Acquiescent
Consultancy Services India Pvt. Ltd.

AWS Security Engineer

Course Outline

1. Get started with Getting Started Guide.

2. Use Handouts to understand the concepts and course flow.

3. Complete Assignments at the end of each day.
4. Complete your project at the end of Course.

Course Content:

Module-1: Intro to AWS Security

1. AWS Cloud Security Overview

- Understanding the Shared Responsibility Model
- Security and compliance objectives in cloud computing

- Core AWS security services overview
- Introduction to AWS Identity and Access Management (IAM)

2. AWS (Identity and Access Management) IAM

- IAM users, groups, roles and policies
- Best practices for IAM, including least privilege access
- Managing IAM credentials and MFA
- Hands-on Lads: Setting up IAM policies and role

Module-2: Network Security and Infrastructure Protection

3. AWS Networking Concepts

- Virtual Private Cloud (VPC) architecture
- Security groups and Network ACLs
- VPC design considerations for security

4. Advanced Network Security

- VPN and Direct Connect
- AWS Security Hub and GuardDuty

- Hands-on Labs: Configuring VPC security features

Module-3: Data Protection

5. Data Encryption and Key Management

- AWS Key Management Service (KMS)
- Server-side encryption (SSE) and client-side encryption
- AWS Certificate Manager (ACM)

6. Securing Data on AWS

- Amazon S3 security best practices
- Securing databases with Amazon RDS and DynamoDB
- Hands-on Labs: Implementing data encryption

Module 4: Governance, Compliance, and Audit

7.Compliance Frameworks and AWS

- Introduction to compliance frameworks
- Using AWS Config for continuous monitoring
- AWS Artifact and compliance reports

8. Auditing and Security Logging

- AWS CloudTrail and AWS Config
- Setting up AWS CloudWatch for security monitoring
- Hands-on Labs: Implementing logging and monitoring

Module 5: Incident Response and Threat Detection

9. Incident Response On AWS

- Incident response planning and automation
- Using AWS Lambda in security automation
- AWS Systems Manager for incident responsear

10. Threat Detection and Management

- AWS WAF and AWS Shield
- Using Amazon Inspector for vulnerability management
- Hands-on Labs: Setting up threat detection Module

Module 6: Security Best Practices and Real-world Applications

11. AWS Security Best Practices

- Securing AWS infrastructure: EC2, S3, RDS
- Best practices for DevSecOps on AWS
- Implementing a secure CI/CD pipeline

12. Third party tools and Final Project*

- Review of tools like Wiz, Panaseer, Aikido
- Final Project: Implementing a comprehensive security solution
- Course Wrap-up and Q&A

Acquiescent
Consultancy Services India Pvt. Ltd.

For More : https://acquiescent.in