Azure Security Technologies

Length: 4 days
Format: Bootcamp
Time: Day

About This Course

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.

Required Exams

Microsoft Azure Security Technologies

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.

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 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 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 Center including policies, recommendations, and just in time virtual machine access.
* Implement Azure Sentinel including workbooks, incidents, and playbooks.

Outline

Module 1: Manage Identity and Access

This module covers Azure Active Directory, Azure Identity Protection, Enterprise Governance, Azure AD PIM, and Hybrid Identity.