AWS Security Best Practices

Course description

Currently, the average cost of a security breach can be upwards of $4 million. *AWS Security Best Practices* provides an overview of some of the industry best practices for using AWS security and control types. This course helps you understand your responsibilities while providing valuable guidelines for how to keep your workload safe and secure. You will learn how to secure your network infrastructure using sound design options. You will also learn how you can harden your compute resources and manage them securely. Finally, by understanding AWS monitoring and alerting, you can detect and alert on suspicious events to help you quickly begin the response process in the event of a potential compromise.

- Course level: Intermediate
- Duration: 1 day

Activities

This course includes presentations, demonstrations, and hands-on labs.

Course objectives

In this course, you will learn to:

- Design and implement a secure network infrastructure
- Design and implement compute security
- Design and implement a logging solution

Intended audience

This course is intended for:

- Solutions architects, cloud engineers, including security engineers, delivery and implementation engineers, professional services, and Cloud Center of Excellence (CCOE)

Prerequisites

Before attending this course, participants should have completed the following:

- AWS Security Fundamentals
- AWS Security Essentials

Course outline

Module 1: AWS Security Overview

- Shared responsibility model
- Customer challenges
- Frameworks and standards
- Establishing best practices
- Compliance in AWS

Module 2: Securing the Network

- Flexible and secure
- Security inside the Amazon Virtual Private Cloud (Amazon VPC)
- Security services
- Third-party security solutions

Lab 1: Controlling the Network

- Create a three-security zone network infrastructure.
- Implement network segmentation using security groups, Network Access Control Lists (NACLs), and public and private subnets.
- Monitor network traffic to Amazon Elastic Compute Cloud (EC2) instances using VPC flow logs.

Module 3: Amazon EC2 Security

- Compute hardening
- Amazon Elastic Block Store (EBS) encryption
- Secure management and maintenance
- Detecting vulnerabilities
- Using AWS Marketplace

Lab 2: Securing the starting point (EC2)

- Create a custom Amazon Machine Image (AMI).
- Deploy a new EC2 instance from a custom AMI.
- Patch an EC2 instance using AWS Systems Manager.
- Encrypt an EBS volume.
- Understand how EBS encryption works and how it impacts other operations.
- Use security groups to limit traffic between EC2 instances to only that which is encrypted.

Module 4: Monitoring and Alerting

- Logging network traffic
- Logging user and Application Programming Interface (API) traffic
- Visibility with Amazon CloudWatch
- Enhancing monitoring and alerting
- Verifying your AWS environment

Lab 3: Security Monitoring

- Configure an Amazon Linux 2 instance to send log files to Amazon CloudWatch.
- Create Amazon CloudWatch alarms and notifications to monitor for failed login attempts.
- Create Amazon CloudWatch alarms to monitor network traffic through a Network Address Translation (NAT) gateway.