SC-100

Microsoft Cybersecurity Architect

Dieser Kurs vermittelt den Teilnehmern 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 Kursteilnehmer lernen außerdem, wie Sie Lösungen mit Zero Trust-Prinzipien entwerfen und Sicherheitsanforderungen für Cloudinfrastruktur in verschiedenen Dienstmodellen (SaaS, PaaS, IaaS) angeben.

Kursinhalt

- Einführung in Zero Trust und Frameworks bewährter Methoden
- Entwerfen von Lösungen, die am Cloud Adoption Framework (CAF) und dem Well-Architected Framework (WAF) ausgerichtet sind
- Entwerfen von Lösungen, die an der Microsoft Cybersecurity Reference Architecture (MCRA) und dem Microsoft Cloud Security Benchmark (MCSB) ausgerichtet sind
- Entwerfen einer Resilienzstrategie für gängige Cyberbedrohungen wie Ransomware
- Fallstudie: Entwerfen von Lösungen, die an den bewährten Sicherheitsmethoden und Prioritäten ausgerichtet sind
- Entwerfen von Lösungen für die Einhaltung gesetzlicher Bestimmungen
- Erstellen von Lösungen für die Identitäts- und Zugriffsverwaltung
- Entwerfen von Lösungen zum Schutz des privilegierten Zugriffs
- Entwerfen von Lösungen für Sicherheitsvorgänge
- Fallstudie: Entwerfen von Funktionen für Sicherheitsvorgänge, Identität und Compliance
- Entwerfen von Lösungen zum Schutz von Microsoft 365
- Entwerfen von Lösungen zum Schutz von Anwendungen
- Entwerfen von Lösungen zum Schutz der Daten einer Organisation
- Fallstudie: Entwerfen von Sicherheitslösungen für Anwendungen und Daten
- Entwerfen einer Strategie zum Schutz von SaaS-, PaaS- und IaaS-Diensten
- Entwerfen von Lösungen für die Verwaltung des Sicherheitsstatus in Hybrid- und Multicloudumgebungen
- Entwerfen von Lösungen zum Schutz von Server- und Clientendpunkten
- Entwerfen von Lösungen für die Netzwerksicherheit
- Fallstudie: Entwerfen von Sicherheitslösungen für die Infrastruktur

E-Book Die originalen Microsoft-Kursunterlagen werden Ihnen online zur Verfügung gestellt.

Zielgruppe

Dieser Kurs richtet sich an erfahrene Cloudsicherheitstechniker, 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.

Voraussetzungen

Dies ist ein Fortgeschrittenenkurs auf Expertenniveau. Lernenden wird dringend empfohlen, vor der Teilnahme an diesem Kurs eine andere Zertifizierung im Portfolio „Sicherheit, Compliance und Identität“ auf Associate-Niveau zu erwerben (z. B. AZ-500, SC-200 oder SC-300) – dies ist allerdings keine Teilnahmevoraussetzung.

Kursziel

Das Examen ist Teil der Anforderungen für die Zertifizierung zum Microsoft Certified: Cybersecurity Architect Expert

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**MC10**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Deutschland	**4 TageCHF 2.920,-**
Online Training	**4 TageCHF 2.920,-**

Termin/Kursort — Kurssprache Deutsch

16.11.-19.11.26	HYMünchen	28.06.-01.07.27	HYOnline
16.11.-19.11.26	HYOnline	05.10.-08.10.27	HYMünchen
05.04.-08.04.27	HYMünchen	05.10.-08.10.27	HYOnline
05.04.-08.04.27	HYOnline	29.11.-02.12.27	HYFrankfurt
28.06.-01.07.27	HYFrankfurt	29.11.-02.12.27	HYOnline

Stand 03.10.2026

ExperTeach

Inhaltsverzeichnis

SC-100 – Microsoft Cybersecurity Architect

Module 1: Build an overall security strategy and architecture
Learn how to build an overall security strategy and architecture.
Lessons
Introduction
Zero Trust overview
Develop Integration points in an architecture
Develop security requirements based on business goals
Translate security requirements into technical capabilities
Design security for a resiliency strategy
Design a security strategy for hybrid and multi-tenant environments
Design technical and governance strategies for traffic filtering and segmentation
Understand security for protocols
Exercise: Build an overall security strategy and architecture
Knowledge check
Summary
After completing this module, students will be able to:
Develop Integration points in an architecture
Develop security requirements based on business goals
Translate security requirements into technical capabilities
Design security for a resiliency strategy
Design security strategy for hybrid and multi-tenant environments
Design technical and governance strategies for traffic filtering and segmentation

Module 2: Design a security operations strategy
Learn how to design a security operations strategy.
Lessons
Introduction
Understand security operations frameworks, processes, and procedures
Design a logging and auditing security strategy
Develop security operations for hybrid and multi-cloud environments
Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration,
Evaluate security workflows
Review security strategies for incident management
Evaluate security operations strategy for sharing technical threat intelligence
Monitor sources for insights on threats and mitigations
After completing this module, students will be able to:
Design a logging and auditing security strategy
Develop security operations for hybrid and multi-cloud environments.
Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, A
Evaluate security workflows.
Review security strategies for incident management.
Evaluate security operations for technical threat intelligence.
Monitor sources for insights on threats and mitigations.

