Microsoft Azure Security Technologies

Duration	Delivery Method	Level
4 days	Online / Instructor Led	Advanced

Introduction:

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organisation'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 specialise in providing security for Azure-based digital platforms and play an integral role in protecting an organisation's data.

Pre-requisites:

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.
- 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.

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.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronisation.
- 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 secretes.
- 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 Centre including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

Course Content

Module 1: Manage Identity and Access

- Azure Active Directory
- Hybrid Identity
- Azure Identity Protection
- Azure AD Privileged Identity Management
- Enterprise Governance

Module 2: Implement Platform Protection

- Perimeter Security

- Network Security
- Host Security
- Container Security

Module 3: Secure Data and Applications

- Azure Key Vault
- Application Security
- Storage Security
- SQL Database Security

Module 4: Manage Security Operations

- Azure Monitor
- Azure Security Centre
- Azure Sentinel