWS.

Section Descriptions

SECTION 1: Cloud Account Management and Identity Foundations

SEC549 kicks off by defining concepts used throughout the course such as threat modeling the cloud, what makes a secure pattern and how our mental models need to adapt for the cloud. This section dedicates a portion of time to foundational concepts of identity in the cloud from users, groups, roles, and machine identities and how those concepts subtly differ across the three major cloud providers. Managing identity in the cloud is an overarching theme of this section. This course teaches students the core concepts of identity federation, single sign-on, and the protocols used in these technologies. Using AWS SSO as an example, students are taught how to enable identity federation in support of a centralized workforce identity, automatically provision users to the cloud and centrally maintain attributes governing access control.

TOPICS:

- Security architecture in the cloud with an emphasis on threat modeling cloud-native services
- Using the large-scale building blocks offered in three CSP to create effective hierarchical designs
- Implementing an identity foundation – understanding how permissions are granted and patterns of IAM in the cloud
- Federated access and single sign-on – managing users at scale with the federation of identity

SECTION 2: Implementing an Identity Perimeter in the Cloud

Identity and access control forms the basis of the concepts of this section. Section 2 starts with an in-depth look at the zero-trust movement, its history and how zero-trust in the cloud can be leveraged to uplift legacy access patterns. We not only discuss permission granting architectures but also how to build identity guardrails into your cloud estates, ensuring constraints are placed for security or compliance purposes. Students will learn how to authenticate end users and machine identities acorss multiple public cloud environments. The section wraps up by implementing policies that restrict access between an organization's resources and trusted third parties.

TOPICS:

- Cloud Migrations – considerations and business drivers
- Zero-Trust Concepts – using cloud services to implement zero-trust patterns in a phased approach
- Implementing the Identity Pillar into Cloud-hosted applications using AWS Cognito
- Establishing Perimeters in the Cloud for Application Access – AWS S3 Use Cases and design patterns to secure your data in the cloud
- Enforcing identity boundaries with guardrails across clouds

Who Should Attend

- Cloud Security Architects
- Security Engineers
- Cloud Engineers
- DevOps Engineers
- Security Auditors
- System Administrators
- Operations
- Anyone who is responsible for:
  - Enabling business through secure cloud architecture
  - Evaluating and adopting new cloud offerings
  - Planning for cloud migrations
  - Identity and access management
  - Managing a cloud-based virtual network

SECTION 3: Network Access Perimeters for the Cloud

With a solid identity foundation, students shift focus to cloud architecture patterns for their organization. Building an enterprise cloud network requires a fundamental understanding of how things change moving from an on-premise network. Section 3 starts with the key resources required to build public, private, and hybrid cloud networks. From there, students learn to centrally manage the configuration of these resources across their organization. Next, we explore cloud micro-segmentation, hub and spoke networks, and routing traffic between micro-networks. Our focus then shifts to centralizing traffic flow through ingress and egress networks, as well as inspecting east-west traffic with third-party security appliances. Finally, students learn how to share network services by adding additional spoke networks and sharing DNS configurations across the organization.

TOPICS:

- Comparing on-premise and cloud-hosted virtual networks
- Managing cloud-hosted networks at scale with VPC sharing and the firewall manager
- Building micro-segmentation and hybrid networks with hub and spoke architecture
- Centralizing ingress and egress traffic network controls
- Inspecting east-west traffic with third-party security appliances
- Sharing network services and private DNS resources

SECTION 4: Data Access Perimeters in the Cloud

Section 4 focuses on cloud-native data protection patterns. Starting with common organization-wide storage service controls, students will establish foundational data perimeter policies. From there, we learn to segment data lake access through views and access points. Next, students explore how attribute-based access control, tagging, and data masking can enable cloud-native data loss prevention controls. Finally, the section wraps up with key management and backup architecture patterns.

TOPICS:

- Managing access to Cloud-Native Storage services
- Establishing perimeters in the Cloud for application access
- Data-Lake access control and governance with access points and views
- Big Query (BQ) identity and data exfiltration controls
- Data tagging for attribute-based access control, masking, and data loss prevention
- Centralizing key management and data backup resources

SECTION 5: Enabling the Cloud-Focused SOC

This section covers how to enable your SOC to operate (investigate incidents, log events, hunt for threats) in the new cloud-based world. Covered in this section is a deep dive on cloud data sources, aggregating logs and cloud-native events within the CSP while positioning them for export to the central SIEM. This section teaches students how to build effective architecture which empowers defenders to respond, contain and ultimately recover from cloud-based incidents.

TOPICS:

- Security Operations in a Cloud-Centric World
- In-depth look at data sources logging and aggregation to ensure sufficient logging coverage given various service models (IaaS, PaaS, SaaS)
- Enabling response in the cloud with network-layer and identity-layer quarantine zones
- Designing break-glass accounts for cloud account recovery with availability in mind