BLACKBIRD FOR TRAINING

Cloud Security for AWS, Azure, and Google Cloud

4 – 8 January 2027
Düsseldorf (Germany)



Cloud Security for AWS, Azure, and Google Cloud

Ref: 3255276_336995 **Date:** 4 – 8 January 2027 **Location:** Düsseldorf (Germany) **Fees:** 5900 GBP

Introduction

In today's rapidly evolving digital environment, cloud computing has become the foundation of modern enterprise infrastructure. As organizations increasingly rely on cloud platforms such as AWS, Microsoft Azure, and Google Cloud, the demand for robust cloud security frameworks has never been greater.

The Cloud Security for AWS, Azure, and Google Cloud course is designed to equip professionals with the knowledge and practical tools necessary to secure multi-cloud environments. It explores the shared responsibility model, data protection mechanisms, access control strategies, and threat mitigation techniques across leading cloud platforms.

This program empowers participants to design, implement, and manage comprehensive cloud security architectures that ensure compliance, resilience, and trust in a multi-cloud world.

Course Objectives

By the end of this course, participants will be able to:

- Understand cloud security fundamentals and the shared responsibility model.
- Implement identity and access management IAM across AWS, Azure, and Google Cloud.
- Configure network security, firewalls, and virtual private clouds VPCs.
- Apply data encryption, key management, and secure storage techniques.
- Detect and respond to cloud-specific threats using built-in security tools.
- Conduct compliance assessments aligned with global standards ISO, GDPR, NIST.
- Design a unified security framework for multi-cloud environments.

Course Outlines

Day 1: Introduction to Cloud Security Fundamentals

- Overview of cloud computing models IaaS, PaaS, SaaS.
- Understanding cloud shared responsibility models.
- Key security principles in public, private, and hybrid clouds.
- Common vulnerabilities and cloud attack vectors.
- Introduction to native security tools in AWS, Azure, and Google Cloud.



Day 2: Identity and Access Management IAM

- Managing users, roles, and policies in AWS, Azure AD, and GCP IAM.
- Implementing multi-factor authentication MFA.
- Least privilege principle and role-based access control RBAC.
- Managing credentials and secrets securely.
- Hands-on configuration of IAM policies across different platforms.

Day 3: Network and Infrastructure Security

- Securing virtual networks and subnets.
- Configuring firewalls, security groups, and network access controls.
- Establishing secure connectivity between clouds and on-premises systems.
- Implementing traffic monitoring and intrusion detection.
- Case study: Multi-cloud network segmentation best practices.

Day 4: Data Protection and Threat Response

- Encryption techniques for data at rest and in transit.
- Key Management Services KMS across cloud providers.
- Configuring security logs and audit trails.
- Detecting and mitigating insider and external threats.
- Using AI and automation for cloud threat detection and incident response.

Day 5: Governance, Compliance, and Continuous Security

- Cloud compliance frameworks: ISO 27001, SOC 2, GDPR, NIST.
- Implementing cloud governance and policy enforcement.
- Automating security through DevSecOps and CI/CD pipelines.
- Developing a cloud security posture management CSPM strategy.
- Final assessment and review of best practices for secure cloud adoption.

Why Attend this Course: Wins & Losses!

- Gain practical, hands-on experience securing AWS, Azure, and Google Cloud.
- Learn to detect and respond to multi-cloud security incidents effectively.
- Understand compliance and data protection across different cloud models.
- Build resilience against cyber threats in cloud-native environments.
- Develop expertise in IAM, encryption, and network security configuration.
- Strengthen your organization’s security governance and risk management.
- Master integration of automation and AI in cloud security operations.
- Receive practical insights and tools from real-world cloud security scenarios.



Conclusion

As organizations embrace multi-cloud strategies, ensuring consistent and effective cloud security has become a mission-critical priority. The complexity of managing multiple cloud platforms demands a unified, risk-based approach that combines technology, policy, and continuous monitoring.

The Cloud Security for AWS, Azure, and Google Cloud course provides professionals with the competencies to build and maintain secure cloud infrastructures. Participants will gain the technical depth and strategic perspective needed to design and execute security frameworks that align with business objectives while ensuring compliance and resilience.

This course is not just about technology—it's about empowering leaders to protect their organizations in an era where the cloud is both the backbone and the battleground of modern digital transformation.

