



Enterprise Computing Solutions - Education Services

## TRAINING OFFERING

---

**Sie erreichen uns hier**

Freistädterstraße 236, A-4040 Linz

Email: [education.ecs.at@arrow.com](mailto:education.ecs.at@arrow.com)

Phone: +43 1 370 94 40 - 34



# SC-100T00: Microsoft Cybersecurity Architect

CODE:	LÄNGE:	PREIS:
MCS_SC-100T00	32 Hours (4 Tage)	€2,485.00

## Description

Dieser Training vermittelt den Teilnehmer\*innen das notwendige Wissen, um Cybersicherheitsstrategien in den folgenden Bereichen zu entwerfen und zu bewerten: Zero Trust, Governance Risk Compliance (GRC), Security Operations (SecOps) sowie Daten und Anwendungen.

Die Trainingsteilnehmer\*innen lernen außerdem, wie Sie Lösungen mit Zero Trust-Prinzipien entwerfen und Sicherheitsanforderungen für Cloudinfrastruktur in verschiedenen Dienstmodellen (SaaS, PaaS, IaaS) angeben.

## Zielgruppe

Dieser Training richtet sich an erfahrene Cloudsicherheitstechniker\*innen, die bereits eine Zertifizierung im Portfolio „Sicherheit, Compliance und Identität“ erworben haben.

Die Lernenden sollten über umfassende Erfahrung und tiefgreifende Kenntnisse in vielen sicherheitstechnischen Bereichen verfügen, z. B. Identität und Zugriff, Plattformschutz, Sicherheitsfunktionen sowie Schutz für Daten und Anwendungen.

Sie sollten auch Erfahrung mit Hybrid- und Cloudimplementierungen haben.

Anfänger sollten stattdessen Kurs SC-900 zu den Grundlagen von Microsoft-Sicherheit, -Compliance und -Identität absolvieren.

## Voraussetzungen

Es wird dringend empfohlen, eine der Zertifizierungen auf Associate-Ebene im Portfolio „Sicherheit, Compliance und Identität“ (z. B. AZ-500, SC-200 oder SC-300) absolviert und bestanden zu haben.

Umfassende Erfahrung und tiefgreifende Kenntnisse bezüglich Identität und Zugriff, Plattformschutz, Sicherheitsvorgängen, Schützen von Daten und Sichern von Anwendungen.

Erfahrung mit Hybrid- und Cloudimplementierungen.

## Inhalt

- Introduction to best practices
- Introduction to Zero Trust
- Zero Trust initiatives
- Zero Trust technology pillars part
- Zero Trust technology pillars part 2
- Introduction to Zero Trust and best practice frameworks
- Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
  - Define a security strategy
  - Introduction to the Cloud Adoption Framework
  - Cloud Adoption Framework secure methodology
  - Introduction to Azure Landing Zones
  - Design security with Azure Landing Zones
  - Introduction to the Well-Architected Framework
  - The Well-Architected Framework security pillar
  - Knowledge check - Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
  - Summary - 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)
  - Introduction to Microsoft Cybersecurity Reference Architecture and cloud security benchmark
  - Design solutions with best practices for capabilities and controls
  - Design solutions with best practices for attack protection

Common cyberthreats and attack patterns  
 Support business resiliency  
 Ransomware protection  
 Configurations for secure backup and restore  
 Security updates

Design a resiliency strategy for common cyberthreats like ransomware

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

Case study description  
 Case study answers  
 Conceptual walkthrough  
 Technical walkthrough

Introduction to regulatory compliance  
 Translate compliance requirements into a security solution  
 Address compliance requirements with Microsoft Purview  
 Address privacy requirements with Microsoft Priva  
 Address security and compliance requirements with Azure policy

