AZ-500T00 Microsoft Azure Security Technologies

Duration	Delivery Methods
4 Days	VILT, Private Group

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

Who Should Attend

This course is for Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

Agenda

1 - SECURE AZURE SOLUTIONS WITH AZURE ACTIVE DIRECTORY

- Explore Azure Active Directory features
- Self-managed Active Directory Domain Services, Azure Active Directory, and managed Azure Active Directory Domain Services
- Azure AD DS and self-managed AD DS

- Azure AD DS and Azure AD
- Investigate roles in Azure AD
- Azure AD built-in roles
- Deploy Azure AD Domain Services
- Create and manage Azure AD users
- Manage users with Azure AD groups
- Configure Azure AD administrative units
- Implement passwordless authentication
- Explore Try-This exercises

2 - IMPLEMENT HYBRID IDENTITY

- Deploy Azure AD connect
- Explore authentication options
- Configure Password Hash Synchronization (PHS)
- Implement Pass-through Authentication (PTA)
- Deploy Federation with Azure AD
- Explore the authentication decision tree
- Configure password writeback

3 - DEPLOY AZURE AD IDENTITY PROTECTION

- Explore Azure AD identity protection
- Configure risk event detections
- Implement user risk policy
- Implement sign-in risk policy
- Deploy multifactor authentication in Azure
- Explore multifactor authentication settings
- Enable multifactor authentication
- Implement Azure AD conditional access
- Configure conditional access conditions
- Implement access reviews
- Explore try-this exercises

4 - CONFIGURE AZURE AD PRIVILEGED IDENTITY MANAGEMENT

- Explore the zero trust model
- Review the evolution of identity management
- Deploy Azure AD privileged identity management
- Configure privileged identity management scope
- Implement privileged identity management onboarding
- Explore privileged identity management configuration settings
- Implement a privileged identity management workflow
- Explore Try-This exercises

5 - DESIGN AN ENTERPRISE GOVERNANCE STRATEGY

- Review the shared responsibility model
- Explore the Azure cloud security advantages
- Review Azure hierarchy of systems
- Configure Azure policies
- Enable Azure role-based access control (RBAC)
- Compare and contrast Azure RBAC vs Azure policies
- Configure built-in roles
- Enable resource locks
- Deploy Azure blueprints
- Design an Azure subscription management plan
- Explore Try-This exercises

6 - IMPLEMENT PERIMETER SECURITY

- Define defense in depth
- Explore virtual network security
- Enable Distributed Denial of Service (DDoS) Protection
- Configure a distributed denial of service protection implementation
- Explore Azure Firewall features
- Deploy an Azure Firewall implementation
- Configure VPN forced tunneling
- Create User Defined Routes and Network Virtual Appliances
- Explore hub and spoke topology
- Perform try-this exercises

7 - CONFIGURE NETWORK SECURITY

- Explore Network Security Groups (NSG)
- Deploy a Network Security Groups implementation
- Create Application Security Groups
- Enable service endpoints
- Configure service endpoint services
- Deploy private links
- Implement an Azure application gateway
- Deploy a web application firewall
- Configure and manage Azure front door
- Review ExpressRoute
- Perform try-this exercises

8 - CONFIGURE AND MANAGE HOST SECURITY

- Enable endpoint protection
- Define a privileged access device strategy
- Deploy privileged access workstations
- Create virtual machine templates
- Enable and secure remote access management

- Configure update management
- Deploy disk encryption
- Managed disk encryption options
- Deploy and configure Windows Defender
- Microsoft cloud security benchmark in Defender for Cloud
- Explore Microsoft Defender for Cloud recommendations
- Perform Try-This exercises

9 - ENABLE CONTAINERS SECURITY

- Explore containers
- Configure Azure Container Instances security
- Manage security for Azure Container Instances (ACI)
- Explore the Azure Container Registry (ACR)
- Enable Azure Container Registry authentication
- Review Azure Kubernetes Service (AKS)
- Implement an Azure Kubernetes Service architecture
- Configure Azure Kubernetes Service networking
- Deploy Azure Kubernetes Service storage
- Secure authentication to Azure Kubernetes Service with Active Directory
- Manage access to Azure Kubernetes Service using Azure role-based access controls

10 - DEPLOY AND SECURE AZURE KEY VAULT

- Explore Azure Key Vault
- Configure Key Vault access
- Review a secure Key Vault example
- Deploy and manage Key Vault certificates
- Create Key Vault keys
- Manage customer managed keys
- Enable Key Vault secrets
- Configure key rotation
- Manage Key Vault safety and recovery features
- Perform Try-This exercises
- Explore the Azure Hardware Security Module

11 - CONFIGURE APPLICATION SECURITY FEATURES

- Review the Microsoft identity platform
- Explore the Application model
- Register an application with App Registration
- Configure Microsoft Graph permissions
- Enable managed identities
- Azure App Services
- App Service Environment
- Azure App Service plan

- App Service Environment networking
- Availability Zone Support for App Service Environments
- App Service Environment Certificates
- Perform Try-This exercises

12 - IMPLEMENT STORAGE SECURITY

- Define data sovereignty
- Configure Azure storage access
- Deploy shared access signatures
- Manage Azure AD storage authentication
- Implement storage service encryption
- Configure blob data retention policies
- Configure Azure files authentication
- Enable the secure transfer required property
- Perform Try-This exercises

13 - CONFIGURE AND MANAGE SQL DATABASE SECURITY

- Enable SQL database authentication
- Configure SQL database firewalls
- Enable and monitor database auditing
- Implement data discovery and classification
- Microsoft Defender for SQL
- Vulnerability assessment for SQL Server
- SQL Advanced Threat Protection
- Explore detection of a suspicious event
- SQL vulnerability assessment express and classic configurations
- Configure dynamic data masking
- Implement transparent data encryption
- Deploy always encrypted features
- Deploy an always encrypted implementation
- Perform Try-This exercises

14 - CONFIGURE AND MANAGE AZURE MONITOR

- Explore Azure Monitor
- Configure and monitor metrics and logs
- Enable Log Analytics
- Manage connected sources for log analytics
- Enable Azure monitor Alerts
- Configure properties for diagnostic logging
- Perform try-this exercises

15 - ENABLE AND MANAGE MICROSOFT DEFENDER FOR CLOUD

- MITRE Attack matrix

EDUCATE 360
877.243.6690
info@educate360.com

- Implement Microsoft Defender for Cloud
- Security posture
- Workload protections
- Deploy Microsoft Defender for Cloud
- Azure Arc
- Azure Arc capabilities
- Microsoft cloud security benchmark
- Configure Microsoft Defender for Cloud security policies
- View and edit security policies
- Manage and implement Microsoft Defender for Cloud recommendations
- Explore secure score
- Define brute force attacks
- Understand just-in-time VM access
- Implement just-in-time VM access
- Perform try-this exercises

16 - CONFIGURE AND MONITOR MICROSOFT SENTINEL

- Enable Microsoft Sentinel
- Configure data connections to Sentinel
- Create workbooks to monitor Sentinel data
- Enable rules to create incidents
- Configure playbooks
- Hunt and investigate potential breaches