AZ-500T00: Microsoft Azure Security Technologies

Course Details

Course Code: AZ-500T00

Duration: 4 days

Notes:

- This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.
- Course content, prices, and availability are subject to change without notice.
- Terms and Conditions apply

Elements of this syllabus are subject to change.

About this course

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.

Audience Profile

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.

Academy IT Pty Ltd
Level 4, 45 Grenfell Street
ADELAIDE 5000

Email: sales@academyit.com.au
Web: www.academyit.com.au

Phone: 08 7324 9800
Brian: 0400 112 083

Manage identities in Microsoft Entra ID

This module focuses on effectively managing identities and enhancing security in Microsoft Entra ID, ensuring that users, groups, and external identities are protected against security threats and unauthorized access.

Learning objectives

By the end of this module, participants are able to:

- Enhance security in Microsoft Entra ID to safeguard user identities and accounts.
- Implement security for group management in Microsoft Entra ID for effective access control.
- Advise on the secure management of external identities in Microsoft Entra ID.
- Utilize Microsoft Entra ID Protection for proactive threat detection and response.

Manage authentication by using Microsoft Entra ID

This module is designed to provide administrators with the knowledge and skills needed to manage authentication effectively using Microsoft Entra ID, ensuring secure access to resources and enhancing user experience.

Learning objectives

By the end of this module, participants are able to:

- Implement multifactor and passwordless authentication for enhanced security and convenience.
- Enforce password protection measures and single sign-on for simplified, secure access.
- Integrate SSO with identity providers and endorse modern authentication protocols.
- Set up Microsoft Entra Verified ID for trusted identity verification.

Manage authorization by using Microsoft Entra ID

This module is designed to provide administrators with the knowledge and skills required to effectively manage authorization using Microsoft Entra ID, ensuring that users have the appropriate access to resources and data.

Learning objectives

By the end of this module, participants will be able to:

- Set Azure role permissions across management groups, subscriptions, and resources for access control.
- Assign built-in roles in Microsoft Entra ID and Azure for predefined user permissions.
- Create custom roles in Azure and Microsoft Entra ID to match organizational access needs.
- Manage Entra Permissions, Privileged Identity Management, and Conditional Access for refined control and compliance.

Manage application access in Microsoft Entra ID

This module covers managing application access in Microsoft Entra ID, including controlling enterprise app access, managing app registrations and permissions, utilizing service principals, and configuring the Microsoft Entra Application Proxy for secure access.

Learning objectives

By the end of this module, participants are able to:

- 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.

Plan and implement security for virtual networks

This module is designed to provide administrators with the knowledge and skills needed to plan and implement robust security measures for Azure virtual networks, ensuring the confidentiality, integrity, and availability of network resources.

Learning objectives

- 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

This module focuses on equipping administrators with the knowledge and skills required to plan and implement robust security measures for private access to Azure resources, safeguarding sensitive data and enhancing network integrity.

Learning objectives

- 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 networks.
- 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

This module empowers admins to plan and implement strong security for Azure resources, ensuring app/service confidentiality, integrity, and availability.

Learning objectives

- 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.

Plan and implement advanced security for compute

This module is designed to provide administrators with the knowledge and skills needed to plan and implement advanced security measures for Azure compute resources, safeguarding applications and data against evolving security threats.

Learning objectives

By the end of this module, participants will be able to:

- 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

This module is designed to provide administrators with the knowledge and skills required to plan and implement comprehensive security measures for Azure storage resources, safeguarding data integrity, confidentiality, and availability.

Learning objectives

By the end of this module, participants will be able to:

- 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

This module is designed to empower administrators with the knowledge and skills needed to plan and implement robust security measures for Azure SQL Database and Azure SQL Managed Instance, ensuring data protection and regulatory compliance.

Learning objectives

By the end of this module, participants will be able to:

- 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.

Plan, implement, and manage governance for security

This module focuses on enabling administrators to effectively plan, implement, and manage security governance in Azure, ensuring compliance with organizational policies and best practices.

Learning objectives

By the end of this module, participants will be able to:

- 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

This module teaches administrators to manage and improve cloud security using Microsoft Defender for Cloud, focusing on proactive risk identification and remediation.

Learning objectives

By the end of this module, you will be able to:

- 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

This module focuses on configuring and managing security monitoring and automation solutions using Azure Monitor and Microsoft Sentinel, enabling organizations to proactively identify and respond to security incidents in their cloud environment.

Learning objectives

By the end of this module, participants will be able to:

- Utilize Azure Monitor for comprehensive monitoring of cloud security events.
- Aggregate diverse security data efficiently with data connectors in Microsoft Sentinel.
- Detect threats using customized analytics rules in Microsoft Sentinel.

- Assess and automate incident responses in Microsoft Sentinel for enhanced security management.

Configure and manage security monitoring and automation solutions

This module teaches how to set up and manage security tools with Azure Monitor and Microsoft Sentinel. It helps organizations quickly find and deal with security issues in their cloud setup.

Learning objectives

By the end of this module, participants are able to:

- 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.