Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Security Engineering on AWS

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **3 Day**

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.

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

Prerequisites

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

- AWS Cloud Practitioner Essentials
- AWS Security Fundamentals
- Architecting on AWS
- Working knowledge of IT security practices and infrastructure concepts
- Familiarity with cloud computing concepts

Who Should Attend

This course is intended for:

- Security engineers
- Security architects
- Security operations
- Information security

What You Will Learn

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

Outline

Intro

- Welcome and introductions
- Introduction to Security on AWS

Identifying entry points on AWS

- Ways to access the platform
- IAM policies
- Securing entry points
- Incident response

Lab - cross-account authentication

Security Considerations - Web Applications

- Security points in an AWS web application environment
- Analyse a three-tier application model and identify common threats
- Assess environments to improve security

Application Security

- Securing EC2 instances
- Assess vulnerabilities with Inspector
- Apply security in an automated way using Systems Manager
- Isolate a compromised instance

Lab - Assessing Security with Inspector and Systems Manager

Securing Networking Communications - Part 1

- Apply security best practices to VPC
- Implement an ELB device as a protection point
- Protect data in transit using certificates

Data Security

- Protect data at rest using encryption and access controls
- AWS services used to replicate data
- Protect archived data

Security Considerations: Hybrid Environments

- Security points outside of a VPC
- Common DoS threats

Monitoring and Collecting Logs on AWS

- Monitor events and collect logs with CloudWatch
- Use Config to monitor resources
- AWS-native services that generate and collect logs

Lab - Server Log Analysis Part 1 - collect logs

Processing Logs on AWS

- Stream and process logs for further analysis
- AWS services used to process logs from S3 buckets

Lab - Server Log Analysis Part 2 - analyse logs

Securing Networking Communications - Part 2

- Identify AWS services used to connect on-premise to AWS
- Data protection between on-premise and AWS
- Securely access VPC resources in other accounts

Out-Of-Region Protection

- Use Route 53 to isolate attacks
- Implement WAF to protect applications
- Use CloudFront to deliver content securely
- Protect applications using Shield

Account Management on AWS

- Manage multiple accounts
- Use identity providers / brokers to acquire access to AWS services

Lab - AWS Federated Authentication with ADFS

Security Considerations: Serverless Environments

- How to secure data in a serverless environment
- Use Cognito to authorize users
- Control API access with API Gateway
- Use AWS messaging services securely
- Secure Lambda functions

Lab - Monitor and Respond with Config and Lambda

Secrets Management on AWS

- Manage key and data encryption with KMS
- Describe how CloudHSM is used to generate and secure keys
- Use Secrets Manager to authenticate applications

Lab - Using KMS

Security Automation on AWS

- Deploy security-oriented AWS environments in a reproducible manner
- Provide management and control of IT services to end-users in a self-serve manner

Lab - Security Automation on AWS with Service Catalog

Threat Detection and Sensitive Data Monitoring

- Threat detection and monitoring for malicious or unauthorized behaviour
- Leverage machine learning to gain visibility into how sensitive data is being managed in the AWS Cloud