COURSE OUTLINE

MS-AZ500T00: MICROSOFT AZURE SECURITY TECHNOLOGIES

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
4 Days	Intermediate	Azure	Instructor-led	NA

INTRODUCTION

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.

PREREQUISITES

Successful learners will have prior knowledge and understanding of:

- Security best practices and industry security requirements such as defence in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model.
- Azure services, particularly Azure Active Directory and Azure Virtual Networks.
- Cloud computing concepts, including the differences between Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- Windows and Linux operating systems and scripting languages.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.

COURSE CONTENT

Module 1: Manage security controls for identity and access

This module focuses on effectively managing security controls in Microsoft Entra ID by securing identities, authentication, and authorization to protect users, groups, and external identities against threats while ensuring secure and seamless access to resources.

Lessons

- Introduction
- Microsoft cloud security benchmark: Identity management and privileged access
- What is Microsoft Entra ID?
- Secure Microsoft Entra users
- Create a new user in Microsoft Entra ID
- Secure Microsoft Entra groups
- Recommend when to use external identities
- Secure external identities
- Implement Microsoft Entra Identity Protection
- Microsoft Entra Connect
- Microsoft Entra Cloud Sync
- Authentication options
- Password hash synchronization with Microsoft Entra ID
- Microsoft Entra pass-through authentication
- Federation with Microsoft Entra ID
- What is Microsoft Entra authentication?
- Kerberos authentication
- New Technology Local Area Network Manager (NTLM)
- Passwordless authentication options for Microsoft Entra ID
- Implement passwordless authentication
- Implement password protection
- Microsoft Entra ID single sign-on
- Implement single sign-on (SSO)
- Integrate single sign-on (SSO) and identity providers
- Introduction to Microsoft Entra Verified ID
- Configure Microsoft Entra Verified ID
- Recommend and enforce modern authentication protocols
- Azure management groups
- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources

- Azure role-based access control
- Azure built-in roles
- Assign Azure role permissions for management groups, subscriptions, resource groups, and resources
- Microsoft Entra built-in roles
- Assign built-in roles in Microsoft Entra ID
- Microsoft Entra role-based access control
- Create and assign a custom role in Microsoft Entra ID
- Microsoft Entra permissions management
- Implement and manage Microsoft Entra permissions management
- Zero Trust security
- Microsoft Entra Privileged Identity Management
- Configure Privileged Identity Management
- Microsoft Entra ID governance
- Identity lifecycle management
- Lifecycle workflows
- Entitlement management
- Delegation and roles in entitlement management
- Access reviews
- Configure role management and access reviews by using Microsoft Entra ID governance
- Implement Conditional Access policies
- Knowledge check
- Summary

After completing this course, students will be able to:

- 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.

Module 2: Manage Microsoft Entra application access

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.

Lessons

- Introduction.
- Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants.
- Manage app registrations in Microsoft Entra ID.
- Configure app registration permission scopes.
- Manage app registration permission consent.
- Manage and use service principals.
- Manage managed identities for Azure resources.
- Recommend when to use and configure a Microsoft Entra Application Proxy, including authentication.
- Knowledge check.

After completing this course, students will be 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.

Module 3: 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.

Lessons

- Introduction
- Microsoft Cloud Security Benchmark: Data Protection, Logging and Threat Detection, and
- Network Security
- What is an Azure Virtual Network
- Azure Virtual Network Manager
- Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Plan and implement User-Defined Routes (UDRs)
- Plan and implement Virtual Network peering or gateway
- Plan and implement Virtual Wide Area Network, including secured virtual hub
- Secure VPN connectivity, including point-to-site and site-to-site
- Azure encryption
- What is Azure Virtual Network encryption
- Azure ExpressRoute
- Implement encryption over ExpressRoute
- Configure firewall settings on Azure resources
- Monitor network security by using Network Watcher
- Knowledge check
- Summary

After completing this module, students will be able to:

- 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

Module 4: 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.

Lessons

- Introduction.
- 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.

- Knowledge check.

After completing this module, students will be able to:

- 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.

Module 5: 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.

Lessons

- Introduction.
- Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management.
- Plan, implement, and manage an Azure Firewall, Azure Firewall Manager and firewall policies.
- Plan and implement an Azure Application Gateway.
- Plan and implement a Web Application Firewall (WAF).
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN).
- Recommend when to use Azure DDoS Protection Standard.
- Knowledge check.

After completing this module, students will be able to:

- 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.

Module 6: 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.

Lessons

- Introduction.
- Plan and implement remote access to public endpoints, Azure Bastion and just-in-time (JIT) virtual machine (VM) access.
- Configure network isolation for Azure Kubernetes Service (AKS).
- Secure and monitor Azure Kubernetes Service.
- Configure authentication for Azure Kubernetes Service.
- Configure security for Azure Container Instances (ACIs).
- Configure security for Azure Container Apps (ACAs).
- Manage access to Azure Container Registry (ACR).
- Configure disk encryption, Azure Disk Encryption (ADE), encryption as host, and confidential disk encryption.
- Recommend security configurations for Azure API Management.
- Knowledge check.

