AZ-500T00: Microsoft Azure Security Technologies

Course Outline

1) Secure identity and access

- Manage security controls for identity and access
  - Secure user identities in Microsoft Entra ID by implementing strong authentication and access management controls
  - Protect groups and access management by enforcing security measures to prevent unauthorized changes or misuse
  - Manage external identities securely by defining policies that ensure confidentiality, integrity, and proper access control
  - Implement Microsoft Entra ID Protection to detect, investigate, and mitigate identity-related security threats
  - Apply Conditional Access policies to enforce security controls based on user behavior, device compliance, and contextual risks
- Manage Microsoft Entra application access
  - Manage enterprise application access in Microsoft Entra ID, including OAuth permission grants for access control
  - Govern application integration with identity platforms through Microsoft Entra ID app registrations
  - Configure app registration permission scopes for appropriate resource access levels
  - Manage app registration consent and use service principals and managed identities for automated management and enhanced security

2) Secure networking

- Plan and implement security for virtual networks
  - Implement security measures for Azure virtual networks to safeguard data and resources
  - Utilize NSGs and ASGs for network traffic security, and manage UDRs for optimal traffic routing
  - Establish secure network connectivity through Virtual Network peering, VPN gateways, and Virtual WAN
  - Enhance network security with VPN configurations, ExpressRoute encryption, PaaS firewall settings, and Network Watcher monitoring
- Plan and implement security for private access to Azure resources
  - Develop security strategies for private access to Azure resources to protect sensitive data
  - Utilize virtual network Service Endpoints and Private Endpoints for secure Azure service access
  - Manage Private Link services for secure resource exposure and integrate Azure App Service and Functions with virtual network
  - Configure network security for App Service Environment and Azure SQL Managed Instance to safeguard web applications and databases
- Plan and implement security for public access to Azure resources
  - Develop strategies for secure public access to Azure resources, preventing

unauthorized access and breaches
    - Implement TLS for Azure App Service and API Management to encrypt data in transit
    - Protect network traffic with Azure Firewall and Application Gateway for optimized web application security and delivery
    - Enhance web app performance with Azure Front Door and CDN, and deploy WAF and DDoS Protection for robust defense against attacks

3) Secure compute, storage, and databases

- Plan and implement advanced security for compute
    - Enhance Azure compute resources' security against vulnerabilities and attacks with advanced measures
    - Secure remote access via Azure Bastion and JIT VM access, and implement network isolation for AKS
    - Strengthen AKS clusters' security, monitor Azure Container Instances and Apps, and manage access to Azure Container Registry
    - Implement disk encryption methods like ADE and manage API access securely in Azure API Management
- Plan and implement security for storage
    - Develop security strategies for Azure storage resources, ensuring data protection during rest and transit
    - Manage storage account access with effective access control and secure key lifecycle management
    - Tailor access methods for Azure Files, Blob Storage, Tables, and Queues to specific use cases
    - Strengthen data security with soft delete, backups, versioning, immutable storage, BYOK, and double encryption
- Plan and implement security for Azure SQL Database and Azure SQL Managed Instance
    - Implement security for Azure SQL Managed Instance to safeguard sensitive data
    - Use Microsoft Enterprise Identity for database authentication and conduct database auditing for compliance
    - Utilize Microsoft Purview for data governance and classification to protect sensitive information
    - Apply dynamic masking and Transparent Database Encryption, and recommend Always Encrypted for client-side data protection

4) Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel

- Implement and manage enforcement of cloud governance policies
    - Enforce compliance using Azure Policy to create and manage security policies
    - Streamline secure infrastructure deployment with Azure Blueprint
    - Utilize landing zones for consistent Azure security and manage sensitive data with Azure Key Vault
    - Enhance key security with HSM recommendations, effective access control, and regular key rotation and backup processes

- Manage security posture by using Microsoft Defender for Cloud
    - Utilize Microsoft Defender for Cloud Secure Score and Inventory to identify and mitigate security risks, enhancing overall security posture
    - Assess and align with security frameworks using Microsoft Defender for Cloud to ensure adherence to security standards and best practices
    - Integrate specific industry and regulatory standards into Microsoft Defender for Cloud for tailored compliance
    - Connect hybrid and multicloud environments to Microsoft Defender for Cloud for centralized security management, and monitor external assets to safeguard against external threats
- Configure and manage threat protection by using Microsoft Defender for Cloud
    - Master the configuration of Microsoft Defender for Cloud to effectively monitor and protect cloud resources
    - Implement advanced threat detection strategies using Microsoft Defender for Cloud's built-in capabilities
    - Utilize Microsoft Defender for Cloud's threat intelligence to proactively identify and mitigate security risks
    - Configure and fine-tuning security policies within Microsoft Defender for Cloud to align with organizational security requirements
    - Develop expertise in incident response and remediation using Microsoft Defender for Cloud's integrated tools and features
- Configure and manage security monitoring and automation solutions
    - Use Azure Monitor for effective security event monitoring in cloud environments
    - Implement data connectors in Microsoft Sentinel for comprehensive security data collection
    - Develop customized analytics rules in Microsoft Sentinel for targeted threat detection
    - Assess and automate responses to security incidents in Microsoft Sentinel to enhance workflow efficiency

5) LAB Outline

- Role Based Access Control
- Network Security Groups and Application Security Groups
- Azure Firewall
- Configuring and Securing ACR and AKS
- Securing Azure SQL Database
- Service Endpoints and Securing Storage
- Key Vault (Implementing Secure Data by setting up Always Encrypted)
- Azure Monitor
- Microsoft Defender for Cloud
- Microsoft Sentinel