Microsoft Azure Security Technologies – Intensive Training («AZ500»)

This AZ-500 training takes place in an intensive format where you have full day sessions with our MCT experts.

Duration: 4 days
Price: 2'550.–
Course documents: Official Microsoft Courseware and Microsoft Learn
Vendor code: AZ-500

Content

The content of this intensive training is derived from the exam «AZ-500: Microsoft Azure Security Technologies». Start preparing for the course on Microsoft Learn now and use the Learning Support if you have any questions. During the intensive training days with the instructor you will work with the official Microsoft course material (more information under «Methodology & didactics»).

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.

Lessons

- 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
Security is job one in the cloud and it's important 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.

Lessons

- 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.

Lessons

- 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 as well as a web management portal.

Lessons

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

Key Learnings

- Describing specialized data classifications on Azure
- Identifying Azure data protection mechanisms
- Implementing Azure data encryption methods
- Securing Internet protocols and how to implement them on Azure
- Describing Azure security services and features

Target audience

Students with at least one year of hands-on experience securing Azure workloads and experience with security controls for workloads on Azure interested in expanding their knowledge of Azure's security features and possibilities.

Requirements

- 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. Course labs may use PowerShell and the CLI.

- Microsoft Azure Fundamentals (Hands-on) – Intensive Training («A900IC»)
- Microsoft Azure Fundamentals – Flexible Training («AZ900V»)

Certification

This intensive training prepares you for:

- **Exam:** «AZ-500: Microsoft Azure Security Technologies» for the
- **Certification:** «Microsoft Certified: Azure Security Engineer Associate»

Additional information

The two workshops SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel and SC-5002: Secure Azure Services and Workloads with Microsoft Defender for Cloud Regulatory Compliance Controls are integrated into this course.

Further courses

- Microsoft Cybersecurity Architect – Intensive Training («SC100»)

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-microsoft-technology/microsoft-azure/microsoft-certified-azure-security-engineer-associate/course-microsoft-azure-security-technologies-intensive-training-az-500