TechPledge®
Connect.Consult.Content

AWS Certified Security - Specialty

The AWS Certified Security – Specialty is intended for individuals who perform a security role with at least two years of hands-on experience securing AWS workloads.

Course Duration:

- 22 Hr.

No of Classes:

- 14 Classes

Course Material:

- Lectures (PDF)
- Lab Manual (PDF)

Abilities Validated by the Certification

- Define what the AWS Cloud is and the basic global infrastructure
- Assimilate and leverage the AWS shared security responsibility model
- Architect and build AWS application infrastructures that are protected against the most common security threats
- Protect data at rest and in transit with encryption
- Apply security checks and analyses in an automated and reproducible manner
- Configure authentication for resources and applications in the AWS Cloud
- Gain insight into events by capturing, monitoring, processing, and analyzing logs
- Identify and mitigate incoming threats against applications and data
- Perform security assessments to ensure that common vulnerabilities are patched and security best practices are applied
-

Syllabus Details

Introduction to Cloud Computing

- Understanding Cloud Computing
- Benefit and Feature of Cloud Computing
- Explain on Platform as a Service (PaaS), SaaS, IaaS
- Cloud Trends
- Introduction to Security on AWS

Identifying entry points on AWS

- Ways to access the platform
- IAM policies
- Securing entry points
- Incident response

Security Considerations - Web Applications

- Security points in an AWS web application environment
- Analyse a three-tier application model and identify common threats

- Assess environments to improve security
- Security Groups

Application Security

- Securing EC2 instances
- Assess vulnerabilities with Inspector
- Apply security in an automated way using Systems Manager
- Isolate a compromised instance

Securing Networking Communications

- Apply security best practices to VPC
- Implement an ELB device as a protection point
- Identify AWS services used to connect on-premise to AWS
- Data protection between on-premise and AWS
- Securely access VPC resources in other accounts

Data Security

- Protect data at rest using encryption and access controls
- AWS services used to replicate data
- Protect archived data

Security Considerations: Hybrid Environments

- Security points outside of a VPC
- Common DoS threats

Monitoring and Collecting Logs on AWS

- Monitor events and collect logs with CloudWatch
- Use Config to monitor resources
- AWS-native services that generate and collect logs

Account Management on AWS

- Manage multiple accounts
- Use identity providers / brokers to acquire access to AWS services

Secrets Management on AWS

- Manage key and data encryption with KMS
- Describe how CloudHSM is used to generate and secure keys
- Use Secrets Manager to authenticate applications
- Use Secret Key to get access to AWS Resources like S3

Threat Detection and Sensitive Data Monitoring

- Threat detection and monitoring for malicious or unauthorized behaviour
- Leverage machine learning to gain visibility into how sensitive data is being managed in the AWS Cloud