MICROSOFT PARTNER OF THE YEAR
INSOMEA
COMPUTER SOLUTIONS
2020 BAHRAIN - 2021 • 2022 TUNISIA
2023 TUNISIA • BAHRAIN

Training Course AZ-500: Microsoft Azure Security Technologies

Overview: 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.

Duration: 4 Days.

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.

Certification: This course prepares you for the AZ-500: Microsoft Azure Security Technologies.

Course Objectives: After completing this course, students will be able to:

- Secure Azure solutions with Azure Active Directory.
- Implement Hybrid identity.
- Deploy Azure AD identity protection.
- Configure Azure AD privileged identity management.
- Design an enterprise governance strategy.
- Implement perimeter security.
- Configure network security.
- Configure and manage host security.
- Enable Containers security.
- Deploy and secure Azure Key Vault.
- Configure application security features.
- Implement storage security.
- Configure and manage SQL database security.
- Configure and manage Azure Monitor.
- Enable and manage Microsoft Defender for Cloud.
- Configure and monitor Microsoft Sentinel.

Course Outline:

1- Secure Azure solutions with Azure Active Directory.
   - Configure Azure AD and Azure AD Domain Services for security.
   - Create users and groups that enable secure usage of your tenant.
   - Use MFA to protect user's identities.

- Configure passwordless security options.

2- Implement Hybrid identity.
- Deploy Azure AD Connect
- Pick and configure that best authentication option for your security needs
- Configure password writeback.

3- Deploy Azure AD identity protection.
- Deploy and configure Identity Protection.
- Configure MFA for users, groups, and applications.
- Create Conditional Access policies to ensure your security.
- Create and follow an access review process.

4- Configure Azure AD privileged identity management.
- Describe Zero Trust and how it impacts security.
- Configure and deploy roles using Privileged Identity Management (PIM).
- Evaluate the usefulness of each PIM setting as it relates to your security goals.

5- Design an enterprise governance strategy.
- Explain the shared responsibility model and how it impacts your security configuration.
- Create Azure policies to protect your solutions.
- Configure and deploy access to services using RBAC.

6- Implement perimeter security.
- Define defense in depth.
- Protect your environment from denial-of-service attacks.
- Secure your solutions using firewalls and VPNs.
- Explore your end-to-end perimeter security configuration based on your security posture.

7- Configure network security.
- Deploy and configure network security groups to protect your Azure solutions.
- Configure and lockdown service endpoints and private links.
- Secure your applications with Application Gateway, Web App Firewall, and Front Door.
- Configure ExpressRoute to help protect your network traffic.

8- Configure and manage host security.
- Configure and deploy Endpoint Protection.
- Deploy a privileged access strategy for devices and privileged workstations.
- Secure your virtual machines and access to them.
- Deploy Windows Defender.
- Practice layered security by reviewing and implementing Security Center and Security Benchmarks.

9- Enable Containers security.
- Define the available security tools for containers in Azure.
- Configure security settings for containers and Kubernetes services.
- Lock down network, storage, and identity resources connected to your containers.
- Deploy RBAC to control access to containers.

10- Deploy and secure Azure Key Vault.
- Define what a key vault is and how it protects certificates and secrets.
- Deploy and configure Azure Key Vault.
- Secure access and administration of your key vault.

- Store keys and secrets in your key vault.
- Explore key security considers like key rotation and backup / recovery.

11- Configure application security features.

- Register an application in Azure using app registration.
- Select and configure which Azure AD users can access each application.
- Configure and deploy web app certificates.

12- Implement storage security.

- Define data sovereignty and how that is achieved in Azure.
- Configure Azure Storage access in a secure and managed way.
- Encrypt your data while it is at rest and in transit.
- Apply rules for data retention.

13- Configure and manage SQL database security.

- Configure which users and applications have access to your SQL databases.
- Block access to your servers using firewalls.
- Discover, classify, and audit the use of your data.
- Encrypt and protect your data while is it stored in the database.

14- Configure and manage Azure Monitor.

- Configure and monitor Azure Monitor.
- Define metrics and logs you want to track for your Azure applications.
- Connect data sources to and configure Log Analytics.
- Create and monitor alerts associated with your solutions security.

15- Enable and manage Microsoft Defender for Cloud.

- Define the most common types of cyber-attacks.
- Configure Azure Security Center based on your security posture.
- Review Secure Score and raise it.
- Lock down your solutions using Security Center and Defender.
- Enable Just-in-Time access and other security features.

16- Configure and monitor Microsoft Sentinel.

- Explain what Azure Sentinel is and how it is used.
- Deploy Azure Sentinel.
- Connect data to Azure Sentinel, like Azure Logs, Azure AD, and others.
- Track incidents using workbooks, playbooks, and hunting techniques.