Cloud Security Architect: AWS, Azure & Google Cloud Defense Training Course

Ref: #CYB9083

Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity professionals and architects with the strategic knowledge and practical skills required to design and implement secure cloud environments on the three major platforms: AWS, Azure, and Google Cloud. The shift to cloud computing has introduced a new set of security challenges. This program goes beyond basic cloud security to focus on the architectural decisions and best practices that ensure a strong security posture from the ground up. Participants will learn how to secure cloud infrastructure, manage identity and access, and protect data in the cloud. We will cover key topics like shared responsibility, DevSecOps, and continuous monitoring across multiple cloud services. Drawing from the academic research of renowned authors like David A. Wheeler and his work on secure software design in his book "Software Security: A Guide for Developers and Architects," this program provides a strategic and practical framework for building a secure and resilient cloud presence. His work highlights that security must be an integral part of the design process, not an afterthought. This course at BIG BEN Training Center will empower you to become a trusted advisor who can build secure, scalable, and compliant cloud architectures.

Target Audience / This training course is suitable for:

- Cloud security architects.
- Cloud engineers.
- DevSecOps professionals.
- Cybersecurity consultants.
- IT and security managers.
- System architects.
- Network security engineers.

Target Sectors and Industries:

- Technology and software.
- Financial services.
- E-commerce.
- Healthcare.
- Telecommunications.
- Government agencies and equivalents.
- Global corporations.

Target Organizations Departments:

- Cloud Operations.
- Information Security.
- DevOps.
- IT Infrastructure.
- Application Development.
- Risk Management.
- Enterprise Architecture.

Course Offerings:

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

- Design a secure cloud architecture on AWS, Azure, and Google Cloud.
- Implement strong identity and access management controls.
- Protect data at rest and in transit.
- Automate security tasks using cloud-native tools.
- Develop a DevSecOps pipeline with security in mind.
- Ensure compliance with key regulations in the cloud.
- Conduct a risk assessment for cloud migration.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, lab-intensive methodology that simulates the real-world challenges of securing a multi-cloud environment. The program includes a series of virtual labs where participants will work with AWS, Azure, and Google Cloud services. You will learn to use cloud-native tools to configure security policies, manage access controls, and monitor for threats. The course emphasizes a practical, architectural approach. It teaches participants to think like a security architect who must design a solution that is both secure and scalable. The instructor will provide expert guidance and feedback throughout the exercises, ensuring that you develop the critical thinking and problem-solving skills required for high-stakes cloud security roles. This approach ensures the knowledge and skills gained are directly applicable to building a secure cloud presence.

Course Agenda (Course Units):

Unit One: Cloud Security Fundamentals

- Introduction to cloud security.
- The shared responsibility models.
- Key security concepts (IaaS, PaaS, SaaS).
- Threat landscape for cloud environments.
- Designing a secure foundation.
- Cloud governance and compliance.
- Case study: a cloud misconfiguration incident.

Unit Two: AWS Security Architecture

- AWS identity and access management (IAM).
- Securing EC2 instances and S3 buckets.
- Network security on AWS (VPC, security groups).
- Data protection and encryption.
- AWS security services (Guard Duty, Inspector).
- Serverless security on AWS Lambda.
- Practical lab: a secure AWS architecture.
- Three: Azure Security Architecture
- Azure Active Directory and identity.
- Securing Azure virtual machines and storage.
- Network security on Azure (VNet, NSG).
- Data protection and encryption.
- Azure security services (Security Center, Sentinel).
- Serverless security on Azure Functions.
- Practical lab: a secure Azure architecture.

Unit Four: Google Cloud Security Architecture

- Google Cloud IAM.
- Securing compute engines and storage buckets.
- Network security on Google Cloud (VPC, firewall rules).
- Data protection and encryption.
- Google Cloud security services (Security Command Center).
- Serverless security on Google Cloud Functions.
- Practical lab: a secure Google Cloud architecture.

Unit Five: Advanced Topics and Best Practices

- DevSecOps and security automation.
- Continuous monitoring and compliance.
- Cloud incident response.
- Multi-cloud security management.
- The future of cloud security.
- Final project: a multi-cloud security plan.
- Vendor-specific solutions vs. open standards.
- Frequently Asked Questions:

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

The shared responsibility model in cloud computing is a foundational concept, but how can an organization accurately and effectively determine which security responsibilities fall to them versus the cloud provider, especially as the complexity of cloud services and third-party integrations increases?

What unique qualities does this course offer compared to other courses?

This course stands out by providing a unique and vital focus on multi-cloud security architecture. Unlike many certification-focused courses that cover only one cloud provider, this program gives you a comprehensive understanding of the three major platforms: AWS, Azure, and Google Cloud. The curriculum is built around a hands-on, architectural approach. It teaches you to think like a security architect, not just a practitioner, enabling you to design resilient, scalable, and compliant cloud environments from the ground up. The emphasis on cross-platform knowledge, DevSecOps, and strategic architectural design distinguishes this course from others. It is for professionals who are ready to secure a multi-cloud enterprise and manage the complexity that comes with it.