GALILEU

SC-100: Microsoft Cybersecurity Architect

Microsoft - Security

Live Training (também disponível em presencial)

- **Localidade:** Imprimir Curso
- **Data:** 16 Dec 2024
- **Preço:** 1750 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das 9h00 às 17h00
- **Nível:** Avançado
- **Duração:** 28h

Sobre o curso

This is an advanced, expert-level course. 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 AZ-500, SC-200 or SC-300) before attending this class.

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).

Destinatários

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: Microsoft Security, Compliance, and Identity Fundamentals.

Objetivos

- Learn how to design an organizations security strategy, including security operations and identity based on the principles of Zero Trust
- Learn how to evaluate cybersecurity strategies for Governance and Risk Compliance as well as security operations (SecOps)
- Learn how to design for infrastructure security, including architecture best practices, endpoint security and cloud security for different service models (SaaS, PaaS and IaaS)
- Learn how to design a cybersecurity strategy for data and applications
- Learn how to use critical Microsoft security best practices to improve an organizations security posture, apply zero trust principles and minimize risk from emerging attacks

Pré-requisitos

Before attending this course, students must have:

  - Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications.

  - Experience with hybrid and cloud implementations.

Programa

- Design solutions that align with security best practices and priorities
- Design security operations, identity, and compliance capabilities
- Design security solutions for applications and data
- Design security solutions for infrastructure

Design solutions that align with security best practices and priorities

You learn how to use critical Microsoft security best practices such as the Cloud Adoption Framework (CAF), Well-Architected Framework (WAF), Microsoft Cybersecurity Reference Architecture (MCRA) to improve an organizations security posture, apply zero trust principles and minimize risk from emerging attacks.

- Introduction to Zero Trust and best practice frameworks
- Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
- Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)
- Design a resiliency strategy for ransomware and other attacks based on Microsoft Security Best Practices
- Case study: Design solutions that align with security best practices and priorities

Design security operations, identity, and compliance capabilities

You learn how to design solutions for security operations (SecOps), identity & access management, privileged access, and regulatory compliance.

- Design solutions for regulatory compliance
- Design solutions for identity and access management
- Design solutions for securing privileged access
- Design solutions for security operations
- Case study: Design security operations, identity and compliance capabilities

Design security solutions for applications and data

Learn how to design solutions to secure data and applications, including: Microsoft 365, application development, existing application portfolios, data discovery and classification with Microsoft Purview and data security for Azure workloads.

- Design solutions for securing Microsoft 365
- Design solutions for securing applications
- Design solutions for securing an organization’s data
- Case study: Design security solutions for applications and data

Design security solutions for infrastructure

You learn how to design for infrastructure security, including specifying requirements for different cloud models, designing solutions for posture management in hybrid and multicloud environments, and securing endpoints.

- Specify requirements for securing SaaS, PaaS, and IaaS services
- Design solutions for security posture management in hybrid and multicloud environments
- Design solutions for securing server and client endpoints
- Design solutions for network security
- Case study: Design security solutions for infrastructure