COMPU EDUCACIÓN®

TEMARIO

SC-100: Microsoft Cybersecurity Architect (4 Days)

Course SC-100: Microsoft Cybersecurity Architect (4 Days)

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).

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.

Prerequisites

- Conceptual knowledge of security policies, requirements, zero trust architecture, and management of hybrid environments.
- Working experience with zero trust strategies, applying security policies, and developing security requirements based on business goals.

TEMARIO

Modulo 1: Introduction to Zero Trust and best practice frameworks

You learn what best practices are and how cybersecurity architects use them as well as some key best practice frameworks for Microsoft cybersecurity capabilities. You also learn about the concept of Zero Trust, and how to get started with Zero Trust in an organization.

Learning objectives

By the end of this module, you'll be able to:

- Understand how to use best practices as a cybersecurity architect.
- Understand the concept of Zero Trust and how it can be used to modernize an organizations cybersecurity.
- Understand when to use different best practice frameworks like MCRA, CAF and WAF.

Modulo 2: Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)

You'll learn about the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF) and how you can use them to design more secure solutions.

Learning objectives

Upon completion of this module, the learner will be able to:

- Upon completion of this module, the learner will be able to:

- Understand the Cloud Adoption Framework and how it can be used to accelerate and secure an organizations move to the cloud.
- Understand the Well-Architected Framework and how it can be used to design solutions in the cloud that adhere to sound design principles including security.

Modulo 3 : Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)

You learn about the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB) and how you can use them to design more secure solutions.

Learning objectives

By the end of this module, you are able to:

- Understand how to use Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB) to design more secure solutions.

Modulo 4: Design a resiliency strategy for common cyberthreats like ransomware

You'll learn about common cyberthreats like ransomware and what kinds of attack patterns an organization must be prepared for.

Learning objectives

By the end of this module, you'll be able to:

- Understand common cyberthreats like ransomware.
- Understand how to support business resiliency.
- Design configurations for secure backup and restore.
- Design solutions for managing security updates.

TEMARIO

Modulo 5 : Case study: Design solutions that align with security best practices and priorities

Apply your cybersecurity architect skills on a real business scenario in the area of security operations, identity and compliance. You will analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

Learning objectives

You learn:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Modulo 6: Design solutions for regulatory compliance

You'll learn how to interpret and translate regulatory requirements into technical solutions. You'll also learn how to use capabilities found in Microsoft Purview, Microsoft Priva, and Defender for Cloud for compliance.

Learning objectives

Upon completion of this module, the learner will be able to:

- Translate compliance requirements into a security solution
- Address compliance requirements with Microsoft Purview
- Design a solution to address privacy requirements with Microsoft Priva
- Design Azure Policy solutions to address security and compliance requirements
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud

Modulo 7 : Design solutions for identity and access management

You learn about various strategies for managing identities and access to resources, including hybrid and multicloud scenarios, external identities, and conditional access.

Learning objectives

By the end of this module, you are able to:

- Design cloud, hybrid and multicloud access strategies
- Design a solution for Azure Active Directory (Azure AD), part of Microsoft Entra
- Design a solution for external identities
- Design modern authentication and authorization strategies
- Specify requirements to secure Active Directory Domain Services
- Design a solution to manage secrets, keys, and certificates

Modulo 8: Design solutions for securing privileged access

You learn advanced techniques for designing solutions that manage privileged access effectively.

Learning objectives

By the end of this module, you are able to:

- Understand privileged access and the Enterprise Access Model
- Design identity governance solutions
- Design a solution for securing administration of cloud tenants
- Design for cloud infrastructure entitlement management

TEMARIO

Modulo 9 : Design solutions for security operations

You learn techniques to design security operations capabilities including logging, auditing, Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), and security workflows.

Learning objectives

By the end of this module, you are able to:

- Design security operations capabilities in hybrid and multicloud environments.
- Design centralized logging and auditing.
- Design Security Information and Event Management (SIEM) solutions.
- Design a solution for detection and response that includes Extended Detection and Response (XDR).
- Design a solution for security orchestration, automation, and response (SOAR).
- Design security workflows.
- Design and evaluate threat detection with the MITRE ATT&CK framework.

