Microsoft Cybersecurity Architect

CODICE	SC-100T00
DURATA	4 gg
PREZZO	1.590,00 €
EXAM	

DESCRIZIONE

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).

OBIETTIVI RAGGIUNTI

- Design a Zero Trust strategy and architecture
- Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies
- Design security for infrastructure
- Design a strategy for data and applications

TARGET

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.

PREREQUISTI

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.

CONTENUTI

Design solutions that align with security best practices and priorities

- Introduction to Zero Trust and best practice frameworks
- Design security 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

- 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

- 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

- 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