Security Engineering on AWS

Course AWS-08 3 Days Instructor-led, Hands on

Course Information

Cybersecurity threats are escalating, and organizations need professionals who can efficiently use AWS security services to stay secure in the AWS Cloud. Security Engineering on AWS focuses on the security practices that AWS recommends for enhancing the security of your data and systems in the cloud. This course highlights the security features of AWS key services including compute, storage, networking, and database services. You'll also learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents.

Through hands-on labs and real-world scenarios, you'll gain practical experience in implementing security solutions, understanding specialized data classifications and AWS data protection mechanisms, and applying security best practices. This training is designed to help you stay secure in the AWS Cloud and prepare for the AWS Certified Security – Specialty certification.

At Course Completion

Upon successful completion of this course, students will be able to:

Security Engineering on AWS prepares you to design, implement, and manage secure infrastructure on the AWS cloud platform. You'll learn to protect applications and data from common security threats, perform and automate security checks, and configure authentication and permissions for applications and resources.

By the end of this course, you'll be able to monitor AWS resources and respond to incidents, capture and process logs, and create automated and repeatable deployments with tools such as AMIs and AWS CloudFormation. This course focuses on the security practices that AWS recommends for enhancing the security of your systems in the cloud.

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 courses.

Course Outline

Module 1: Introduction to Security in the AWS Cloud

- Understand the AWS Shared Responsibility Model
- Explore core cloud security principles
- Review incident response strategies in AWS
- Align DevOps processes with security engineering

Module 2: Managing Identity and Access Control

- Define and apply IAM policies, roles, and permissions boundaries
- Use IAM Access Analyzer for insight into access risks
- Implement multi-factor authentication (MFA)
- Monitor access activity with AWS CloudTrail

Module 3: Securing Web Application Environments

- Analyze threats to 3-tier application architectures
- Address common risks around user and data access
- Leverage AWS Trusted Advisor for continuous improvement

Module 4: Application Security at Scale

- Harden Amazon Machine Images (AMIs)
- Perform automated security assessments with Amazon Inspector
- Apply secure configuration management with AWS Systems Manager

Module 5: Data Protection and Encryption Best Practices

- Encrypt data in S3, RDS, DynamoDB, and Glacier
- Apply key management strategies using AWS KMS
- Use S3 Access Analyzer and Access Points for precise control

Module 6: Network Security and Traffic Protection

- Implement best practices for securing Amazon VPCs
- Use VPC Traffic Mirroring for deep packet inspection
- Respond to compromised instances
- Secure endpoints with AWS Certificate Manager and ELB

Module 7: Centralized Monitoring and Logging

- Configure CloudWatch, AWS Config, and Amazon Macie
- Enable VPC Flow Logs, ELB Logs, and S3 Server Access Logs

Module 8: Log Processing and Analysis

- Aggregate log data with Amazon Kinesis
- Analyze security events using Amazon Athena

Module 9: Securing Hybrid Cloud Architectures

- Connect environments with VPNs and Direct Connect
- Secure cross-region traffic with AWS Transit Gateway

Module 10: Building Global Resilience and DDoS Protection

- Use Route 53 and CloudFront for edge-level protection
- Defend against attacks with AWS WAF, Shield, and Firewall Manager

Module 11: Serverless Security Practices

- Control access in serverless environments with Amazon Cognito
- Secure APIs with API Gateway
- Implement least-privilege execution in AWS Lambda

Module 12: Threat Detection and Investigation

- Identify suspicious activity with Amazon GuardDuty
- Consolidate findings in AWS Security Hub
- Perform forensic analysis with Amazon Detective

Module 13: Secrets and Key Management

- Manage encryption keys using AWS KMS and CloudHSM
- Store and rotate secrets with AWS Secrets Manager

Module 14: Automating Security by Design

- Create secure, repeatable deployments with AWS CloudFormation
- Standardize infrastructure with AWS Service Catalog

Module 15: Governance and Account Management at Scale

- Manage multi-account environments with AWS Organizations
- Enforce controls using AWS Control Tower and AWS SSO
- Integrate centralized identity with AWS Directory Services