Modulo 11 : Design solutions for securing Microsoft 365

You learn how to design security solutions for Exchange, Sharepoint, OneDrive and Teams.

Learning objectives

By the end of this module, you are able to:

- Evaluate security posture for collaboration and productivity workloads
- Design a Microsoft Defender XDR solution
- Design configurations and operational practices for Microsoft 365

Modulo 10: Case study: Design security operations, identity and compliance capabilities

Apply your cybersecurity architect skills on a real business scenario in the area of security operations, identity and compliance. You analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

Learning objectives

You learn:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Modulo 12: Design solutions for securing applications

You learn how to secure applications, APIs and the development process using techniques like posture management, threat modeling, and secure access for workload identities.

Learning objectives

By the end of this module, you're able to:

- Evaluate security posture of existing application portfolios
- Evaluate threats to business-critical applications by using threat modeling
- Design and implement a full lifecycle strategy for application security
- Design and implement standards and practices for securing the application development process
- Design a solution for workload identity to authenticate and access Azure cloud resources
- Design a solution for API management and security
- Design a solution for secure access to applications

TEMARIO

Modulo 13 : Design solutions for securing an organization's data

You learn about designing solutions that secure an organization's data using capabilities like Microsoft Purview, Defender for SQL, Defender for Storage.

Learning objectives

By the end of this module, you are able to:

- Design a solution for data discovery and classification using Microsoft Purview
- Specify priorities for mitigating threats to data
- Design a solution for protection of data at rest, data in motion, and data in use
- Design a security solution for data in Azure workloads
- Design a security solution for data in Azure Storage
- Design a security solution that includes Microsoft Defender for SQL and Microsoft Defender for Storage

Modulo 14: Case study: Design security solutions for applications and data

Apply your cybersecurity architect skills on a real business scenario in the area of securing applications and data. You will analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

Learning objectives

You learn:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Modulo 15 : Specify requirements for securing SaaS, PaaS, and IaaS services

You learn how to analyze security requirements for different cloud offerings (SaaS, PaaS, and IaaS), IoT workloads, web workloads and containers.

Learning objectives

By the end of this module, you are able to:

- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for web workloads
- Specify security requirements for containers and container orchestration

Modulo 16: Design solutions for security posture management in hybrid and multicloud environments

You learn how to design security posture management solutions that integrate into hybrid and multicloud scenarios using capabilities in Microsoft Defender for Cloud, Azure Arc and Microsoft Cloud Security Benchmark (MCSB).

Learning objectives

By the end of this module, you're able to:

- Evaluate security posture by using Microsoft Cloud Security Benchmark, Microsoft Defender for Cloud, and Secure Scores
- Design integrated security posture management and workload protection solutions in hybrid and multicloud environments
- Design cloud workload protection solutions that use Microsoft Defender for Cloud

TEMARIO

Modulo 17 : Design solutions for securing server and client endpoints

You learn how to analyze the security requirements for different types of endpoints including servers, clients, IoT, OT, mobile, and embedded devices. These requirements will take into account different platforms and operating systems and set standards for endpoint protection, hardening and configuration.

Learning objectives

By the end of this module, you are able to:

- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify security requirements for IoT devices and embedded systems
- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT
- Specify security baselines for server and client endpoints
- Design a solution for secure remote access

Modulo 18: Design solutions for network security

You learn how to design secure network solutions using techniques like network segmentation, traffic filtering, network monitoring and posture management.

Learning objectives

By the end of this module, you are able to:

- Design solutions for network segmentation
- Design solutions for filtering traffic with network security groups
- Design solutions for network posture measurement
- Design solutions for network monitoring

Modulo 19 : Case study: Design security solutions for infrastructure

Apply your cybersecurity architect skills on a real business scenario in the area of infrastructure security. You analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

Learning objectives

You learn:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Contacto

CDMX
informacion@compueducacion.mx
55 5283 8260

MTY
mktmty@compueducacion.mx
81 83568394

COMPU EDUCACIÓN®