Microsoft Cybersecurity Architect (SC-100T00)

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

This course is for experienced cloud security engineers who have taken a previous certification in the security, compliance and identity portfolio. Specifically, students should have advanced experience and knowledge in a wide range of security engineering areas, including identity and access, platform protection, security operations, securing data, and securing applications. They should also have experience with hybrid and cloud implementations.

Beginning students should instead take the course SC-900: Introduction to Microsoft Security, Compliance, and Identity.

Training objectives

By the end of this

course, students will be able to:

- Design a Zero Trust strategy and architecture:
- Learn how to create secure environments based on the principles of zero trust.
- Secure infrastructure: Develop strategies to protect IT infrastructures against threats.
- Secure data and applications: Develop plans for data and application protection across various cloud environments.
- Recommend security best practices and priorities: Identify and advise on best practices to strengthen security.
- Assess governance, risk, and compliance (GRC) strategies:
- Analyze and manage risks, ensure compliance with regulations, and govern security policies.
- Setting up and managing security operations to protect infrastructure and data.

Summary

Copyright © 2026 AFI by Edgenda inc.

This is an advanced, expert-level course. This course prepares students with the expertise to design and evaluate cybersecurity strategies in the following areas: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications. Students will also learn how to design and architect solutions using zero trust principles and specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS).

Course outline

Learning Path 1: Design solutions that align with security best practices and priorities

- Module 1: Introduction to Zero Trust and best practice frameworks
- Module 2: Design solutions aligned with the Cloud Adoption Framework (CAF) and Well Architected Framework (WAF)
- Module 3: Design solutions aligned with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft Cloud Security Benchmark (MCSB)
- Module 4: Design a resiliency strategy for common cyberthreats such as ransomware

Learning Path 2: Design security operations, identity, and compliance capabilities

- Module 1: Design solutions for regulatory compliance
- Module 2: Design solutions for identity and access management
- Module 3: Design solutions for securing privileged access
- Module 4: Design solutions for security operations
- Case Study 1: Interactive case study — Design security solutions for infrastructure
- Case Study 2: Interactive case study — Modernizing access control and threat resilience

Learning Path 3: Design security solutions for applications and data

- Module 1: Design solutions for securing Microsoft 365
- Module 2: Design solutions for securing applications
- Module 3: Design solutions for securing organizational data
- Case Study 1: Interactive case study — Securing apps and data

Copyright © 2026 AFI by Edgenda inc.

Learning Path 4: Design security solutions for infrastructure

- Module 1: Specify requirements for securing SaaS, PaaS, and IaaS services
- Module 2: Design solutions for security posture management in hybrid and multicloud environments
- Module 3: Design solutions for securing server and client endpoints
- Module 4: Evaluate solutions for network security and Security Service Edge (SSE)
- Case Study 1: Interactive case study — Securing endpoints and infrastructure

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants gradually develop an expertise as a Microsoft cybersecurity architect through concrete exercises inspired by professional scenarios, promoting an immediate application of the learnings.

They learn how to design global security strategies, integrate Microsoft solutions, and build robust security architectures that are aligned with best practices and compliance requirements.

Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable strategic and technical skills to effectively secure environments in a professional context.

Prerequisites

Students

should have the following knowledge and experience before attending this

course:

- Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications.
- Experience with hybrid and cloud implementations.

Recommendations

Optional Prerequisites:

-

Copyright © 2026 AFI by Edgenda inc.

Strong knowledge of cybersecurity (principles, threats, risk management)

- Experience with Microsoft Security solutions (Defender, Sentinel, Entra ID, Purview)
- Familiarity with CAF, WAF, MCRA, and MCSB frameworks
- Understanding of cloud concepts (Azure, Microsoft 365)
- Notions of security architecture and governance
- Experience in security administration or engineering (highly recommended)
- Awareness of resiliency strategies for cyberthreats (e.g., ransomware)

Although not required to attend, students are strongly encouraged to have taken and passed another associate level certification in the security, compliance and identity portfolio (such as SC-200, SC-300, SC-401 or SC-500) before attending this class.

Certifications

Microsoft Certified: Cybersecurity Architect Expert

Legal notices

© AFI Expertise inc.

Copyright © 2026 AFI by Edgenda inc.