AZ-500: Azure Security Engineer Course Outline

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

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 plays an integral role in protecting an organization's data.

Prerequisites

To get the most out of this course students should:

- Understand 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. This course will use PowerShell and the CLI.

To get ready for class, consider this free online training.

- Azure Fundamentals
- AZ-104: Prerequisites for Azure Administrators

Course Objectives

After completing the 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.

AZ-500: Azure Security Engineer Course Outline

- 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.

Course Outline

Lesson 01 - Azure Active Directory

- Azure AD Features
- Azure AD vs AD DS
- Roles for Azure AD
- Azure AD Domain Services
- Azure AD Users
- Azure AD Groups
- Azure MFA Concepts
- Enabling MFA
- MFA Settings
- Demonstrations (Navigating Azure, Users and Groups, MFA)

Lesson 02 – Azure AD Identity Protection

- Azure AD Identity Protection Features
- Risk Events
- User Risk Policy
- Sign-in Risk Policy

- Azure AD Conditional Access
- Conditional Access Conditions
- Access Reviews
- Demonstration (Azure AD Identity Protection)
- Lab 04 – MFA, Conditional Access, Identity Protection

Lesson 03 – Enterprise Governance Security

- Shared Responsibility Model
- Azure Cloud Security Advantages
- Azure Hierarchy
- Azure Policies
- Azure RBAC
- Azure RBAC vs Azure Policies
- Built-in Roles for Azure
- Resource Locks
- Azure Blueprints
- Azure Subscription Management
- Demonstrations (RBAC, Resource Locks)
- Lab 01 – RBAC
- Lab 02 – Azure Policy
- Lab 03 – Resource Manager Locks

Lesson 04 – Azure AD Privileged Identity Management

- Zero Trust model
- Identity Management
- Azure AD Privileged Identity Management
- PIM Scope
- PIM Onboarding
- PIM Configuration Settings
- PIM Workflow
- Demonstration (PIM)
- Lab 05 - PIM

Lesson 05 – Hybrid Identity

- Azure AD Connect
- Authentication Options
- Password Hash Synchronization (PHS)
- Pass-through Authentication (PTA)
- Federation with AD
- Password Writeback
- Authentication Decision Tree
- Lab 06 - Implement Directory Synchronization

AZ-500: Azure Security Engineer Course Outline

Module 02: Implement Platform Protection

Lesson 01 – Perimeter Security

- Defense in Depth
- Virtual Network Security
- Distributed Denial of Service
- DDoS Implementation
- Azure Firewall Features
- Firewall Implementation
- VPN Forced Tunneling
- Demonstrations (VNet Peering, Azure Firewall)
- Lab 08 – Azure Firewall

Lesson 02 – Network Security

- Network Security Groups (NSG)
- NSG Implementation
- Application Security Groups
- Service Endpoints and Private Links
- Azure Application Gateway
- Web Application Firewall
- Azure Front Door
- UDRs and NVAs
- ExpressRoute
- Demonstrations: (Storage Endpoints, Network Security Groups, Application Security Groups, Front Door)
- Lab 07 – Network and Application Security Groups

Lesson 03 - Host Security

- Endpoint Protection
- Privileged Access Workstations
- Virtual Machine Templates
- Remote Access Management
- Update Management
- Disk Encryption
- Windows Defender
- Security Center Host Recommendations
- Securing Azure Workloads
- Demonstrations (Bastion, VM updates, VM extensions, Disk Encryption, RDP connections (optional), SSH connections (optional))

Lesson 04 – Container Security

- Containers
- ACI Security
- Azure Container Instances (ACI)

- Azure Container Registry (ACR)
- ACR Authentication
- Azure Kubernetes Service (AKS)
- AKS Terminology
- AKS Architecture
- AKS Networking
- AKS Storage
- AKS and Active Directory
- Lab 09 – Configuring and Securing ACR and AKS

Module 03: Data and Applications

Lesson 01 - Azure Key Vault

- Azure Key Vault Features
- Key Vault Access
- Key Vault Example
- Key Vault Certificates
- Key Vault Keys
- Customer Managed Keys
- Key Vault Secrets
- Key Vault Rotation
- Demonstrations (Create a Key Vault, Settings, Access Policies)

Lesson 02 - Application Security

- Microsoft Identity Platform
- Azure AD Application Scenarios
- App Registration
- Microsoft Graph Permissions
- Managed Identities
- Web App certificates
- Demonstration (App registration)
- Lab 10 – Key Vault and App Registration

Lesson 03 - Storage Security

- Data Sovereignty
- Azure Storage Access
- Shared Access Signatures
- Azure AD Storage Authentication
- Storage Service Encryption
- Blob Data Retention Policies
- Azure File Authentication
- Secure Transfer Required

- Demonstrations (SAS, Storage Explorer Key Rollover, Blob Storage Access Policies, AD Authentication, Storage Endpoints (optional))
- Lab 12 – Service Endpoints and Securing Storage

Lesson 04 - SQL Database Security

- SQL Database Authentication
- SQL Database Firewalls
- Database Auditing
- Data Discovery and Classification
- Vulnerability Assessment
- Advanced Threat Protection (ATP)
- Dynamic Data Masking (DDM)
- Transparent Data Encryption (TDE)
- Always Encrypted (AE)
- Demonstrations (SQL DB diagnostics, Advanced Data Security, AD Authentication)
- Lab 11 – Securing Azure SQL Database

Module 04: Manage Security Operations

Lesson 01 - Azure Monitor

- Azure Monitor
- Metrics and Logs
- Log Analytics
- Connected Sources
- Azure Monitor Alerts
- Diagnostic Logging
- Demonstration (Alerts, Log Analytics)
- Lab 13 – Azure Monitor

Lesson 02 - Azure Security Center

- Cyber Kill Chain
- Azure Security Center
- Security Center Policies
- Security Center Recommendations
- Secure Score
- Brute Force Attacks
- Just in Time Virtual Machine Access
- Demonstrations (Recommendations, Policies, Regulatory Compliance)
- Lab 14 – Azure Security Center

Lesson 03 - Azure Sentinel

- Azure Sentinel
- Data Connections

- Workbooks
- Incidents
- Playbooks
- Hunting
- Lab 15 - Azure Sentinel