Microsoft Cybersecurity Architect (SC-100T00)

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

This course is intended for experienced cloud security engineers who have completed a previous certification in the security, compliance, and identity portfolio. In particular, you should have advanced experience and knowledge in a wide range of areas of security engineering, including identity and access, platform protection, security operations, data security, and application security. You should also be familiar with hybrid and cloud implementations. Entry-level students should instead take the course SC-900: Fundamentals of Microsoft Security, Compliance, and Identity.

Training objectives

- 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.
- Security Operations (SecOps): Setting up and managing security operations to protect infrastructure and data.

Summary

This is an advanced expert-level course. While it is not necessary to attend, you are strongly encouraged to have completed and passed another associated level certification in the Security, Compliance, and Identity Portfolio (e.g., AZ-500, SC-200, or SC-300) prior to attending this class. This course prepares students with expertise in designing and evaluating cybersecurity strategies in

the following areas: Zero Trust, Governance Compliance (GRC) Risk, Security Operations (SecOps), and Data and Applications. You will also learn how to design solution architecture using zero trust principles and specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS).

Course outline

Design solutions aligned with security best practices and priorities

- Introduction to Zero Trust and Best Practice Frameworks
- Design solutions aligned with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
- Design solutions aligned with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft Cloud Security Benchmark (MCSB)
- Design a resiliency strategy against common cyber threats like ransomware
- Case Study 1 Design Security Operations, Identity, and Compliance Capabilities
- Design Solutions for Regulatory Compliance
- Design Solutions for Identity and Access Management
- Design Solutions to Secure Privileged Access
- Design Solutions for Security Operations
- Case Study 2 Design Security Solutions for Applications and Data
- Design Solutions for Secure Microsoft 365
- Design solutions to secure applications
- Design solutions to secure an organization's data
- Case Study 3 Design security solutions for infrastructure
- Specify requirements to secure SaaS, PaaS, and IaaS services
- Design solutions for security posture management

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

Conceptual knowledge of security policies, requirements, Zero Trust architecture, and management of hybrid environments. Hands-on experience with Zero Trust strategies, enforcing security policies, and developing security requirements based on business objectives.

Recommendations

Strong knowledge of cybersecurity (principles, threats, risk management) Experience with Microsoft Security solutions (Defender, Sentinel, Entra ID, Purview) Understanding of cloud concepts (Azure, Microsoft 365) Notions of security architecture and governance Experience in security administration or engineering (highly recommended)