AZ-500T00: Microsoft® Azure® Security Technologies

Duration: 4 Days

Method: Instructor-Led Training (ILT) | Live Online Training

***Certification**: Microsoft Certified: Azure Security Engineer Associate —*
***Exam:** AZ-500: Microsoft Azure Security Technologies*

Course Description

This course provides participants with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities. This course also looks at security for identity and access, platform protection, data and applications, and security operations.

Target Audience

This course is intended for:

- Security Engineers

Prerequisites

To attend this course, candidates must have:

- Understanding of security's best practices and industry security requirements such as defence in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model.
- Familiarity with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead, the course content builds on that knowledge by adding security-specific information.
- Experience with Windows and Linux operating systems and scripting languages.

  ***NOTE:** Course labs may use PowerShell and CLI.*

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.
- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.
- Implement Azure Key Vault including certificates, keys, and secrets.
- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.
- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

Course Topics

Module 1: Manage Identity and Access

- Azure Active Directory
- Azure Identity Protection
- Enterprise Governance
- Azure AD Privileged Identity Management
- Hybrid Identity

Module 2: Implement Platform Protection

- Perimeter Security
- Network Security
- Host Security
- Container Security

Module 3: Secure Data and Applications

- Azure Key Vault
- Application Security
- Storage Security
- SQL Database Security

Module 4: Manage Security Operations

- Azure Monitor
- Azure Security Center
- Azure Sentinel

LABS INCLUDED