SEC549: **Cloud Security Architecture™**

GCAD
Cloud Security Architecture and Design
giac.org/gcad

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Design secure, enterprise-ready cloud architectures that support business goals.
- Build a scalable identity foundation by centralizing workforce identity with conditional access policies and break-glass access
- Learn how the cloud enables zero-trust for workforce, customer, and workload identities with both identity-based and network-based security controls.
- Create micro-network segmentation using with hub-and-spoke models and centralized inspection firewalls.
- Protect data stored in the cloud with strong network and identity perimeters
- Learn how to create centralized Key Management Service (KMS), AI service, and disaster recovery designs
- Enable cloud incident response and telemetry, using centralized intra-cloud and cross-cloud push and pull logging designs.

Business Takeaways:

- Reduce cloud risks with strategic, phased adoption plans
- Prevent identity sprawl and technical debt through centralization
- Support growth with high-level guardrails and secure architecture
- Avoid costly anti-patterns with thoughtful cloud design
- Move toward zero-trust using proven access control patterns
- Create effective conditional access and manage policy exceptions

Design It Right from the Start

SEC549 teaches students how to design secure, enterprise-scale cloud infrastructure that supports real business needs while preventing the identity sprawl and technical debt that accumulate when security is bolted on later. Students learn to use the cloud providers' well-architected frameworks to design centralized security controls across AWS, Azure, and Google Cloud while still supporting the speed organizations expect from cloud adoption.

The course focuses on how security architecture changes in the cloud, where perimeters are widely distributed, trust boundaries are unfamiliar, and identity often becomes the primary control point. Building on a zero-trust foundation, students design strategies for workforce identity, conditional access, policy guardrails, workload identity, network security controls, data perimeters, AI service architecture, key management, disaster recovery, and cloud logging.

SEC549 follows the cloud migration journey of a fictional enterprise. Students threat model the organization's existing cloud infrastructure, analyze design risks, and perform security architecture reviews that weigh the strengths, weaknesses, and tradeoffs of new cloud design patterns. Across five days, students complete 15 hands-on labs, 25 security architecture reviews, and 10 CloudWars challenge rounds.

Throughout the course, students work in live, enterprise-scale AWS, Azure, and Google Cloud environments, with access to the lab environment and sandbox cloud accounts so they can observe the patterns discussed in class firsthand.

At the end of each section, CloudWars challenge rounds ask students to create architecture design plans for the enterprise's acquisition of a young startup. Each scenario provides the startup's existing cloud resources, interviews with key employees, and migration requirements. Students work in teams to build migration plans, architecture diagrams, and supporting documentation, then present their final plans in the capstone exercise to decide which team wins the SEC549 challenge coin.

What Is Cloud Security Architecture?

Cloud security architecture is the practice of designing secure cloud systems that align with business goals and can be implemented, operated, and maintained in real environments. It requires architects to understand both the organization's requirements and the capabilities of cloud services in order to create secure access patterns, network controls, and data protection strategies.

Cloud security architects must design across Infrastructure as a Service, Platform as a Service, and Software as a Service. Hybrid environments, where cloud workloads connect with on-premises systems, add another layer of complexity. The goal is to identify design flaws, inefficient patterns, and risky trust relationships early, then address them with cloud-native security controls before systems go live.

"The problems we talk about are some that I face in my job every day or know I will face shortly. Getting definitive answers for many of these issues is very helpful for me. Getting years of experience from the instructors and what they have worked on is invaluable."

—Patrick Haughney, **Paylocity**

Section Descriptions

SECTION 1: Cloud Account Management and Identity Foundations

Section 1 introduces core concepts like cloud threat modeling and secure design, then moves into cloud identity. Students build identity foundations, enable federation from Entra ID to AWS and GCP, design resource hierarchies, set up policy guardrails, and manage cloud access.

TOPICS:

- Security Architecture in the Cloud
- Cloud Identity Foundations
- Federated Access / Single Sign-On (SSO)
- Creating Hierarchical Cloud Structures and Guardrails
- Privileged Identity Management

SECTION 2: Implementing an Identity Perimeter in the Cloud

Section 2 explores zero-trust in the cloud, focusing on conditional access policies, customer identity and access management (CIAM), and authenticating users and machines across clouds.

TOPICS:

- Implementing Zero-Trust Architecture
- Conditional Access Policies
- Customer Identity and Access Management (CIAM)
- Architecting Cross-Cloud Authentication

SECTION 3: Network Access Perimeters for the Cloud

Section 3 covers cloud network components and design, starting with the key resources for public, private, and hybrid clouds. Students learn centralized management, micro-segmentation, traffic inspection, and how to access shared services.

TOPICS:

- On-Premises versus Cloud Networks
- Managing Cloud-Hosted Networks at Scale
- Cloud Network Micro-Segmentation
- Network Firewalls and Traffic Inspection
- Centralized Shared Network Services

SECTION 4: Data Access Perimeters in the Cloud

Section 4 covers cloud-native data protection: storage controls, data lake security, and sensitive information discovery using tags, attribute-based access control (ABAC), and masking. Students apply these controls to design cloud-hosted AI services, then finish with key management, data backup, and disaster recovery architecture.

TOPICS:

- Data Security and Privacy Playbook
- Data Lake and Cloud Storage Security
- AI Service Architecture
- Business Continuity and Disaster Recovery Design

SECTION 5: Enable the Cloud-Focused SOC

Section 5 teaches students how to enable SOC operations in the cloud, covering cloud data sources, log aggregation, and exporting to a central SIEM. Students design logging architectures that support threat detection, response, and recovery from cloud incidents.

TOPICS:

- Security Operations in a Cloud-Centric World
- Intra-cloud Logging and Aggregation
- Centralized Log Export Patterns

"The content is excellent. It provides a lens and framework to look at enterprise problems from an architectural lens and will provide actionable information that can be used on Day 1 after this course."

—Tyler Piller, **British Columbia Lottery Corporation**

Who Should Attend

- Solutions architects
- Security auditors
- Cloud architects
- Security engineers
- Security architect
- Cloud engineers
- DevOps engineers
- System administrators
- Operations
- Anyone who is responsible for:
  - Enabling business through secure cloud architecture
  - Evaluating and adopting new cloud offerings
  - Planning for cloud migrations
  - Implementing or managing cloud identity and access management
  - Managing a cloud-based virtual network

GCAD
Cloud Security Architecture and Design
giac.org/gcad

GIAC Cloud Security Architecture and Design

The GIAC Cloud Security Architecture and Design (GCAD) certification validates a practitioner's understanding of cloud provider frameworks and design approaches for secure architecture in the cloud. GCAD certification holders have demonstrated knowledge of the strategies and design techniques for topics such as workforce identity, conditional access, network security controls, and centralized logging.

- Identity and access management
- Design and implement Zero-Trust concepts
- Network architecture and design
- Data protection
- Configuring centralized monitoring