AWS Security Essentials Training

Duration: **1 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

The **{*training}** provides participants with a foundational understanding of the key security concepts required to build and operate secure cloud environments on AWS. The course focuses on the core components of AWS security, including identity and access management, data protection, network security, and security monitoring.

Based on the **AWS Shared Responsibility Model**, learners will gain a clear understanding of security responsibilities within AWS environments and discover how AWS security services can be used to meet organisational security requirements. Key topics include **AWS Identity and Access Management (IAM)**, data encryption, secure network access, logging, monitoring, and cloud security best practices.

Through practical examples and real-world scenarios, participants will develop the knowledge needed to implement foundational security controls, reduce security risks, and protect workloads operating in the AWS Cloud.

Prerequisites

Recommended prerequisites include:

- Working knowledge of IT security practices
- Familiarity with infrastructure concepts
- Basic understanding of cloud computing technologies

Who Should Attend

This course is intended for:

- **IT Security Professionals**
- **Cloud Security Engineers**
- **Security Analysts**
- **System Administrators**
- Business professionals interested in cloud security practices
- Individuals with limited AWS security experience
- Technical teams responsible for cloud security governance

AWS Security Essentials Training

Duration: **1 Day**

BILGINC 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:

- Identify security benefits and responsibilities within AWS Cloud environments.
- Explain the **AWS Shared Responsibility Model**.
- Understand AWS access control and identity management features.
- Apply data encryption methods to protect sensitive information.
- Secure network access to AWS resources.
- Identify AWS services used for security monitoring and logging.
- Select AWS security services aligned with organisational requirements.

AWS Security Essentials Training

Duration: **1 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Introduction to AWS Cloud Security

- Cloud Security Fundamentals
- AWS Security Overview
- Security and Compliance Concepts
- AWS Security Services

AWS Shared Responsibility Model

- AWS Responsibilities
- Customer Responsibilities
- Security Control Areas
- Governance and Compliance

Identity and Access Management

- **AWS Identity and Access Management (IAM)**
- Users, Groups, and Roles
- IAM Policies
- Security Best Practices

Data Security and Encryption

- Data Protection Strategies
- Encryption Methods
- Protecting Data in Transit
- Protecting Data at Rest

Network Security

- AWS Network Security Fundamentals
- Secure Connectivity
- Access Control Mechanisms
- Network Protection Layers

Security Logging and Monitoring

- Security Event Monitoring
- AWS Logging Services
- Security Auditing
- Threat Visibility and Analysis

AWS Security Services

- AWS Security Solutions
- Identity and Access Controls
- Data Protection Services
- Monitoring and Auditing Tools