

Secure cloud resources with Microsoft security technologies

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy
Get Your Free Copy Now

Course Number: AZ-500T00

Duration: 4 days

Overview

Course Description

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.

Skills Gained

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.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.
- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.
- Implement Azure Key Vault including certificates, keys, and secrets.
- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.
- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

Prerequisites

Successful learners will have prior knowledge and understanding of:

- Security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model.
- Be familiar with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.

- Have experience with Windows and Linux operating systems and scripting languages. Course labs may use PowerShell and the CLI.

Prerequisite courses (or equivalent knowledge and hands-on experience):

This free online training will give you the experience you need to be successful in this course.

- AZ-104: Manage identities and governance in Azure - Learn | Microsoft Docs
- AZ-104: Implement and manage storage in Azure - Learn | Microsoft Docs
- AZ-104: Configure and manage virtual networks for Azure administrators - Learn | Microsoft Docs
- AZ-104: Monitor and back up Azure resources - Learn | Microsoft Docs
- AZ-104: Deploy and manage Azure compute resources - Learn | Microsoft Docs

Audience

Course Details

Outline

- Manage security controls for identity and access
 - 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?
 - Implement multifactor authentication (MFA)
 - 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
- 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 for Cloud Resources in Azure
- Azure lighthouse overview
- Module assessment
- Manage Microsoft Entra application access

- 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
 - Module assessment
- Plan and implement security for virtual networks
 - 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
 - Module assessment
- 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
- Module assessment
- 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, 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
 - Module assessment
- Plan and implement advanced security for compute
 - Plan and implement remote access to public endpoints, Azure Bastion and just-in-time (JIT) virtual machine (VM) access
 - What is Azure Kubernetes Service?
 - 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
 - Module assessment
- Plan and implement security for storage
 - 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 Blobs
- 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
- Module assessment
- Plan and implement security for Azure SQL Database and Azure SQL Managed Instance
 - Azure SQL Database and SQL Managed Instance security
 - Enable Microsoft Entra database authentication
 - 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
 - Implement an Azure SQL Database firewall
 - Module assessment
- Implement and manage enforcement of cloud governance policies
 - 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
 - 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
- Module assessment
- Manage security posture by using Microsoft Defender for Cloud
 - 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
 - Implement and use Microsoft Defender External Attack Surface Management
 - Module assessment
- Configure and manage threat protection by using Microsoft Defender for Cloud
 - 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
- Exercise - Configuring Microsoft Defender for Cloud for Enhanced Protection
- Knowledge check
- Configure and manage security monitoring and automation solutions
 - 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
 - Module assessment