Secure cloud resources with Microsoft security technologies (AZ-500T00)

ID AZ-500T00 **Price** CHF 3,380.—(excl. VAT) **Duration** 4 days

Who should attend

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.

This course is part of the following Certifications

Microsoft Certified: Azure Security Engineer Associate (MCASEA)

Prerequisites

Successful learners will have prior knowledge and understanding of:

- 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.

Prior attendance of the course Microsoft Azure Administrator (AZ-104T00) is recommended.

Course Objectives

- 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.

Course Content

Module 1: Manage Identity and Access

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

Lessons

- Azure Active Directory
- Azure Identity Protection
- Enterprise Governance
- Azure AD Privileged Identity Management
- Hybrid Identity
- Lab: Role-Based Access Control
- Lab: Azure Policy
- Lab: Resource Manager Locks
- Lab: MFA, Conditional Access and AAD Identity Protection
- Lab: Azure AD Privileged Identity Management
- Lab: Implement Directory Synchronization

After completing this module, 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.

Module 2: Implement Platform Protection

This module covers perimeter, network, host, and container security.

Lessons

- Perimeter Security
- Network Security
- Host Security
- Container Security
- Lab: Network Security Groups and Application Security Groups
- Lab: Azure Firewall
- Lab: Configuring and Securing ACR and AKS

After completing this module, students will be able to:

- 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.

Module 3: Secure Data and Applications

This module covers Azure Key Vault, application security, storage security, and SQL database security.

Lessons

- Azure Key Vault
- Application Security
- Storage Security
- SQL Database Security
- Lab: Key Vault (Implementing Secure Data by setting up Always Encrypted)
- Lab: Securing Azure SQL Database
- Lab: Service Endpoints and Securing Storage

After completing this module, students will be able to:

- 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.

Module 4: Manage Security Operations

This module covers Azure Monitor, Azure Security Center, and Azure Sentinel.

Lessons

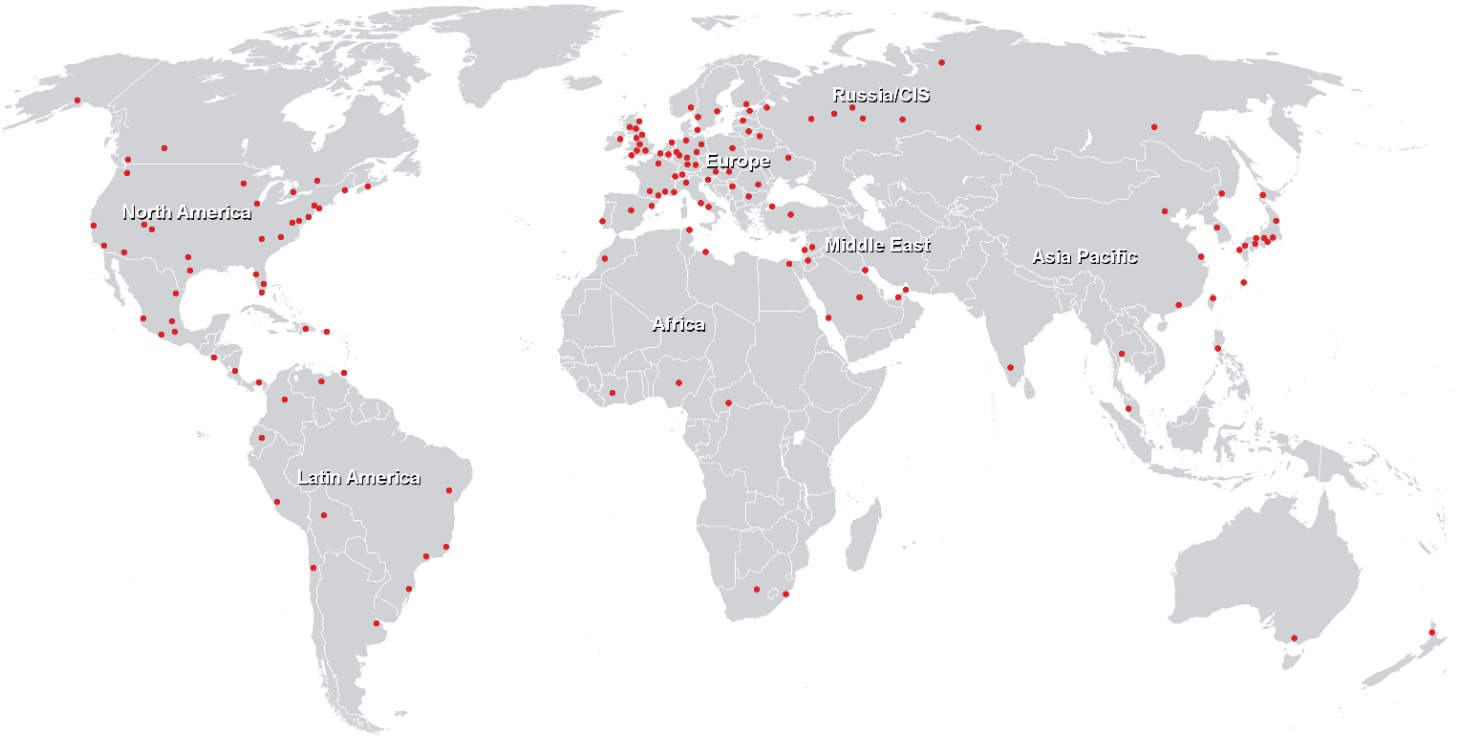
- Azure Monitor
- Azure Security Center
- Azure Sentinel
- Lab: Azure Monitor
- Lab: Azure Security Center
- Lab: Azure Sentinel

After completing this module, students will be able to:

- 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.

Microsoft Solutions Partner
Microsoft Cloud Training Services

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch