March 2023

Azure Security Engineer Learning Pathway

www.aka.ms/pathways

Getting started

Responsibilities for an Azure Security Engineer include managing the security posture, identifying and remediating vulnerabilities, performing threat modelling, implementing threat protection, and responding to security incident escalations. Azure Security Engineers often serve as part of a larger team to plan and implement cloud-based management and security.

Microsoft Learn

- Build your Tech resilience
- New to the Cloud or Azure? Start with Azure Fundamentals
- New to Security? Continue with Microsoft Security, Compliance, and Identity Fundamentals
- Microsoft Trust Centre
- Compliance
- What is Azure Security Center?
- Azure Monitor – Security & Audit Dashboard
- Introduction to Azure security
- Introduction to key Azure network security services
- Microsoft Security Blog
- Microsoft Security YouTube Channel
- Intro to data protection and privacy regulations

Doing More

- Threat Modeling Security Fundamentals
- Secure your infrastructure with threat modelling
- Protect identity and access with Azure Active Directory
- Implement Windows Server IaaS VM Identity
- Secure your cloud data
- Architect secure infrastructure in Azure
- Azure security best practices and patterns
- Develop a security and compliance plan

Additional Study

Manage identity and access:

- What is Azure Active Directory?
- Built-in roles for Azure Resources
- Create and manage users
- Create and manage groups
- Choose the right authentication method for your Azure Active Directory hybrid identity solution
- What is password hash synchronization
- Implement password hash synchronization with Azure AD Connect sync
- Azure Active Directory Pass-through Authentication: Technical deep dive
- Azure Active Directory Pass-through Authentication: Quickstart
- Azure Active Directory pricing
- Create an Azure AD tenant and configure registration for your application
- Azure Active Directory consent framework
- What are managed identities for Azure resources?
- Protect against security threats on Azure
- Delegate access to Privileged Identity Management
- Configure Azure AD role settings in Privileged Identity Management
- Building a Conditional Access policy
- Assign Azure AD roles in Privileged Identity Management
- What is Azure AD Multi-Factor Authentication?
- Create an access review of groups and applications in Azure AD access reviews
- Create an access review of Azure AD roles in Privileged Identity Management
- What is Azure RBAC?
- Understand the difference between Azure roles and Azure AD roles
- Create or update Azure custom roles using the Azure portal
- Use resource locks to protect resources

Implement Platform Protection:

- Protect against security threats on Azure
- Use network security groups to control network access
- Network security groups
- Create, change, or delete a network security group
- Azure Firewall features
- Deploy and configure Azure Firewall
- What is Azure Web Application Firewall on Azure Application Gateway?
- What is Azure Front Door?
- What is Azure Bastion?
- Tutorial: Configure Bastion and connect to a Windows VM through a browser
- Secure network access to PaaS services with virtual network service endpoints
- Endpoint protection assessment and recommendations in Security Center
- Implement vulnerability management
- Update Management overview
- Add a TLS/SSL certificate in Azure App Service
- Container security in Security Center
- Access and identity options for Azure Kubernetes Service (AKS)
- Authenticate with an Azure container registry
- Network concepts for applications in Azure Kubernetes Service (AKS)

Manage Security Operations:

- Features of Azure Monitor logs
- Explore the different alert types that Azure Monitor supports
- Create, view, and manage log alerts
- Configuring diagnostic logging and log retention
- Monitor your security status with Security Center recommendations
- Centralized policy management
- Manage security policies
- Vulnerability Scanner
- Exercise - Enable JIT VM access
- Tutorial: Protect your resources with Azure Security Center
- What is Azure Sentinel?
- Tutorial: Detect threats out-of-the-box
- Sentinel - Connect data sources
- Automatically create incidents from Microsoft security alerts
- Tutorial: Investigate incidents with Sentinel
- Use playbooks with automation rules
- What is Azure Policy?
- Tutorial: Create and manage policies to enforce compliance
- Tutorial: Create a custom policy definition
- Tutorial: Create and manage policies to enforce compliance
- What is Azure Blueprints?
- Create and assign blueprints

Secure Data and Operations:

- Azure Storage Overview
- Authorizing access to data in Azure Storage
- Delegate access with a shared access signature
- Encryption
- What is Azure Key Vault?
- Key rotation
- Azure Key Vault security
- Quickstart: Create a key vault using the Azure portal
- Create an Azure SQL Database baseline
- Server-level vs. database-level auditing policy
- Create an Azure SQL Database baseline
- Azure Defender for SQL
- Authorize database access to SQL Database, SQL Managed Instance, and Azure Synapse Analytics
- Manage transparent data encryption
- Configure Always Encrypted by using Azure Key Vault

Role Based Certification

Azure Security Engineer

AZ-500 Microsoft Azure Security Technologies

Skills measured:

- Manage identity and access (25–30%)
- Secure networking (20–25%)
- Secure compute, storage, and databases (20–25%)
- Manage security operations (25–30%)

Microsoft Learn:

- Manage Identity and Access
- Implement Platform Protection
- Secure your data and applications
- Manage Security Operation

Exam Skills Outline | Course Page | Exam Page

Exam Sandbox | Practice Test | Security Documentation

Learn Live

Azure Core IaaS Study Hall
Learn about highly secure, available, and scalable cloud services. Running through to June 2023.

On demand library: Watch all previous shows on demand HERE

Microsoft Virtual Training Days

Build the technical skills you need with free Virtual Training Days.

Click Here