Design solutions for regulatory compliance

Evaluate infrastructure compliance with Defender for Cloud

Design solutions for identity and access management

Introduction to Identity and Access Management  
 Design cloud, hybrid and multicloud access strategies (including Azure AD)  
 Design a solution for external identities  
 Design modern authentication and authorization strategies  
 Align conditional access and Zero Trust  
 Specify requirements to secure Active Directory Domain Services (AD DS)  
 Design a solution to manage secrets, keys, and certificates

Design solutions for securing privileged access

The enterprise access model  
 Design identity governance solutions  
 Design a solution to secure tenant administration  
 Design a solution for cloud infrastructure entitlement management (CIEM)  
 Design a solution for privileged access workstations and bastion services

Design solutions for security operations

Introduction to Security operations (SecOps)  
 Design security operations capabilities in hybrid and multicloud environments  
 Design centralized logging and auditing  
 Design security information and event management (SIEM) solutions  
 Design solutions for detection and response  
 Design a solution for security orchestration, automation, and response (SOAR)  
 Design security workflows  
 Design threat detection coverage

Case study description  
 Case study answers  
 Conceptual walkthrough  
 Technical walkthrough

Case study: Design security operations, identity and compliance capabilities

Introduction to security for Exchange, Sharepoint, OneDrive and Teams  
 Evaluate security posture for collaboration and productivity workloads  
 Design a Microsoft 365 Defender solution

Design solutions for securing Microsoft 365

Design configurations and operational practices for Microsoft 365

Introduction to application security  
 Design and implement standards to secure application development  
 Evaluate security posture of existing application portfolios  
 Evaluate application threats with threat modeling  
 Design security lifecycle strategy for applications  
 Secure access for workload identities  
 Design a solution for API management and security

Design solutions for securing applications

Design a solution for secure access to applications

Design solutions for securing an organization's data

Introduction to data security  
 Design a solution for data discovery and classification using Microsoft Purview  
 Design a solution for data protection  
 Design data security for Azure workloads  
 Design security for Azure Storage  
 Design a security solution with Microsoft Defender for SQL and Microsoft Defender for Storage

Case study description  
 Case study answers  
 Conceptual walkthrough

Case study: Design security solutions for applications and data

Technical walkthrough

Specify requirements for securing SaaS, PaaS, and IaaS services

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

Design solutions for security posture management in hybrid and multicloud environments

- Introduction to hybrid and multicloud posture management
- Evaluate security posture by using Microsoft Cloud Security Benchmark
- Design integrated posture management and workload protection
- Evaluate security posture by using Microsoft Defender for Cloud
- Posture evaluation with Microsoft Defender for Cloud secure score
- Design cloud workload protection with Microsoft Defender for Cloud
- Integrate hybrid and multicloud environments with Azure Arc
- Design a solution for external attack surface management
- Knowledge check - Design solutions for security posture management in hybrid and multicloud environments
- Design solutions for securing server and client endpoints
  - Introduction to endpoint security
  - Specify server security requirements
  - Specify requirements for mobile devices and clients
  - Specify internet of things (IoT) and embedded device security requirements
  - Secure operational technology (OT) and industrial control systems (ICS) with Microsoft Defender for IoT
  - Specify security baselines for server and client endpoints
  - Design a solution for secure remote access
    - Design solutions for network segmentation
    - Design solutions for traffic filtering with network security groups
    - Design solutions for network posture management
    - Design solutions for network monitoring
- Design solutions for network security
  - Knowledge check - Design solutions for network security
  - Case study description
  - Case study answers
  - Conceptual walkthrough
- Case study: Design security solutions for infrastructure
  - Technical walkthrough

## Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
20 Jan 2025	Wien	CET	German	Instructor Led Online		€2,485.00
07 Apr 2025	Wien	CEDT	German	Instructor Led Online	Yes	€2,485.00
11 Aug 2025	Wien	CEDT	German	Instructor Led Online		€2,485.00
09 Dec 2025	Wien	CET	German	Instructor Led Online	Yes	€2,485.00

## Zusätzliche Information

[Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.](#)