

Course : Implement end-to-end security controls for cloud and AI workloads (Microsoft SC-500)

Official SC-500 Course: Exam Preparation

Practical course - 4d - 28h00 - Ref. MS5

Price : 2890 € E.T.

NEW

ActionCo

Formation éligible au financement Atlas

With this training, you will gain the skills needed to design, deploy, and manage security solutions in Microsoft Azure and Microsoft 365 environments. You'll learn how to secure identities, protect cloud infrastructures, detect threats, and strengthen your security posture—including for AI workloads.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Implement identity security with Microsoft Entra ID
- ✓ Securing Azure Resources and Cloud Workloads
- ✓ Protecting Data, Storage, and Databases
- ✓ Implement security controls for AI environments
- ✓ Monitor security posture and ensure compliance

Intended audience

Security engineers working in cloud, hybrid, and multi-cloud environments.

Prerequisites

Hands-on experience administering Microsoft Azure (compute, networking, storage), strong knowledge of Microsoft Entra ID, basic knowledge of Microsoft 365 administration, and experience implementing security controls in cloud or hybrid environments. Strong written English skills.

Course schedule

PARTICIPANTS

Security engineers working in cloud, hybrid, and multi-cloud environments.

PREREQUISITES

Hands-on experience administering Microsoft Azure (compute, networking, storage), strong knowledge of Microsoft Entra ID, basic knowledge of Microsoft 365 administration, and experience implementing security controls in cloud or hybrid environments. Strong written English skills.

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

1 Securing Access to Resources with Microsoft Entra

- Manage and implement authentication methods in Microsoft Entra ID.
- Deploy and configure Privileged Identity Management (PIM).
- Authenticate an API plug-in for declarative agents using secure APIs.

Hands-on work

Configure authentication methods in Microsoft Entra ID. Integrate an API plug-in with a key-secured API. Integrate an API plug-in with an OAuth-secured API.

2 Securing Azure Key Vault with a defense-in-depth strategy for the cloud and AI workloads

- Configure and secure Azure Key Vault.
- Manage keys and secrets in Azure Key Vault.
- Manage certificates and monitor Azure Key Vault.
- Protect Azure Key Vault with Microsoft Defender for Cloud.

3 Implement security governance and regulatory compliance

- Implement governance using Azure Policy and resource locks.
- Configure security controls and address recommendations in Microsoft Defender for Cloud.
- Assess regulatory compliance in Microsoft Defender for Cloud.
- Manage and adjust RBAC role assignments according to the principle of least privilege.
- Protect backup data using Azure Backup's security features.
- Implement security controls in Infrastructure as Code (IaC).

4 Implement Azure Storage security for cloud environments and AI workloads

- Describe the Azure Storage services.
- Implement security and manage access to Azure Storage.
- Configure Azure Storage network security.
- Deploy Microsoft Defender for Storage.

5 Implement Azure SQL Database Security

- Configure security at the Azure SQL platform level.
- Configure auditing for Azure SQL Database and SQL Managed Instance.
- Deploy Microsoft Defender for Databases.

Options

Certification : 190 € H.T.

Optional certification: "Cloud and AI Security Engineer Associate (SC-500)"

[Comment passer votre examen ?](#)

ASSESSMENT TERMS

Assessment of targeted skills prior to training.

Assessment by the participant, at the end of the training course, of the skills acquired during the training course.

Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.

At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.

An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

This programme is an original creation, developed by the teaching teams at ORSYS Formation. Any reproduction, representation, adaptation or use, in

whole or in part, without the prior written authorisation of ORSYS, is strictly prohibited. ORSYS reserves the right to take any action necessary to protect its intellectual property rights.

Dates and locations

REMOTE CLASS

2026 : 8 Dec.

2027 : 9 Mar., 15 June, 14 Sep., 7 Dec.

PARIS LA DÉFENSE

2027 : 9 Mar., 15 June, 14 Sep., 7 Dec.