TechPledge®
Connect.Consult.Content

AZ-500 Azure Security Engineer Associate

Azure Security Engineers implement security controls and threat protection; manage identity and access; and protect data, applications, and networks in cloud and hybrid environments as part of end-to-end infrastructure.

Course Duration:

- 36 Hr.

Exam Preparation Duration:

- 8 Hr.

Course Material:

- Lectures (PDF)
- Lab Manual (PDF)
- Recorded Video

Abilities Validated by the Certification

- Managing Azure subscriptions and resources
- Implementing and managing Azure storage
- Deployment and management of the virtual machines (VMs)
- Configuration and management of the virtual networks
- Identity management

Detail Syllabus:

Configure Azure Active Directory for workloads

- Create App Registration
- Configure App Registration Permission Scopes
- Manage App Registration Permission Consent
- Configure Multi-Factor Authentication Settings
- Manage Azure AD Directory Groups
- Manage Azure AD Users
- Install and Configure Azure AD Connect
- Configure Authentication Methods
- Implement Conditional Access Policies

Configure Azure AD Privileged Identity Management

- Monitor Privileged Access
- Configure Access Reviews
- Activate Privileged Identity Management
- Create Access Package and assign the package

Configure Azure Tenant Security

- Transfer Azure Subscriptions Between Azure AD Management Group
- Manage API Access To Azure Subscriptions And Resources

Implement network security

- Configure Virtual Network Connectivity
- Configure Network Security Groups (NSG)
- Create and Configure Azure Front Door Service

- Create and Configure Application Security Groups
- Configure Remote Access Management
- Configure Baseline

Implement Host Security

- Configure Endpoint Security Within The VM
- Configure VM Security
- Harden Vms In Azure
- Configure System Updates For Vms In Azure
- Configure Baseline

Implement Azure Resource Management Security

- Create Azure Resource Locks
- Manage Resource Group Security
- Configure Azure Policies
- Configure Custom RBAC Roles
- Configure Subscription and Resource Permissions

Configure Security Services

- Configure Azure Monitor
- Configure Diagnostic Logging and Log Retention
- Configure Vulnerability Scanning
- Configure Centralized Policy Management By Using Azure Security Center
- Configure Just In Time VM Access By Using Azure Security Center

Configure Security for Data Infrastructure

- Enable Database Authentication
- Enable Database Auditing
- Configure Azure Sql Database Advanced Threat Protection
- Configure Access Control for Storage Accounts
- Configure Key Management for Storage Accounts
- Configure Azure Ad Authentication for Azure Storage

Configure Encryption for Data At Rest

- Implement Azure SQL Database Always Encrypted
- Implement Database Encryption
- Implement Storage Service Encryption
- Implement Disk Encryption

Configure application security

- Configure SSL/TLS Certs
- Configure Azure Services To Protect Web Apps
- Create An Application Security Baseline

Configure and Manage Key Vault

- Manage Access to Key Vault
- Manage Permissions to Secrets, Certificates, And Keys
- Configure RBAC Usage In Azure Key Vault

- Manage Certificates
- Manage Secrets
- Configure Key Rotation