+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on September 14, 2026

Sign Up

Microsoft Cloud and AI Security Engineer Associate (SC-500) Training

Formerly AZ-500

4 days (28 hours)

Overview

The Microsoft Cloud and AI Security Engineer Associate training prepares you to secure identities, data, cloud infrastructure, and new AI workloads in Azure, hybrid, and multicloud environments.

You'll learn how to protect access with Microsoft Entra ID, secure networks, compute resources, storage, and databases, and then apply security and compliance policies tailored to cloud environments.

The course covers the latest security challenges related to AI applications and agents. You'll explore how to protect data, agent-based identities, and workloads using Microsoft Foundry and Copilot Studio, as well as the controls needed to reduce their attack surface.

You'll also learn how to assess and improve your security posture with Microsoft Defender for Cloud and how to use Microsoft tools to monitor, investigate, and prioritize risks in cloud and AI environments.

Upon completion of the course, you will be able to implement an end-to-end security strategy and prepare for the Microsoft Certified: Cloud and AI Security Engineer Associate certification.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Secure identities and access with Microsoft Entra ID
- Protect Azure networks, data, and computing resources
- Implement a Cloud Security Posture Management approach
- Secure applications, workloads, and AI agents in the Microsoft ecosystem
- Monitor and prioritize risks with Microsoft security solutions
- Prepare for the Microsoft Cloud and AI Security Engineer Associate certification

Target Audience

- Cloud security engineers
- Azure security engineers
- Cloud security administrators
- IAM Engineers
- Cloud Security Consultants

Prerequisites

- Have hands-on experience administering Microsoft Azure
- Understand the fundamentals of Azure networking, storage, and compute resources
- Proficiency in identity and access management principles using Microsoft Entra ID
- Understand the fundamentals of cloud security and the shared responsibility model
- Knowledge of Microsoft 365 and hybrid environments is recommended

Technical Prerequisites

- Computer running Windows 10 or 11, macOS, or Linux, with at least 8 GB of RAM
- A Microsoft work account associated with a Microsoft Entra ID training tenant

Curriculum for our Microsoft Cloud and AI Security Engineer Associate certification training

[Day 1 - Morning]

Securing Identities and Access with Microsoft Entra

- Apply Zero Trust principles to identity and access management in Azure
- Configure multi-factor authentication, passwordless methods, and conditional access policies
- Administer Azure RBAC roles and Microsoft Entra ID roles according to the principle of least privilege
- Secure privileged access with Privileged Identity Management (PIM) and Just-In-Time mechanisms
- Protect application identities, Managed Identities, OAuth authorizations, and workload access

- Control the identities used by applications and AI agents in the Microsoft ecosystem

[Day 1 - Afternoon]

Protect secrets and enforce cloud governance

- Administer Azure Key Vault to protect secrets, keys, and certificates
- Configure permissions, secret rotation, and the use of managed identities
- Implement Azure Policy to enforce security and compliance requirements
- Evaluate recommendations, regulatory standards, and configuration discrepancies with Microsoft Defender for Cloud
- Apply governance principles to Azure, hybrid, and multicloud resources
- Hands-on workshop: Securing privileged identities, protecting secrets, and enforcing a compliance policy across the entire environment

[Day 2 - Morning]

Securing Azure Networks and Communications

- Segment networks with NSG, ASG, and Azure Virtual Network Manager
- Configure Azure Firewall and communication filtering policies
- Protect connections with VPN, Virtual WAN, and private access mechanisms
- Use Private Endpoint and Private Link to limit public exposure of Azure services
- Secure access to internal applications and resources with private connectivity mechanisms
- Analyze traffic flows and identify network configurations that increase the attack surface

[Day 2 - Afternoon]

Protect storage, databases, and sensitive data

- Secure Azure Storage with RBAC, SAS, encryption, and network restrictions
- Configure client-managed keys and mechanisms for protecting sensitive data
- Protect Azure SQL with Microsoft Entra authentication, encryption, auditing, and network restrictions
- Use Microsoft Defender to strengthen protection for storage services and databases
- Implement immutability and mechanisms designed to protect against modification or deletion
- Hands-on workshop: Isolate data services from the production environment and secure their access, communications, and secrets

[Day 3 - Morning]

Securing Compute and Application Platforms

- Hardening virtual machines with Secure Boot, vTPM, and workload protection mechanisms
- Implement vulnerability management, endpoint protection, and recommendations from Microsoft Defender for Servers
- Secure Azure application services and limit their network exposure
- Protect containerized environments, image registries, and cloud-native workloads
- Configure managed identities and secure access to resources from applications
- Identify and correct misconfigurations affecting compute security

[Day 3 - Afternoon]

Securing workloads, applications, and AI agents

- Identify risks specific to AI applications and agents: sensitive data, identities, permissions, and connected tools
- Assess the security posture of data used by AI solutions using Microsoft capabilities Purview
- Secure the identities and permissions used by intelligent agents and applications
- Apply security controls to solutions developed with Microsoft Foundry and Microsoft Copilot Studio
- Implement the necessary safeguards and protection mechanisms for interactions with external models and tools
- Hands-on workshop: Analyze an agent-based application, identify its exposure to data and tools, and then define appropriate security controls

[Day 4 - Morning]

Manage cloud, hybrid, and multicloud security posture

- Configure Microsoft Defender for Cloud and use the Secure Score to prioritize remediation actions
- Implement Cloud Security Posture Management (CSPM) features
- Assess vulnerabilities, exposed secrets, misconfigurations, and attack vectors
- Verify resource compliance with standards and regulatory requirements
- Extend posture management and workload protection to hybrid, AWS, and GCP environments
- Prioritize recommendations based on risk, exposure, and impact on workloads

[Day 4 - Afternoon]

Monitor security and prepare for the Cloud and AI Security Engineer Associate certification

- Centralize and analyze security signals from cloud resources, identities, and workloads

- Use Microsoft Sentinel and Microsoft Defender XDR to investigate alerts and incidents
- Leverage Microsoft Security Copilot to assist with analysis, investigation, and remediation
- Correlate posture, vulnerability, identity, and threat information to prioritize security actions
- Review the SC-500 exam topics and analyze scenarios representative of the certification
- Final workshop: audit the environment, identify cloud and AI risks, prioritize remediation, and resolve a scenario

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific domain knowledge or modern methodologies.

Pre-training Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.