

## Microsoft Cybersecurity Architect (SC-100T00)

**ID SC-100T00** Preis CHF 3'380.– (exkl. MwSt.) **Dauer 4 Tage**

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

### Empfohlenes Training für die Zertifizierung zum

Microsoft Certified: Cybersecurity Architect Expert (MCCAE)

### Voraussetzungen

Vor der Teilnahme an diesem Kurs müssen die Teilnehmer folgende Voraussetzungen erfüllen:

- 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.
- Inhalte der Kurse [Microsoft Azure Administrator \(AZ-104T00\)](#), [Microsoft 365 Administrator \(MS-102T00\)](#) und [Defend against cyberthreats with Microsoft's security operations platform \(SC-200T00\)](#) oder entsprechende Kenntnisse
- Umfassende Erfahrung und tiefgreifende Kenntnisse bezüglich Identität und Zugriff, Plattformschutz, Sicherheitsvorgängen, Schützen von Daten und Sichern von Anwendungen.
- Erfahrung mit Hybrid- und Cloudimplementierungen.

### Kursinhalt

#### Entwerfen von Lösungen, die an den bewährten Sicherheitsmethoden und Prioritäten ausgerichtet sind

- Einführung in Zero Trust und Best Practices-Frameworks

- Entwerfen Sie Sicherheitslösungen, die mit dem Cloud Adoption Framework (CAF) und dem Well-Architected Framework (WAF) übereinstimmen.
- 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

#### 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
- Entwerfen von Lösungen für Sicherheitsvorgänge
- Interaktive Fallstudie: Modernisieren von Identität und Datensicherheit
- Interaktive Fallstudie: Modernisieren der Benutzerzugriffskontrolle und Bedrohungsresilienz

#### Entwerfen von Sicherheitslösungen für Anwendungen und Daten

- Bewerten von Lösungen zum Schutz von Microsoft 365
- Entwerfen von Lösungen zum Schutz von Anwendungen
- Entwerfen von Lösungen zum Schutz der Daten einer Organisation
- Interaktive Fallstudie: Sichern von Apps und Daten

#### Entwerfen von Sicherheitslösungen für die Infrastruktur

- 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
- Interaktive Fallstudie: Sichern von Endpunkten und Infrastruktur

## Weltweite Trainingscenter



## Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3  
CH-8304 Wallisellen  
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>