

CS100 Microsoft Cybersecurity Architect (SC-100)

Kurzbeschreibung:

Teilnehmer erhalten eine praxisnahe Einführung in die Cybersicherheitsarchitektur nach Microsoft-Standard. Vermittelt werden Zero-Trust-Prinzipien, Governance Risk Compliance (GRC), Security Operations (SecOps) sowie Sicherheitsanforderungen für Cloud-Infrastrukturen in SaaS-, PaaS- und IaaS-Umgebungen. Behandelt werden zudem Design und Evaluierung von Cybersicherheitsstrategien auf Expertenniveau.

Zielgruppe:

Der Kurs **CS100 Microsoft Cybersecurity Architect (SC-100)** richtet sich an:

- Erfahrene IT-Experten mit tiefen Kenntnissen der Sicherheitstechnik
- Cloudsicherheitstechniker
- Solution Architects

Voraussetzungen:

Um dem Lerntempo und den Inhalten des Trainings **CS100 Microsoft Cybersecurity Architect (SC-100)** gut folgen zu können, sind folgende Vorkenntnisse notwendig:

- ◆ Langjährige Erfahrung und tiefgreifendes Wissen bezüglich Identity & Access, Plattform Protection, Security Operations, Securing Data und Securing Applications
- ◆ Kenntnisse der Konzepte von Sicherheitsrichtlinien, Anforderungen, Zero Trust-Architektur und der Verwaltung von Hybridumgebungen
- ◆ Praktische Erfahrung mit Zero Trust-Strategien, der Anwendung von Sicherheitsrichtlinien und der Entwicklung von Sicherheitsanforderungen auf der Grundlage von Geschäftszielen

Wir empfehlen vorab den Besuch des Workshops: [AZ500 Microsoft Azure Security Technologies](#)

Sonstiges:

Dauer: 4 Tage

Preis: 2650 Euro plus Mwst.

Ziele:

Im Workshop **CS100 Microsoft Cybersecurity Architect (SC-100)** werden folgende Kenntnisse und Fähigkeiten vermittelt:

- Verständnis von Sicherheitsrichtlinien und -standards, um sicherzustellen, dass Lösungen den relevanten Vorschriften entsprechen
- Fähigkeit, Lösungen zu entwerfen, die eine sichere und effiziente Verwaltung von Benutzeridentitäten und Zugriffsrechten gewährleisten

- Implementierung von Sicherheitsmaßnahmen, die den Zugriff auf privilegierte Konten und Ressourcen schützen
- Erstellung von Sicherheitslösungen, die eine effektive Überwachung, Erkennung und Reaktion auf Sicherheitsvorfälle ermöglichen
- Verständnis und die Anwendung des Zero-Trust-Modells, das davon ausgeht, dass kein Benutzer oder Gerät implizit vertrauenswürdig ist und kontinuierlich überprüft werden muss
- Verständnis der Sicherheitsaspekte verschiedener Cloud-Servicemodelle (SaaS, PaaS, IaaS) und die Fähigkeit, entsprechende Sicherheitsanforderungen zu definieren

Dieses Training bereitet auf die Prüfung **SC-100: Microsoft Cybersecurity Architect** vor. Die Prüfung ist immer separat bei einem Pearson VUE Test-Center oder online abzulegen.

Um die Zertifizierung **Microsoft Certified: Cybersecurity Architect Expert** erfolgreich abschließen zu können, wird dringend empfohlen, vorab eine Associate-Level Zertifizierung im Bereich Sicherheit, Compliance und Identität zu erwerben, wie z.B.

- Microsoft Certified: Security Operations Analyst Associate | Exam SC-200
- Microsoft Certified: Identity and Access Administrator Associate | Exam SC-300
- Microsoft Certified Azure Security Engineer Associate | Exam AZ-500

Inhalte/Agenda:

- **◆ Entwerfen von Lösungen, die an den bewährten Sicherheitsmethoden und Prioritäten ausgerichtet sind**
 - ◆ ◇ Einführung in Zero Trust und Frameworks bewährter Methoden
 - ◆ ◇ Entwerfen von Lösungen, die an Cloud Adoption Framework (CAF) und 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 Ransomware und andere Angriffe auf der Grundlage bewährter Sicherheitsmethoden von Microsoft
 - ◆ ◇ Fallstudie: Entwerfen von Lösungen, die an den bewährten Sicherheitsmethoden und Prioritäten ausgerichtet sind
- ◆ Entwerfen von Funktionen für Sicherheitsvorgänge, Identität und Compliance**
 - ◆ ◇ Entwerfen von Lösungen für die Einhaltung gesetzlicher Bestimmungen
 - ◆ ◇ Erstellen von Lösungen für die Identitäts- und Zugriffsverwaltung
 - ◆ ◇ Entwerfen von Lösungen zum Schutz des privilegierten Zugriffs
 - ◆ ◇ Design von Lösungen für Security Operations
 - ◆ ◇ Fallstudie: Entwerfen von Funktionen für Sicherheitsvorgänge, Identität und Compliance
- ◆ Entwerfen von Sicherheitslösungen für Anwendungen und Daten**
 - ◆ ◇ 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
- ◆ Design von Security-Lösungen für die Infrastructure**
 - ◆ ◇ 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