Module Title : Security Engineering on AWS
Duration : 3 days

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. The course 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.

Intended Audience

This course is intended for:

- Security engineers
- Security architects
- Information security

Course Objectives

In this course, you will learn how to:

- 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

Prerequisites

We recommend that attendees of this course have the following prerequisites:

- AWS Cloud Practitioner
- AWS Security Fundamentals

- Architecting on AWS
- Working knowledge of IT security practices and infrastructure concepts
- Familiarity with cloud computing concepts

Delivery Method

This course is delivered through a mix of:

- Classroom training
- Hands-on labs
- Group exercises

Hands-on Activity

This course allows you to test new skills and apply knowledge to your working environment through a variety of practical exercises.

Course Outline

This course covers the following concepts:

Day 1

- Entry points on AWS
- Security considerations for Web Application environments
- Securing network communications inside the Amazon VPC
- Application security with incident response

Day 2

- Data security with incident response
- Security considerations for a hybrid environment
- AWS monitoring and log collecting
- Processing logs on AWS
- Protecting against threats outside of the Amazon VPC

Day 3

- Account management on AWS
- Security considerations for a serverless environment
- Secrets management on AWS
- Automating security and incident response on AWS
- Threat detection and sensitive data monitoring