Module 3: Design an identity security strategy
Learn how to design an identity security strategy.
Lessons
Introduction
Secure access to cloud resources
Recommend an identity store for security
Recommend secure authentication and security authorization strategies
Secure conditional access
Design a strategy for role assignment and delegation
Define Identity governance for access reviews and entitlement management
Design a security strategy for privileged role access to infrastructure
Design a security strategy for privileged activities
Understand security for protocols
After completing this module, students will be able to:
Recommend an identity store for security.
Recommend secure authentication and security authorization strategies.
Secure conditional access.
Design a strategy for role assignment and delegation.
Define Identity governance for access reviews and entitlement management.
Design a security strategy for privileged role access to infrastructure.
Design a security strategy for privileged access.

Module 4: Evaluate a regulatory compliance strategy
Learn how to evaluate a regulatory compliance strategy.
Lessons
Introduction
Interpret compliance requirements and their technical capabilities
Evaluate infrastructure compliance by using Microsoft Defender for Cloud
Interpret compliance scores and recommend actions to resolve issues or improve security
Design and validate implementation of Azure Policy
Design for data residency Requirements
Translate privacy requirements into requirements for security solutions
After completing this module, students will be able to:
Interpret compliance requirements and their technical capabilities
Evaluate infrastructure compliance by using Microsoft Defender for Cloud
Interpret compliance scores and recommend actions to resolve issues or improve security
Design and validate implementation of Azure Policy
Design for data residency requirements
Translate privacy requirements into requirements for security solutions

Module 5: Evaluate security posture and recommend technical strategies to manage risk
Learn how to evaluate security posture and recommend technical strategies to manage risk.
Lessons
Introduction
Evaluate security postures by using benchmarks
Evaluate security postures by using Microsoft Defender for Cloud
Evaluate security postures by using Secure Scores
Evaluate security hygiene of Cloud Workloads
Design security for an Azure Landing Zone
Interpret technical threat intelligence and recommend risk mitigations
Recommend security capabilities or controls to mitigate identified risks
After completing this module, students will be able to:
Evaluate security postures by using benchmarks
Evaluate security postures by using Microsoft Defender for Cloud
Evaluate security postures by using Secure Scores
Evaluate security hygiene of Cloud Workloads
Design security for an Azure Landing Zone
Interpret technical threat intelligence and recommend risk mitigations
Recommend security capabilities or controls to mitigate identified risks

Module 6: Understand architecture best practices and how they are changing with the Cloud
Learn about architecture best practices and how they are changing with the Cloud.
Lessons
Introduction
Plan and implement a security strategy across teams
Establish a strategy and process for proactive and continuous evolution of a security strategy
Understand network protocols and best practices for network segmentation and traffic filtering
After completing this module, students will be able to:
Describe best practices for network segmentation and traffic filtering.
Plan and implement a security strategy across teams.
Establish a strategy and process for proactive and continuous evaluation of security strategy.

Module 7: Design a strategy for securing server and client endpoints
Learn how to design a strategy for securing server and client endpoints.
Lessons
Introduction
Specify security baselines for server and client endpoints
Specify security requirements for servers
Specify security requirements for mobile devices and clients
Specify requirements for securing Active Directory Domain Services
Design a strategy to manage secrets, keys, and certificates
Design a strategy for secure remote access
Understand security operations frameworks, processes, and procedures
Understand deep forensics procedures by resource type
After completing this module, students will be able to:
Specify security baselines for server and client endpoints
Specify security requirements for servers
Specify security requirements for mobile devices and clients
Specify requirements for securing Active Directory Domain Services
Design a strategy to manage secrets, keys, and certificates
Design a strategy for secure remote access
Understand security operations frameworks, processes, and procedures
Understand deep forensics procedures by resource type

Module 8: Design a strategy for securing PaaS, IaaS, and SaaS services
Learn how to design a strategy for securing PaaS, IaaS, and SaaS services.
Lessons
Introduction
Specify security baselines for PaaS services
Specify security baselines for IaaS services
Specify security baselines for SaaS services
Specify security requirements for IoT workloads
Specify security requirements for data workloads
Specify security requirements for web workloads
Specify security requirements for storage workloads
Specify security requirements for containers
Specify security requirements for container orchestration
After completing this module, students will be able to:
Specify security baselines for PaaS, SaaS and IaaS services
Specify security requirements for IoT, data, storage, and web workloads
Specify security requirements for containers and container orchestration

Module 9: Specify security requirements for applications
Learn how to specify security requirements for applications.
Lessons
Introduction
Understand application threat modeling
Specify priorities for mitigating threats to applications
Specify a security standard for onboarding a new application
Specify a security strategy for applications and APIs
After completing this module, students will be able to:
Specify priorities for mitigating threats to applications
Specify a security standard for onboarding a new application
Specify a security strategy for applications and APIs

Module 10: Design a strategy for securing data
Learn how to design a strategy for securing data.
Lessons
Introduction
Prioritize mitigating threats to data
Design a strategy to identify and protect sensitive data
Specify an encryption standard for data at rest and in motion
After completing this module, students will be able to:
Prioritize mitigating threats to data
Design a strategy to identify and protect sensitive data
Specify an encryption standard for data at rest and in motion

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch