# Microsoft Cybersecurity Architect (SC-100T00)

**ID** SC-100T00 **Preis** 2.690,– € (exkl. MwSt.) **Dauer** 4 Tage

*Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.*

## Kursüberblick

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. 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.

## 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

- Erstellen einer allgemeinen Sicherheitsstrategie und -architektur
- Entwerfen einer Strategie für Sicherheitsvorgänge
- Entwerfen einer Identitätssicherheitsstrategie
- Bewerten einer Strategie zur Einhaltung gesetzlicher Bestimmungen
- Bewerten des Sicherheitsstatus und Empfehlen technischer Strategien zum Verwalten von Risiken
- Verstehen bewährter Methoden für die Architektur und wie diese sich mit der Cloud ändern
- Entwerfen einer Strategie zum Sichern von Server- und Clientendpunkten
- Entwerfen einer Strategie zur Sicherung von PaaS-, IaaS- und SaaS-Diensten
- Angeben von Sicherheitsanforderungen für Anwendungen
- Entwerfen einer Strategie zum Sichern von Daten
- Empfehlen bewährter Methoden für die Sicherheit anhand von Microsoft Cybersecurity Reference Architectures (MCRA) und Microsoft Cloud Security Benchmarks
- Empfehlen einer sicheren Methodik mithilfe des Cloud Adoption Framework (CAF)
- Empfehlen einer Strategie gegen Ransomware mithilfe bewährter Methoden von Microsoft für Sicherheit

## Detaillierter Kursinhalt

## Modul 1: Aufbau einer umfassenden Sicherheitsstrategie und -architektur

Lernen Sie, wie man eine umfassende Sicherheitsstrategie und -architektur aufbaut.

### Lektionen

- Einführung
- Zero Trust Übersicht
- Entwicklung von Integrationspunkten in einer Architektur
- Entwicklung von Sicherheitsanforderungen auf der Grundlage von Geschäftszielen
- Umsetzung von Sicherheitsanforderungen in technische Fähigkeiten
- Sicherheit für eine Ausfallsicherheitsstrategie entwickeln
- Entwurf einer Sicherheitsstrategie für hybride und mehrmandantenfähige Umgebungen
- Entwicklung von technischen und Governance-Strategien für die Filterung und Segmentierung des Datenverkehrs
- Verstehen der Sicherheit von Protokollen
- Übung: Aufbau einer umfassenden Sicherheitsstrategie und -architektur
- Wissens-Check
- Zusammenfassung

Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:

- Entwicklung von Integrationspunkten in einer Architektur
- Entwicklung von Sicherheitsanforderungen auf der Grundlage von Geschäftszielen
- Umsetzung von Sicherheitsanforderungen in technische Fähigkeiten
- Sicherheit für eine Ausfallsicherheitsstrategie entwickeln
- Entwurf einer Sicherheitsstrategie für hybride und mandantenfähige Umgebungen
- Entwicklung von technischen und Governance-Strategien für die Filterung und Segmentierung des Datenverkehrs

## Modul 2: Entwurf einer Strategie für Sicherheitsmaßnahmen

Lernen Sie, wie man eine Strategie für Sicherheitsmaßnahmen entwickelt.

### Lektionen

- Einführung
- Verstehen von Rahmenwerken, Prozessen und Verfahren für Sicherheitsmaßnahmen
- Entwurf einer Sicherheitsstrategie für die Protokollierung und Überprüfung
- Entwicklung von Sicherheitsmaßnahmen für hybride und Multi-Cloud-Umgebungen
- Entwicklung einer Strategie für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM) und für die Sicherheitsorganisation (Security Orchestration),
- Bewertung von Sicherheitsabläufen
- Überprüfung der Sicherheitsstrategien für das Management von Zwischenfällen
- Bewertung der Strategie für Sicherheitsoperationen zum Austausch technischer Bedrohungsdaten
- Überwachen Sie Quellen für Erkenntnisse über Bedrohungen und Abhilfemaßnahmen
- Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:
- Entwurf einer Sicherheitsstrategie für die Protokollierung und Überprüfung
- Entwicklung von Sicherheitsmaßnahmen für hybride und Multi-Cloud-Umgebungen.
- Entwurf einer Strategie für das Sicherheitsinformations- und Ereignis-Management (SIEM) und die Sicherheits-Orchestrierung, A
- Bewertung der Sicherheitsabläufe.
- Überprüfung der Sicherheitsstrategien für das Management von Zwischenfällen.
- Bewertung von Sicherheitsmaßnahmen im Hinblick auf technische Bedrohungsdaten.
- Überwachen Sie Quellen, um Erkenntnisse über Bedrohungen und Abhilfemaßnahmen zu gewinnen.

## Modul 3: Entwurf einer Strategie für Identitätssicherheit

Erfahren Sie, wie man eine Strategie für die Identitätssicherheit entwickelt.

### Lektionen

- Einführung
- Sicherer Zugang zu Cloud-Ressourcen
- Empfehlen Sie einen Identitätsspeicher für die Sicherheit
- Empfehlung sicherer Authentifizierungs- und Sicherheitsautorisierungsstrategien
- Sichere Zugangskontrolle
- Entwicklung einer Strategie für Rollenzuweisung und Delegation
- Definition von Identity Governance für Zugriffsüberprüfungen und Berechtigungsmanagement
- Entwurf einer Sicherheitsstrategie für den Zugang privilegierter Rollen zur Infrastruktur
- Entwurf einer Sicherheitsstrategie für privilegierte Aktivitäten
- Verstehen der Sicherheit von Protokollen

Nach Abschluss dieses Moduls werden die Studierenden in der

Lage sein:

- Empfehlen Sie einen Identitätsspeicher für die Sicherheit.
- Empfehlung sicherer Authentifizierungs- und Sicherheitsautorisierungsstrategien.
- Sichere Zugangskontrolle.
- Entwicklung einer Strategie für die Rollenzuweisung und -delegation.
- Definieren Sie Identity Governance für Zugriffsüberprüfungen und Berechtigungsmanagement.
- Entwurf einer Sicherheitsstrategie für den Zugang privilegierter Rollen zur Infrastruktur.
- Entwurf einer Sicherheitsstrategie für privilegierten Zugang.

## Modul 4: Bewertung einer Strategie zur Einhaltung von Vorschriften

Erfahren Sie, wie Sie eine Strategie zur Einhaltung von Vorschriften bewerten können.

### Lektionen

- Einführung
- Interpretation der Compliance-Anforderungen und ihrer technischen Möglichkeiten
- Bewertung der Compliance der Infrastruktur mit Microsoft Defender for Cloud
- Interpretation der Konformitätsbewertungen und Empfehlung von Maßnahmen zur Behebung von Problemen oder zur Verbesserung der Sicherheit
- Entwurf und Validierung der Implementierung der Azure-Richtlinie
- Design für Datenresidenz Anforderungen
- Umsetzung von Datenschutzanforderungen in Anforderungen für Sicherheitslösungen
- Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:
- Interpretation der Compliance-Anforderungen und ihrer technischen Möglichkeiten
- Bewertung der Compliance der Infrastruktur mit Microsoft Defender for Cloud
- Interpretation der Konformitätsbewertungen und Empfehlung von Maßnahmen zur Behebung von Problemen oder zur Verbesserung der Sicherheit
- Entwurf und Validierung der Implementierung der Azure-Richtlinie
- Design für Anforderungen an die Datenresidenz
- Umsetzung von Datenschutzanforderungen in Anforderungen für Sicherheitslösungen

## Modul 5: Bewertung der Sicherheitslage und Empfehlung technischer Strategien zur Risikobewältigung

Lernen Sie, wie Sie die Sicherheitslage bewerten und technische Strategien zur Risikobewältigung empfehlen können.

### Lektionen

- Einführung
- Bewertung der Sicherheitsmaßnahmen anhand von Benchmarks
- Bewertung von Sicherheitsmaßnahmen mit Microsoft Defender for Cloud
- Bewertung der Sicherheitsvorkehrungen mit Hilfe von Secure Scores
- Bewertung der Sicherheitshygiene von Cloud-Workloads
- Entwurf der Sicherheit für eine Azure Landing Zone
- Interpretation technischer Bedrohungsdaten und Empfehlung von Risikominderungsmaßnahmen
- Empfehlung von Sicherheitskapazitäten oder -kontrollen zur Abschwächung der festgestellten Risiken

Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:

- Bewertung der Sicherheitsmaßnahmen anhand von Benchmarks
- Bewertung von Sicherheitsmaßnahmen mit Microsoft Defender for Cloud
- Bewertung der Sicherheitsvorkehrungen mit Hilfe von Secure Scores
- Bewertung der Sicherheitshygiene von Cloud-Workloads
- Entwurf der Sicherheit für eine Azure Landing Zone
- Interpretation technischer Bedrohungsdaten und Empfehlung von Risikominderungsmaßnahmen
- Empfehlung von Sicherheitskapazitäten oder -kontrollen zur Abschwächung der festgestellten Risiken

## Modul 6: Verstehen der bewährten Architekturpraktiken und wie sie sich durch die Cloud verändern

Erfahren Sie mehr über bewährte Architekturverfahren und wie sich diese mit der Cloud verändern.

