ICTD
المركز العالمي للتدريب والتطوير
International Centre For Training & Development

SEC549: Cloud Security Architecture

Course Introduction:

As organizations increasingly migrate to cloud environments, securing cloud architectures has become a top priority. **SEC549: Cloud Security Architecture** is designed to provide cybersecurity professionals with a deep understanding of cloud security principles, frameworks, and best practices. This course focuses on securing cloud infrastructures, identifying threats in cloud environments, implementing identity and access management (IAM), and aligning security strategies with compliance and regulatory requirements. Participants will gain insights into securing multi-cloud and hybrid environments while ensuring resilience against evolving cyber threats.

Over five days, attendees will explore cloud security architecture design, risk management strategies, threat modeling, and security controls for major cloud service providers (CSPs) such as AWS, Azure, and Google Cloud. The course also covers cloud governance, security automation, and incident response strategies. By the end of the program, participants will have the theoretical knowledge required to design, assess, and improve cloud security postures in complex enterprise environments.

Course Objectives:

Upon completion of this course, participants will:

- Understand the core principles of cloud security architecture.
- Learn best practices for securing cloud infrastructure, platforms, and applications.
- Explore cloud security frameworks and compliance standards (CSA, NIST, ISO 27017).
- Identify key risks and threats in cloud environments and develop mitigation strategies.
- Gain insights into cloud identity and access management (IAM) and Zero Trust models.
- Understand security controls for cloud-native applications and DevSecOps practices.
- Analyze incident response strategies and forensic techniques in cloud environments.
- Learn how to design security architectures for multi-cloud and hybrid deployments.

Who Should Attend?

This course is designed for professionals involved in Cloud security architecture and engineering, Cybersecurity and IT risk management, Cloud governance and compliance, Security operations in cloud environments, DevSecOps and cloud security automation, and IT infrastructure and enterprise cloud migration strategies.

Course Outline:

Day 1: Foundations of Cloud Security Architecture

- Overview of cloud computing models (IaaS, PaaS, SaaS)
- Shared responsibility model and cloud security fundamentals
- Cloud security governance and risk management frameworks
- Security challenges in cloud adoption and migration

Day 2: Cloud Security Controls and Risk Management

- Cloud security controls: preventive, detective, and corrective measures
- Identity and access management (IAM) and least privilege principles
- Zero Trust architecture (ZTA) and cloud security best practices
- Threat modeling and risk assessment in cloud environments

Day 3: Multi-Cloud and Hybrid Cloud Security Strategies

- Security considerations for AWS, Azure, and Google Cloud
- Secure networking and segmentation in cloud environments
- Encryption and data protection strategies in multi-cloud setups
- Compliance and regulatory requirements for cloud security (GDPR, HIPAA, SOC 2)

Day 4: Cloud Security Automation and Incident Response

- Automating cloud security with Infrastructure as Code (IaC)
- Security monitoring, logging, and SIEM integration in cloud platforms
- Incident response and digital forensics in cloud environments
- Cloud security breaches and lessons learned

Day 5: Advanced Cloud Security Design and Future Trends

- Designing resilient cloud security architectures
- DevSecOps and integrating security into CI/CD pipelines
- Emerging trends in cloud security: AI-driven security, serverless security, and SASE
- Course review, Q&A session, and cloud security strategy discussions

Course Methodology:

A variety of methodologies will be used during the course that including:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play

- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentation

Course Certificate:

International Center for Training & Development (**ICTD**) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Fees:

To be advised as per course location. This rate includes participant's manual, Hand-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session

ICTD
المركز العالمي للتدريب والتطوير
International Centre For Training & Development