Secure Cloud Resources with Microsoft Security Technologies (AZ-500) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The training prepares IT security professionals to implement advanced security controls within **Microsoft Azure** environments, manage vulnerabilities, and strengthen organisational security posture.

The course covers **Identity and Access Management (IAM)**, **Microsoft Entra ID**, **Platform Protection**, **Azure Network Security**, **Microsoft Defender for Cloud**, **Security Operations**, **Data Protection**, **Encryption**, and **Application Security**.

Participants will learn how to secure Azure environments, detect threats, and manage security operations using Microsoft security technologies.

This course prepares learners for the **Microsoft Certified: Azure Security Engineer Associate (AZ-500)** certification exam.

Participants develop expertise in Azure security, identity management, threat protection, and cloud security operations.

It is one of the most valuable Microsoft security training courses for professionals pursuing careers in cloud security and Azure security engineering.

Prerequisites

Participants should have:

- Experience as a **Microsoft Azure Administrator**
- Preferably **AZ-104** certification or equivalent knowledge
- At least one year of hands-on experience securing Azure workloads
- Knowledge of networking and identity management concepts

Secure Cloud Resources with Microsoft Security Technologies (AZ-500) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

This course is ideal for:

- **Azure Security Engineers**
- **Cloud Security Engineers**
- **Cyber Security Specialists**
- **Security Administrators**
- **Security Analysts**
- **SOC Analysts**
- **Azure Administrators**
- **Cloud Infrastructure Engineers**
- IT professionals responsible for Azure security

What You Will Learn

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

- Configure **Microsoft Entra ID**
- Implement secure access management in Azure environments
- Configure **Privileged Identity Management (PIM)**
- Secure Azure platforms and networks
- Use **Microsoft Defender for Cloud** for threat protection
- Monitor and respond to security incidents
- Implement data protection and encryption solutions
- Apply governance and compliance best practices

Outline

1. Identity and Access Management

Identity and Access Management (IAM)

Configuring identity and access controls for Azure environments.

Topics

- **Microsoft Entra ID**
- Azure Identity Management
- User and Group Management
- Authentication
- Authorization
- Conditional Access
- Multi-Factor Authentication (MFA)

Privileged Identity Management (PIM)

- Privileged Access Control

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Just-in-Time Access
- Role Management
- Risk Reduction Strategies

2. Platform Protection

Azure Platform Security

Implementing platform security controls across Azure environments.

Topics

- Cloud Security Fundamentals
- Azure Security Architecture
- Azure Subscription Security
- Resource Security
- Security Baselines

Azure Network Security

- Network Security Groups (NSG)
- Azure Firewall
- Azure DDoS Protection
- Private Endpoints
- Virtual Network Security

Host Protection

- VM Security
- Endpoint Protection
- Secure Configuration
- Hardening Techniques

3. Security Operations

Security Operations and Threat Protection

Managing security operations and detecting threats across Azure workloads.

Microsoft Defender for Cloud

- Defender for Cloud Configuration
- Secure Score
- Security Recommendations
- Compliance Dashboard

Security Monitoring

- Security Alerts
- Incident Response
- Threat Detection
- Security Analytics

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Security Baselines

- Establishing Security Standards
- Continuous Security Assessment
- Vulnerability Remediation

4. Data and Application Security

Protecting data and applications within Azure environments.

Data Protection

- Azure Data Security
- Data Encryption
- Encryption at Rest
- Encryption in Transit
- Key Management

Azure Storage Security

- Secure Storage Configuration
- Access Control
- Data Classification
- Data Protection Policies

Application Security

- Azure Application Security
- Secure Application Design
- Endpoint Security
- Application Access Control

Azure Security Best Practices

- Zero Trust Security
- Least Privilege Access
- Security Governance
- Compliance Management
- Security Monitoring
- Threat Protection