Microsoft Azure Security Technologies

(MOC AZ-500)

Course 22916 - 32 Hours

Overview

In this course students will gain the knowledge and skills needed to implement security controls, maintain the security posture, and identify and remediate vulnerabilities by using a variety of security tools. The course covers scripting and automation, virtualization, and cloud N-tier architecture.

On Completion, Delegates will be able to

- Describe specialized data classifications on Azure
- Identify Azure data protection mechanisms
- Implement Azure data encryption methods
- Secure Internet protocols and how to implement them on Azure
- Describe Azure security services and features

Who Should Attend

Students should have at least one year of hands-on experience securing Azure workloads and experience with security controls for workloads on Azure.

Prerequisites

Before attending this course, students must have knowledge of:

- Microsoft Azure Administrator Associate

Course Contents

Module 1: Manage Identity and Access

Gone are the days when security focused on a strong perimeter defense to keep malicious hackers out. Anything outside the perimeter was treated as hostile, whereas inside the wall, an organization's systems were trusted. Today's security posture is to assume breach and use the Zero Trust model. Security professionals no longer focus on perimeter defense. Modern organizations have to support access to data and services evenly from both inside and outside the corporate firewall. This module will serve as your roadmap as you start building more security into your Azure solutions.

- Configure Azure AD PIM
- Configure and manage Azure Key Vault
- Configure Azure AD for Azure workloads
- Security for an Azure subscription

Module 2: Implement Platform Protection

We know that security is job one in the cloud and how important it is that you find accurate and timely information about Azure security. One of the best reasons to use Azure for your applications and services is to take advantage of its wide array of security tools and capabilities. These tools and capabilities help make it possible to create secure solutions on the secure Azure platform.

- Understand cloud security
- Azure networking
- Secure the network
- Implementing host security
- Implement platform security
- Implement subscription security

Module 3: Secure Data and applications

Azure security for data and applications offers a comprehensive solution that helps organizations take full advantage of the promise of cloud applications while maintaining control with improved visibility into activity. It also increases protection of critical data across cloud applications. With tools to help uncover Shadow IT, assess risk, enforce policies, investigate activities and stop threats, organizations can safely move to the cloud while maintaining control of critical data.

- Configure security policies to manage data
- Configure security for data infrastructure
- Configure encryption for data at rest
- Understand application security
- Implement security for application lifecycle
- Secure applications

Module 4: Manage Security Operations

Azure provides security mechanisms to aid administrators who manage Azure cloud services and virtual machines. These mechanisms include: Authentication and role-based access control. Monitoring, logging, and auditing. Certificates and encrypted communications. A web management portal.

- Configure security services
- Configure security policies using Azure Security Center
- Manage security alerts
- Respond to an remediation of security issues
- Create security baselines