Security Engineering on AWS Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The training course provides advanced knowledge and hands-on experience for designing, implementing, and managing secure applications and cloud infrastructures on AWS. Based on AWS security best practices and recommended architectures, the course covers key areas including data protection, identity and access management, threat detection, incident response, and security operations.

Participants will gain expertise in the **AWS Shared Responsibility Model**, **Identity and Access Management (IAM)**, encryption, security monitoring, network security, threat mitigation, and security automation. The course demonstrates how to effectively use AWS security services to reduce risk, strengthen security controls, and protect cloud workloads against evolving cyber threats.

Through hands-on labs and real-world scenarios, learners will develop practical skills in detecting threats, responding to security incidents, maintaining compliance, and building secure, resilient cloud environments on AWS.

Prerequisites

Recommended prerequisites include:

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

Who Should Attend

This course is designed for:

- **Security Engineers**
- **Security Architects**
- **Security Operations Teams**
- **Information Security Professionals**
- **Cloud Security Engineers**
- **DevSecOps Professionals**
- IT professionals responsible for securing AWS environments

Security Engineering on AWS Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this training, you will have gained knowledge and skills in the following areas:

- Apply the **AWS Shared Responsibility Model**.
- Design AWS environments protected against common security threats.
- Protect data both at rest and in transit using encryption.
- Automate security checks and compliance assessments.
- Configure authentication and authorization mechanisms.
- Monitor security events and analyse logs.
- Detect and mitigate threats against applications and data.
- Perform security assessments and vulnerability reviews.
- Implement security automation and continuous compliance strategies.

Outline

Introduction to AWS Security

- AWS Security Fundamentals
- AWS Security Services
- AWS Shared Responsibility Model
- Identifying AWS Entry Points

Identity and Access Management

- **AWS Identity and Access Management (IAM)**
- IAM Policies
- Authentication Mechanisms
- Securing Access Points

Incident Response

- Incident Response Processes
- Cross-Account Authentication
- Security Event Handling

Web Application Security

- Security in AWS Web Applications
- Three-Tier Architecture Threat Analysis
- Security Improvement Strategies

Application Security

- Securing **Amazon EC2**
- **AWS Inspector**
- **AWS Systems Manager**
- Isolating Compromised Instances

Network Security

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Securing **Amazon VPC**
- **Elastic Load Balancing (ELB)**
- SSL/TLS Certificates
- Secure Data Transmission

Data Security

- Encryption Strategies
- Access Control Mechanisms
- Data Replication Services
- Archive Protection

Hybrid Environment Security

- Hybrid Cloud Security
- DoS and DDoS Threats
- Security Beyond the VPC

Monitoring and Logging

- **Amazon CloudWatch**
- **AWS Config**
- AWS Logging Services
- Security Event Monitoring

Log Processing and Analysis

- Log Processing Pipelines
- S3-Based Log Analysis
- Security Analytics

AWS and On-Premises Security

- Hybrid Connectivity Security
- Data Protection
- Cross-Account Access Controls

Out-of-Region Protection

- **Amazon Route 53**
- **AWS WAF**
- **Amazon CloudFront**
- **AWS Shield**

Account Management and Federation

- Multi-Account Management
- Federated Authentication
- Identity Providers and Brokers

Serverless Security

- **AWS Lambda**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- **Amazon Cognito**
- **Amazon API Gateway**
- AWS Messaging Services Security

Secrets Management

- **AWS Key Management Service (KMS)**
- **AWS CloudHSM**
- **AWS Secrets Manager**

Security Automation

- Security-Focused Infrastructure Deployment
- **AWS Service Catalog**
- Governance and Compliance Automation

Threat Detection and Sensitive Data Monitoring

- Threat Detection Strategies
- Malicious Activity Monitoring
- Machine Learning for Security Visibility
- Sensitive Data Protection and Monitoring