SC-100T00-A (MICROSOFT CYBERSECURITY ARCHITECT) 2023

Objetivo

–

PÃºblico Alvo

Audience Profile 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.

PrÃ©-Requisitos

Prerequisites Before attending this course, students must have: â□¢ Highly recommended to have attended and passed one of the associate level certifications in the security, compliance and identity portfolio (such as AZ-500, SC-200 or SC-300) â□¢ Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications. â□¢ Experience with hybrid and cloud implementations.

Carga HorÃ¡ria

32 horas (4 dias).

ConteÃºdo ProgramÃ¡tico

COURSE OUTLINE

Module 1: SC-100: 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 common cyberthreats like ransomware

• Case study: Design solutions that align with security best practices and priorities

Module 2: SC-100: 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

Module 3: SC-100: Design security solutions for applications and data

Learn how to design a cybersecurity strategy for data and applications.

• 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

Module 4: SC-100: 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
• Case study: Design security solutions for infrastructure