AZ-500: Microsoft Azure Security Engineer Associate

Level: Associate
Duration: 40–50 Hours

Course Overview

The **AZ-500: Microsoft Azure Security Engineer Associate** course is designed for professionals responsible for managing security in Azure environments. The course focuses on securing Azure identities, implementing platform protection, managing security operations, and ensuring data security. It prepares candidates for the **AZ-500 certification exam**.

Course Objectives

- Implement Azure security controls and threat protection
- Manage identity and access for Azure resources
- Configure and manage Azure network security
- Implement security monitoring and governance
- Prepare for the **AZ-500** certification exam

Course Outline

Module 1: Implementing Azure Identity and Access Management

- Managing Azure Active Directory (Azure AD) users and groups
- Implementing and managing role-based access control (RBAC)
- Configuring Azure AD identities and integrating with on-premises directories
- Securing identity and authentication using Multi-Factor Authentication (MFA)
- Implementing conditional access policies for security

Module 2: Implementing Azure Platform Protection

- Configuring Azure Firewall and managing network security groups (NSGs)
- Implementing network segmentation and virtual network peering

- Deploying and managing Azure Web Application Firewall (WAF)
- Configuring DDoS protection and Azure Bastion
- Implementing Azure Key Vault for secrets management

Module 3: Managing Azure Security Operations

- Implementing Microsoft Defender for Cloud for threat protection
- Configuring security alerts and monitoring using Azure Security Center
- Responding to security incidents and applying remediation actions
- Monitoring security events using Azure Sentinel and Security Information and Event Management (SIEM)
- Configuring Azure Security Center for compliance and regulatory reporting

---

Module 4: Implementing Security for Data and Applications

- Implementing encryption for data at rest and in transit
- Managing Azure Disk Encryption and Azure Storage Service Encryption
- Securing applications with Azure AD Authentication and Azure AD Application Proxy
- Protecting APIs using Azure API Management
- Implementing security for databases (Azure SQL, Cosmos DB) and storage solutions

---

Module 5: Configuring Azure Network Security

- Configuring network security for Azure Virtual Networks (VNets)
- Implementing network segmentation and virtual network security
- Managing traffic using Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Deploying and managing a Secure Virtual Private Network (VPN)
- Implementing hybrid network security using VPN Gateway and ExpressRoute

---

Module 6: Managing Security for Hybrid Cloud Environments

- Configuring and securing hybrid environments with Azure Arc
- Managing security for Azure AD, on-premises AD, and hybrid setups
- Implementing VPNs and ExpressRoute for hybrid connectivity
- Protecting multi-cloud environments with Azure Security Center
- Configuring hybrid cloud security solutions with Azure Sentinel

---

Module 7: Security Monitoring and Governance

- Implementing logging, monitoring, and auditing of Azure resources
- Configuring Azure Monitor and Application Insights for security
- Ensuring compliance using Azure Blueprints and Azure Policy
- Configuring alerts and automation for security incident management
- Managing identity and governance using Azure AD Identity Protection

---

Module 8: Exam Preparation and Practice

- Review of all modules and key topics
- Practice questions based on exam objectives
- Real-world scenarios and hands-on labs for practical knowledge
- Mock exam and exam tips to ensure exam success

Target Audience

- IT professionals responsible for security management in Azure
- Security engineers, architects, and administrators
- Candidates preparing for the **AZ-500** certification exam

Prerequisites

- Familiarity with networking concepts and security best practices
- Experience with Microsoft Azure services, especially networking and security
- Basic knowledge of PowerShell and command-line tools is beneficial