After completing this module, students 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.

Module 7: 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.

Lessons

- Introduction.
- Azure Storage.
- Configure access control for storage accounts.
- Manage life cycle for 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 an appropriate method for access to Azure Tables.
- Select and configure an appropriate method for access to Azure Queues.
- 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.
- Knowledge check.

After completing this module, students 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.

Module 8: 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.

Lessons

- Introduction.
- Azure SQL Database and SQL Managed Instance security.
- Enable database authentication by using Microsoft Entra ID.
- Enable and monitor database audit.

- Identify use cases for the Microsoft Purview governance portal.
- Implement data classification of sensitive information by using the Microsoft Purview governance portal.
- Plan and implement dynamic mask.
- Implement transparent data encryption.
- Recommend when to use Azure SQL Database Always Encrypted.
- Knowledge check.

After completing this module, students 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.

Module 9: Implement and manage enforcement of cloud governance policies

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

Lessons

- Introduction
- Microsoft cloud security benchmark: Access, Data, Identity, Network, Endpoint, Governance, Recovery, Incident, and Vulnerability Management
- Azure governance
- Create, assign, and interpret security policies and initiatives in Azure Policy
- Azure Blueprints
- Configure security settings by using Azure Blueprint
- Deploy secure infrastructures by using a landing zone
- Azure Key Vault
- Azure Key Vault security
- Azure Key Vault authentication
- Create and configure an Azure Key Vault
- Recommend when to use a dedicated Hardware Security Module (HSM)
- Configure access to Key Vault, including vault access policies and Azure role-based access control
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys
- Implement security controls to protect backups
- Implement security controls for asset management
- Knowledge check
- Summary

After completing this course, students 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.

Module 10: 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.

Lessons

- Introduction.
- Implement Microsoft Defender for Cloud
- Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory
- Assess compliance against security frameworks and Microsoft Defender for Cloud
- Add industry and regulatory standards to Microsoft Defender for Cloud
- Add custom initiatives to Microsoft Defender for Cloud
- Connect hybrid cloud and multicloud environments to Microsoft Defender for Cloud
- Identify and monitor external assets by using Microsoft Defender External Attack Surface Management
- Knowledge check.

After completing this module, students 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.

Module 11: Configure and manage threat protection by using Microsoft Defender for Cloud

This module focuses on the essential techniques for configuring and managing threat protection exclusively with Microsoft Defender for Cloud, empowering cybersecurity specialists to strengthen the security posture of their cloud environments.

Lessons

- Introduction.
- Enable workload protection services in Microsoft Defender for Cloud
- Defender for Servers
- Defender for Storage
- Malware scanning in Defender for Storage
- Detect threats to sensitive data
- Deploy Microsoft Defender for Storage
- Enable configure Azure built-in policy
- Configure Microsoft Defender plans for Servers, Databases, and Storage
- Implement and manage Microsoft Defender Vulnerability Management
- Log Analytics workspace
- Manage data retention in a Log Analytics workspace
- Deploy the Azure Monitor Agent
- Collect data with Azure Monitor Agent
- Data collection rules (DCRs) in Azure Monitor
- Transformations in data collection rules (DCRs)
- Monitor network security events and performance data by configuring data collection rules (DCRs) in Azure Monitor
- Connect your Azure subscriptions
- Just-in-time machine access
- Enable just-in-time access
- Container security in Microsoft Defender for Containers

- Managed Kubernetes threat factors
- Defender for Containers architecture
- Configure Microsoft Defender for Containers components
- Microsoft Defender for Cloud DevOps Security
- DevOps Security support and prerequisites
- DevOps environment security posture
- Connect your GitHub lab environment to Microsoft Defender for Cloud
- Configure the Microsoft Security DevOps GitHub action
- Defender for Cloud AI threat protection
- Enable threat protection for AI workloads in Defender for Cloud
- Gain application and end-user context for AI alerts
- Knowledge check
- Summary

After completing this module, students will be able to:

- 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.

Module 12: 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.

Lessons

- Introduction
- Manage and respond to security alerts in Microsoft Defender for Cloud
- Configure workflow automation by using Microsoft Defender for Cloud
- Log retention plans in Microsoft Sentinel
- Alerts and Incidents from Microsoft Sentinel
- Configure data connectors in Microsoft Sentinel
- Enable analytics rules in Microsoft Sentinel
- Configure automation in Microsoft Sentinel
- Automating Threat Response with Microsoft Sentinel
- Knowledge check
- Summary

After completing this module, students will be 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.

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the Microsoft AZ-500: Microsoft Azure Security Technologies exam.