Security Engineering on AWS

Course 3568 – 24 Hours

Overview

This course demonstrates how to efficiently use AWS security services to stay secure in the AWS Cloud. The course focuses on the security practices that AWS recommends for enhancing the security of your data and systems in the cloud. It highlights the security features of AWS key services including compute, storage, networking, and database services. You will also learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents.

On Completion, Delegates will be able to

- Identify security benefits and responsibilities of using the AWS Cloud
- Build secure application infrastructures
- Protect applications and data from common security threats
- Perform and automate security checks
- Configure authentication and permissions for applications and resources
- Monitor AWS resources and respond to incidents
- Capture and process logs
- Create and configure automated and repeatable deployments with tools such as AMIs and AWS
- CloudFormation

Who Should Attend

This course is intended for security engineers, security architects, and information security professionals.

Prerequisites

We recommend that attendees of this course have:

- Working knowledge of IT security practices and infrastructure concepts
- Familiarity with cloud computing concepts
- Completed AWS Security Essentials and Architecting on AWS instructor-led courses

Course Contents

Module 1: Security on AWS

- Security in the AWS cloud
- AWS Shared Responsibility Model
- Incident response overview
- DevOps with Security Engineering

Module 2: Identifying Entry Points on AWS

- Identify the different ways to access the AWS platform
- Understanding IAM policies
- IAM Permissions Boundary
- IAM Access Analyzer
- Multi-factor authentication
- AWS CloudTrail
- Lab 01: Cross-account access

Module 3: Security Considerations: Web Application Environments

- Threats in a three-tier architecture
- Common threats: user access
- Common threats: data access
- AWS Trusted Advisor

Module 4: Application Security

- Amazon Machine Images
- Amazon Inspector
- AWS Systems Manager
- Lab 02: Using AWS Systems Manager and Amazon Inspector

Module 5: Data Security

- Data protection strategies
- Encryption on AWS
- Protecting data at rest with Amazon S3, Amazon RDS, Amazon DynamoDB
- Protecting archived data with Amazon S3 Glacier
- Amazon S3 Access Analyzer
- Amazon S3 Access Points

Module 6: Securing Network Communications

- Amazon VPC security considerations
- Amazon VPC Traffic Mirroring
- Responding to compromised instances
- Elastic Load Balancing
- AWS Certificate Manager

Module 7: Monitoring and Collecting Logs on AWS

- Amazon CloudWatch and CloudWatch Logs
- AWS Config
- Amazon Macie
- Amazon VPC Flow Logs
- Amazon S3 Server Access Logs
- ELB Access Logs
- Lab 03: Monitor and Respond with AWS Config

Module 8: Processing Logs on AWS

- Amazon Kinesis
- Amazon Athena
- Lab 04: Web Server Log Analysis

Module 9: Security Considerations: Hybrid Environments

- AWS Site-to-Site and Client VPN connections
- AWS Direct Connect
- AWS Transit Gateway

Module 10: Out-Of-Region Protection

- Amazon Route 53
- AWS WAF
- Amazon CloudFront
- AWS Shield
- AWS Firewall Manager
- DDoS mitigation on AWS

Module 11: Security Considerations: Serverless Environments

- Amazon Cognito
- Amazon API Gateway
- AWS Lambda

Module 12: Threat Detection and Investigation

- Amazon GuardDuty
- AWS Security Hub
- Amazon Detective

Module 13: Secrets Management on AWS

- AWS KMS
- AWS CloudHSM
- AWS Secrets Manager
- Lab 05: Using AWS KMS

Module 14: Automation and Security by Design

- AWS CloudFormation
- AWS Service Catalog
- Lab 06: Security automation on AWS with AWS Service Catalog

Module 15: Account Management and Provisioning on AWS

- AWS Organizations
- AWS Control Tower
- AWS SSO
- AWS Directory Service
- Lab 07: Federated Access with ADFS