January 2024

Azure Security Engineer Learning Pathway (1/2)

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.

Security Documentation

- 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

Security Engineer Skill Assessment

Unlock Your Potential as a Security Engineer or Elevate Your Skills! Take our exclusive assessment to discover your strengths, uncover growth opportunities, and receive personalized learning path recommendations. Supercharge your career today!.

Click Here

Learning Paths from Microsoft Learn

Implement resource management security in Azure START
Learn how to secure resources using policy, role-based access control, and other Azure services.

Architect secure infrastructure in Azure START
earn about the tools and services available on Azure to ensure your resources are secure.

Manage identities and governance for Azure administrators START
Learn how to manage users, subscriptions, role-based access control (RBAC), and governance in Azure.

Secure your cloud data START
Azure was designed for security and compliance. Learn how to leverage the built-in services to store your app data securely to ensure that only authorized services and clients have access to it.

Microsoft Azure Well-Architected Framework – Security START
Learn how to incorporate security into your architecture design, and Discover the tools that Azure provides to help you create a secure environment.

Secure Azure AI services START
Securing Azure AI services can help prevent data loss and privacy violations for user data that may be a part of the solution.

Microsoft Applied Skill START
Implement security through a pipeline using Azure DevOps

Manage identity and access in Microsoft Entra ID START
Learn how to work with subscriptions, users, and groups by configuring Microsoft Entra ID for workloads.

Microsoft Applied Skill START
Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Role Based Certification

Azure Security Engineer

AZ-500 Microsoft Azure Security Technologies

Skills measured
- Manage identity and access
- Secure networking
- Secure compute, storage, and databases
- Manage security operations

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

Course Page

Practice Assessment

Security Documentation

Exam Skills Outline

Exam Sandbox

Exam Page

Microsoft Learn/Documentation

- Threat Modeling Security Fundamentals
- Secure your infrastructure with threat modelling
- Manage identity and access in Microsoft Entra ID
- Implement Windows Server IaaS VM Identity
- Azure security best practices and patterns
- Develop a security and compliance plan

Azure Security Engineer Learning Pathway (2/2)

www.aka.ms/pathways

Microsoft Learn/Documentation

Manage identity and access

- What is Microsoft Entra ID?
- Built-in roles for Azure Resources
- Create and manage users
- Create and manage groups
- Choose the right authentication method for your Microsoft Entra hybrid identity solution
- What is password hash synchronization
- Implement password hash synchronization with Microsoft Entra Connect sync
- Microsoft Entra Pass-through Authentication: Technical deep dive
- Microsoft Entra Pass-through Authentication: Quickstart
- Microsoft Entra Plans and Pricing
- OpenID connect on the Microsoft identity platform
- Consent experience for applications in Microsoft Entra ID
- What are managed identities for Azure resources?
- Protect against security threats on Azure
- Delegate access to Privileged Identity Management
- Configure Entra role settings in Privileged Identity Management
- Building a Conditional Access policy
- Assign Entra roles in Privileged Identity Management
- What is Microsoft Entra Multi-Factor Authentication?

Manage identity and access

- Create an access review of groups and applications in Microsoft Entra ID
- Create an access review of Azure resource and Entra roles in PIM
- What is Azure RBAC?
- Understand the difference between Azure roles and Microsoft Entra 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

Implement Platform Protection

- 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?

Manage Security Operations

- 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