Azure Security Training

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and continuously identify and remediate vulnerabilities by using a variety of security tools. It focuses on securing identity, platforms, data, applications, and operations in Azure. The training aligns with the Microsoft Certified: Azure Security Engineer Associate certification exam (AZ-500)

Course Outline

Module 1: Secure Identity and Access

Lessons

- Manage security controls for identity and access
    - Manage Azure built-in role assignments
    - Manage custom roles, including Azure roles and Microsoft Entra roles
    - Plan and manage Azure resources in Microsoft Entra Privileged Identity Management (PIM), including settings and assignments
    - Implement multi-factor authentication (MFA) for access to Azure resources
    - Implement Conditional Access policies for cloud resources in Azure
- Manage Microsoft Entra application access
    - Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants
    - Manage Microsoft Entra app registrations
    - Configure app registration permission scopes
    - Manage app registration permission consent
    - Manage and use service principals
    - Manage managed identities

Labs

- Implementing PIM and role assignments
- Configuring Conditional Access policies
- Managing app registrations and service principals

Module 2: Secure Networking

Lessons

- Plan and implement security for virtual networks
    - Plan and implement Network Security Groups (NSGs) and

Application Security Groups (ASGs)

- Manage virtual networks by using Azure Virtual Network Manager
- Plan and implement user-defined routes (UDRs)
- Plan and implement Virtual Network peering or VPN gateway
- Plan and implement Virtual WAN, including secured virtual hub
- Secure VPN connectivity, including point-to-site and site-to-site
- Implement encryption over ExpressRoute
- Configure firewall settings on Azure resources
- Monitor network security by using Network Watcher

- Plan and implement security for private access to Azure resources
  - Plan and implement virtual network Service Endpoints
  - Plan and implement Private Endpoints
  - Plan and implement Private Link services
  - Plan and implement network integration for Azure App Service and Azure Functions
  - Plan and implement network security configurations for an App Service Environment (ASE)
  - Plan and implement network security configurations for an Azure SQL Managed Instance
- Plan and implement security for public access to Azure resources
  - Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management
  - Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies
  - Plan and implement an Azure Application Gateway
  - Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
  - Plan and implement a Web Application Firewall (WAF)
  - Recommend when to use Azure DDoS Protection Standard

Labs

- Configuring NSGs and ASGs
- Implementing Private Endpoints and Private Link
- Deploying Azure Firewall and Application Gateway

Module 3: Secure Compute, Storage, and Databases

Lessons

- Plan and implement advanced security for compute
  - Plan and implement remote access to virtual machines,

including Azure Bastion and just-in-time (JIT)

- Configure network isolation for Azure Kubernetes Service (AKS)
- Secure and monitor AKS
- Configure authentication for AKS
- Configure security monitoring for Azure Container Instances (ACIs)
- Configure security monitoring for Azure Container Apps (ACAs)
- Manage access to Azure Container Registry (ACR)
- Configure disk encryption, including Azure Disk Encryption (ADE), encryption at host, and confidential disk encryption
- Recommend security configurations for Azure API Management

- Plan and implement security for storage
  - Configure access control for storage accounts
  - Manage storage account access keys
  - Select and configure an appropriate method for access to Azure Files
  - Select and configure an appropriate method for access to Azure Blob Storage
  - Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage
  - Configure Bring your own key (BYOK)
  - Enable double encryption at the Azure Storage infrastructure level
- Plan and implement security for Azure SQL Database and Azure SQL Managed Instance
  - Enable Microsoft Entra database authentication
  - Enable database auditing
  - Plan and implement dynamic data masking
  - Implement Transparent Data Encryption (TDE)
  - Recommend when to use Azure SQL Database Always Encrypted

Labs

- Securing AKS clusters and containers
- Configuring storage encryption and access controls
- Implementing SQL database security features like TDE and auditing

Module 4: Secure Data and Applications

Lessons

- Identify Azure data protection mechanisms
  - Configure security policies to manage data
  - Configure security for data infrastructure

    - Configure encryption for data at rest and in transit
- Implement application security
    - Understand application security concepts
    - Implement security for application lifecycle (development, deployment, operations)
    - Secure applications using Azure security features, including endpoint security
    - Configure and manage Azure Key Vault for secrets management
- Manage security operations for data and apps
    - Configure Microsoft Defender for Cloud for data and app protection
    - Implement threat protection and vulnerability management

Labs

- Configuring Key Vault and secret management
- Implementing application security in App Service
- Using Defender for Cloud to assess data and app security

Module 5: Manage Security Operations

Lessons

- Configure security services and policies
    - Configure Microsoft Defender for Cloud
    - Configure security policies using Azure Policy and Blueprints
- Manage and respond to security alerts
    - Manage security alerts and recommendations
    - Respond to and remediate security issues using Defender for Cloud
- Create and manage security baselines
    - Develop regulatory compliance baselines
    - Configure workflow automation for compliance

Labs

- Setting up Defender for Cloud and policies
- Responding to security incidents and alerts
- Creating custom security baselines