Course Name: Cloud Security Professional Certification Course

Course Overview

The "Cloud Security Professional Certification Course" course provides a comprehensive understanding of securing cloud environments, focusing on the unique challenges and opportunities of cloud platforms like AWS, Azure, and Google Cloud. This advanced course covers essential topics such as the Shared Responsibility Model, Identity and Access Management (IAM), and compliance with global standards. With practical labs, hands-on projects, and real-world scenarios, learners will gain expertise in implementing robust security policies, responding to incidents, and ensuring data protection in the cloud.

Course Type

Advanced-level course.

Course Objectives

- Understand cloud security principles, challenges, and the Shared Responsibility Model.

- Master Identity and Access Management (IAM) across AWS, Azure, and Google Cloud.

- Learn to secure cloud platforms and implement best practices for data protection.

- Gain proficiency in compliance standards like ISO 27017, GDPR, and HIPAA.

- Develop and implement cloud security policies through hands-on projects.

What You'll Learn?

Participants will explore the fundamentals of cloud security, including IAM, multi-factor authentication, and encryption methods for data protection. You'll dive deep into securing AWS, Azure, and Google Cloud platforms using their native tools and best practices. The course emphasizes compliance with industry standards and equips you with skills for cloud incident response. Practical projects, including implementing and automating cloud security policies, will ensure you can translate theory into actionable strategies.

Duration

40–50 hours.

Requirements

- Access to cloud platforms like AWS, Azure, or Google Cloud (free tiers are sufficient for most exercises).

- A computer with stable internet connectivity.

Pre-requisites

- Basic knowledge of cloud computing concepts.

- Familiarity with cybersecurity fundamentals.

- Experience with IT systems or cloud platforms is helpful but not mandatory.

Target Audience

- Cloud architects and security engineers seeking advanced cloud security skills.

- IT professionals transitioning to cloud security roles.

- Compliance officers and auditors working with cloud-based environments.

- Organizations aiming to enhance the security of their cloud infrastructure.

Curriculum

Module 1: Introduction to Cloud Security

- Overview of Cloud Computing Models (IaaS, PaaS, SaaS)

- Understanding the Shared Responsibility Model

- Challenges and Threats in Cloud Security

Module 2: Identity and Access Management (IAM)

- Principles of IAM

- Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)

- Multi-Factor Authentication (MFA)

- Implementing IAM in AWS, Azure, and Google Cloud

Module 3: Securing Cloud Platforms (Part 1)

- AWS Security:

- AWS Security Best Practices

- Configuring AWS Security Groups

- Using AWS Inspector and AWS Shield

Module 4: Securing Cloud Platforms (Part 2)

- Azure Security:

- Azure Security Center

- Azure Policy for Compliance

- Configuring Network Security Groups

- Google Cloud Security:

- Security Command Center

- Identity-Aware Proxy (IAP)

Module 5: Data Protection and Compliance in the Cloud

- Data Encryption (at rest, in transit)

- Key Management in the Cloud

- Cloud-Specific Compliance Standards (ISO 27017, GDPR, HIPAA)

- Data Loss Prevention (DLP) Solutions

Module 6: Incident Response for Cloud Environments

- Understanding Cloud Incident Response

- Cloud Monitoring and Alerting Tools

- Log Analysis in Cloud Environments

- Steps to Mitigate a Cloud Security Incident

Module 7: Hands-on Project (Part 1)

- Defining Security Policies for a Cloud Environment

- Implementing IAM and Network Security

Module 8: Hands-on Project (Part 2) and Course Wrap-Up

- Automating Compliance Checks

- Final Presentation of Cloud Security Policies

- Review and Next Steps in Cloud Security

Projects:

- Title: Implementing Security Policies in a Cloud Environment

- Details: Participants will select a cloud provider (AWS, Azure, or Google Cloud) and implement a comprehensive security policy.

- Deliverables: Policy documentation, configuration scripts, and a walkthrough presentation.