SEC549: Enterprise Cloud Security Architecture

2	12	Laptop
Day Course	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
- Learn how to incorporate both network-based and identity-based controls
- Ability to create data perimeters for cloud-hosted data repositories
- Strategically approach a phased cloud migration

"All three of today's labs were helpful in cementing the concepts. The "See It In Action" portions were particularly useful."

—Oritse Uku

"The lab was straightforward and didn't require much existing AWS cloud knowledge. The lab demonstrated the how and why policies need to be manageable."

—Andrew Guggenberger

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. In the SEC549, students are introduced 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.

The course 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 and designing secure patterns for enabling 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 confidentially 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 SEC549 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 1correct 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 1:** Structuring Accounts to Create Effective Hierarchies, Transitioning Access from IAM Users to Roles, AWS SSO for Permission Management
- **Section 2:** Integrating Modern Authentication into Legacy Applications, Creating a Shared VPC Architecture, Access Control for Shared Data Sets

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 3 major cloud providers. Managing identity in the cloud is an over-arching 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 Zero-Trust in the Cloud

Opening up Section 2 is 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. Dividing the day are the complementary concepts of network-layer controls and identity-layer controls. Both are covered in detail as we look to build business enabling patterns such as shared VPCs and the connection of VPC-aware to non VPC-aware resources. Finally, to frame the discussion around S3 Bucket controls, several common use cases for cloud-hosted data repositories are outlined and with the use cases, the accompanied controls that can be leveraged to enable them.

TOPICS:

- **Cloud Migrations—**Considerations and business drivers
- **Zero-Trust Concepts—**Using cloud services to implement zero-trust patterns in a phased approach
- **Establishing Perimeters in the Cloud for Application Access—**Network patterns in the cloud and using network-layer controls to enable application workloads
- **Establishing Perimeters in the Cloud for Application Access—**AWS S3 Use Cases and design patterns to secure your data in the cloud

Course Author's Statement

"The cloud has turned our perimeter increasingly distributed and is often solely enforced with identity-based controls. In the cloud, safeguards have been lifted and the room for error is slim. Even with this grim reality, I am still optimistic. The migration to the cloud has enabled our most innovative technologies and presents an opportunity for the security sector to evolve and mature.

If armed with the correct foundational principles, we can as an industry build a more secure future, with greater availability and confidentiality than ever possible on-premises. If history has taught us anything, transitioning to the new cloud-native, zero-trust world will be bumpy but I am so pleased to help shepherd you along the journey."

—Kat Traxler

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

NICE Work Roles

- Security Architect - SP-ARC-002
- Research & Developmental Specialist - SP-TRD-001
- Information Systems Security Developer - SP-SYS-001
- Systems Developer - SP-SYS-002
- IT Program Auditor OV-OMA-005
- System Administrator OM-ADM-001
- Information Systems Security Manager OV-MGT-001

Additional Free Resources

- Privilege Escalation in GCP – A Transitive Path
- It's Like Chipotle – Demystifying GCP PaaS Services
- Fix Security Issues Left of Prod
- Detecting and Locking Down Malware in Azure, by Brandon Evans
- Top 5 Considerations for Multicloud Security, by Brandon Evans