

**Security Engineering on AWS**

**Course Number:** AWS-124  
**Duration:** 3 days

**Overview**

This Security Engineering on AWS training course teaches attendees how to use AWS security services to secure their AWS Cloud environments. Attendees explore the security features of key AWS services, including compute, storage, networking, and database services. In addition, they learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents.

Accelebrate is an AWS Training Partner (ATP) and this hands-on official AWS Classroom Training course is taught by an accredited Amazon Authorized Instructor (AAI).

**Prerequisites**

All students should have:

* Taken [Architecting on AWS classroom training](file:////training/aws-architecture) and the [AWS Security Fundamentals classroom training](file:////training/aws-security-essentials), or have equivalent experience
* Working knowledge of IT security practices and infrastructure concepts
* Familiarity with cloud computing concepts

**Materials**

All AWS training students will receive comprehensive courseware.

**Software Needed on Each Student PC**

A modern web browser and an Internet connection free of restrictive firewalls, so that the student can connect by SSH or Remote Desktop (RDP) into AWS virtual machines.

**Objectives**

* 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

**Outline**

* Security on AWS
  + Security in the AWS cloud
  + AWS Shared Responsibility Model
  + Incident response overview
  + DevOps with Security Engineering
* 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
  + Cross-account access
* Security Considerations: Web Application Environments
  + Threats in a three-tier architecture
  + Common threats: user access
  + Common threats: data access
  + AWS Trusted Advisor
* Application Security
  + Amazon Machine Images
  + Amazon Inspector
  + AWS Systems Manager
  + Using AWS Systems Manager and Amazon Inspector
* 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
* Securing Network Communications
  + Amazon VPC security considerations
  + Amazon VPC Traffic Mirroring
  + Responding to compromised instances
  + Elastic Load Balancing
  + AWS Certificate Manager
* 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
  + Monitor and Respond with AWS Config
* Processing Logs on AWS
  + Amazon Kinesis
  + Amazon Athena
  + Web Server Log Analysis
* Security Considerations: Hybrid Environments
  + AWS Site-to-Site and Client VPN connections
  + AWS Direct Connect
  + AWS Transit Gateway
* Out-Of-Region Protection
  + Amazon Route 53
  + AWS WAF
  + Amazon CloudFront
  + AWS Shield
  + AWS Firewall Manager
  + DDoS mitigation on AWS
* Security Considerations: Serverless Environments
  + Amazon Cognito
  + Amazon API Gateway
  + AWS Lambda
* Threat Detection and Investigation
  + Amazon GuardDuty
  + AWS Security Hub
  + Amazon Detective
* Secrets Management on AWS
  + AWS KMS
  + AWS CloudHSM
  + AWS Secrets Manager
  + Using AWS KMS
* Automation and Security by Design
  + AWS CloudFormation
  + AWS Service Catalog
  + Security automation on AWS with AWS Service Catalog
* Account Management and Provisioning on AWS
  + AWS Organizations
  + AWS Control Tower
  + AWS SSO
  + AWS Directory Service
  + Federated Access with ADFS