Azure Cloud Security

Detailed Syllabus

Manage identity and access

Learning Objective

- **Understanding identity and access management Role in Security**

Topics Covered

- Manage Azure Active Directory Access
  - configure security for service principals
  - manage Azure AD directory groups
  - manage Azure AD users
  - configure password writeback
  - configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless
  - transfer Azure subscriptions between Azure AD tenants
- Configure secure access by using Azure AD
  - monitor privileged access for Azure AD Privileged Identity Management (PIM)
  - configure Access Reviews
  - activate and configure PIM
  - implement Conditional Access policies including Multi-Factor Authentication (MFA)
  - configure Azure AD identity protection
- Manage access control
  - configure subscription and resource permissions
  - configure resource group permissions
  - configure custom RBAC roles
  - identify the appropriate role
  - apply principle of least privilege
  - interpret permissions
  - check access

❑ Manage application access

- ❑ create App Registration
- ❑ configure App Registration permission scopes
- ❑ manage App Registration permission consent
- ❑ manage API access to Azure subscriptions and resources

Implement platform protection

Learning Objective

- ❖ **Understanding Platform Protection Role in Security**

Topics Covered

❑ Implement advanced network security

- ❑ secure the connectivity of virtual networks (VPN authentication, Express Route encryption)
- ❑ configure Network Security Groups (NSGs) and Application Security Groups (ASGs)
- ❑ create and configure Azure Firewall
- ❑ implement Azure Firewall Manager
- ❑ configure Azure Front Door service as an Application Gateway
- ❑ configure a Web Application Firewall (WAF) on Azure Application Gateway
- ❑ configure Azure Bastion
- ❑ configure a firewall on a storage account, Azure SQL, KeyVault, or App Service
- ❑ implement Service Endpoints
- ❑ implement DDoS protection

❑ Configure advanced security for compute

- ❑ configure endpoint protection
- ❑ configure and monitor system updates for VMs
- ❑ configure authentication for Azure Container Registry
- ❑ configure security for different types of containers
- ❑ implement vulnerability management
- ❑ configure isolation for AKS
- ❑ configure security for container registry
- ❑ implement Azure Disk Encryption
- ❑ configure authentication and security for Azure App Service
- ❑ configure SSL/TLS certs
- ❑ configure authentication for Azure Kubernetes Service
- ❑ configure automatic updates

Manage security operations

Learning Objective

- **Understanding security operations**

Topics Covered

❑ Monitor security by using Azure Monitor

- ❑ create and customize alerts
- ❑ monitor security logs by using Azure Monitor
- ❑ configure diagnostic logging and log retention

❑ Monitor security by using Azure Security Center

- ❑ evaluate vulnerability scans from Azure Security Center
- ❑ configure Just in Time VM access by using Azure Security Center
- ❑ configure centralized policy management by using Azure Security Center
- ❑ configure compliance policies and evaluate for compliance by using Azure Security Center

❑ Monitor security by using Azure Sentinel

- ❑ create and customize alerts
- ❑ configure data sources to Azure Sentinel
- ❑ evaluate results from Azure Sentinel
- ❑ configure workflow automation by using Azure Sentinel

❑ Configure security policies

- ❑ configure security settings by using Azure Policy
- ❑ configure security settings by using Azure Blueprint
- ❑ configure a playbook by using Azure Sentinel

Secure data and applications

Learning Objective

- **Understanding security operations**

Topics Covered

❑ Configure security for storage

- ❑ configure access control for storage accounts
- ❑ configure key management for storage accounts
- ❑ configure Azure AD authentication for Azure Storage
- ❑ configure Azure AD Domain Services authentication for Azure Files
- ❑ create and manage Shared Access Signatures (SAS)
- ❑ create a shared access policy for a blob or blob container
- ❑ configure Storage Service Encryption
- ❑ configure Azure Defender for Storage
- ❑ configure Storage Service Encryption
- ❑ configure Azure Defender for Storage

❑ Configure security for databases

- ❑ enable database authentication
- ❑ enable database auditing
- ❑ configure Azure Defender for SQL
- ❑ configure Azure Defender for SQL
- ❑ configure Azure SQL Database Advanced Threat Protection
- ❑ implement database encryption
- ❑ implement Azure SQL Database Always Encrypted

❑ 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
- ❑ backup and restore of Key Vault items
- ❑ configure Azure Defender for Key Vault