Course: Security Engineering on AWS

Course description

Security is a concern for both customers in the cloud, and those considering cloud adoption. An increase in cyberattacks and data leaks remains top of mind for most industry personnel. The 32 hrs Instructor-led Training on Security Engineering on AWS addresses these concerns by helping you better understand how to interact and build with Amazon Web Services (AWS) in a secure way. In this course, you will learn about managing identities and roles, managing and provisioning accounts, and monitoring API activity for anomalies. You will also learn about how to protect data stored on AWS.

The Training explores how you can generate, collect, and monitor logs to help identify security incidents. Finally, you will review detecting and investigating security incidents with AWS services.

Course Highlights:

- Identity Security
- Network Security with AWS Network Firewall
- DDOS protection AWS Shield
- Protecting Web Application using AWS WAF
- Application threats and vulnerability management using AWS Inspector
- Encrypting Services and Application in AWS Secret Manager
- Configuring PKI for AWS Services and Applications using AWS Certificate manager

Duration: 4 Days

100 % Hands-on

Module Overview

Module-1: Architecture of AWS Security technologies

- Top Security Threats
- Zero-Trust Security principles
- Case Study: AWS Architecture with Security Technologies

Module-2: AWS Identity Security

- Identities
- Roles, Policies and access
- Multifactor Authentication
- Restricted authorization
- Federated Authentication
- Privileged Identity and Access Management

Module-3 AWS Infrastructure layer Security

- Securing VPC
- Securing Subnets
- Securing EC2 Instances
- Securing Containers and EKS (Kubernetes)

Module-4 AWS Storage layer Security

- Securing the Elastic Block Storage
- Securing the S3 Storage
- Securing EFS Storage

Module-5 AWS Load Balancing and Gateway Security

- Securing AWS Classic, Network and Application Load Balancers
- Securing AWS Network gateways (Internet, NAT, VPN and Direct Connect)
- Securing Cloud Front

Module-6 AWS Application Infrastructure

- Securing AWS Elastic Bean Stalk
- Securing AWS S3 Storage Static Web Application
- Configuring and managing PKI Infrastructure for AWS Applications

Module-7 AWS Security Information and event Management

- Identify AWS services that address attacks from external sources.
- Monitor, generate, and collect logs.
- Identify indicators of security incidents.
- Identify how to investigate threats and mitigate using AWS services.

-