### Lektionen

- Einführung
- Planung und Umsetzung einer teamübergreifenden Sicherheitsstrategie
- Festlegung einer Strategie und eines Verfahrens für die proaktive und kontinuierliche Weiterentwicklung einer Sicherheitsstrategie
- Verstehen von Netzwerkprotokollen und bewährten Verfahren zur Netzwerksegmentierung und Verkehrsfilterung

Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:

- Beschreiben Sie bewährte Verfahren für die Netzwerksegmentierung und die Filterung des Datenverkehrs.
- Planung und Umsetzung einer teamübergreifenden Sicherheitsstrategie.
- Festlegung einer Strategie und eines Verfahrens zur proaktiven und kontinuierlichen Bewertung der Sicherheitsstrategie.

## Modul 7: Entwurf einer Strategie zur Sicherung von Server- und Client-Endpunkten

Erfahren Sie, wie Sie eine Strategie zur Sicherung von Server- und Client-Endpunkten entwickeln.

### Lektionen

- Einführung
- Festlegen von Sicherheits-Baselines für Server- und Client-Endpunkte
- Festlegung von Sicherheitsanforderungen für Server
- Festlegung von Sicherheitsanforderungen für mobile Geräte und Clients
- Spezifizieren Sie die Anforderungen für die Sicherung von Active Directory Domain Services
- Entwurf einer Strategie zur Verwaltung von Geheimnissen, Schlüsseln und Zertifikaten
- Entwicklung einer Strategie für sicheren Fernzugriff
- Verstehen von Rahmenwerken, Prozessen und Verfahren für Sicherheitsmaßnahmen
- Tiefe forensische Verfahren nach Ressourcentyp verstehen

Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:

- Festlegen von Sicherheits-Baselines für Server- und Client-Endpunkte
- Festlegung von Sicherheitsanforderungen für Server
- Festlegung von Sicherheitsanforderungen für mobile Geräte und Clients
- Spezifizieren Sie die Anforderungen für die Sicherung von Active Directory Domain Services
- Entwurf einer Strategie zur Verwaltung von Geheimnissen, Schlüsseln und Zertifikaten
- Entwicklung einer Strategie für sicheren Fernzugriff
- Verstehen von Rahmenwerken, Prozessen und Verfahren für Sicherheitsmaßnahmen
- Tiefe forensische Verfahren nach Ressourcentyp verstehen

## Modul 8: Entwurf einer Strategie zur Sicherung von PaaS-, IaaS- und SaaS-Diensten

Erfahren Sie, wie Sie eine Strategie für die Sicherung von PaaS-, IaaS- und SaaS-Diensten entwickeln.

### Lektionen

- Einführung
- Festlegung von Sicherheitsgrundlagen für PaaS-Dienste
- Festlegung von Sicherheitsgrundlagen für IaaS-Dienste
- Festlegung von Sicherheitsgrundlagen für SaaS-Dienste
- Spezifizieren Sie die Sicherheitsanforderungen für IoT-Workloads
- Spezifizieren von Sicherheitsanforderungen für Daten-Workloads
- Spezifizieren von Sicherheitsanforderungen für Web-Workloads
- Spezifizieren von Sicherheitsanforderungen für Speicher-Workloads
- Festlegung von Sicherheitsanforderungen für Container
- Spezifizieren Sie die Sicherheitsanforderungen für die Container-Orchestrierung

Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:

- Festlegung von Sicherheitsgrundlagen für PaaS-, SaaS- und IaaS-Dienste
- Spezifizieren Sie Sicherheitsanforderungen für IoT-, Daten-, Speicher- und Web-Workloads
- Spezifizierung der Sicherheitsanforderungen für Container und Container-Orchestrierung

## Modul 9: Festlegen von Sicherheitsanforderungen für Anwendungen

Lernen Sie, wie man Sicherheitsanforderungen für Anwendungen spezifiziert.

### Lektionen

- Einführung
- Verstehen der Modellierung von Anwendungsbedrohungen
- Festlegung von Prioritäten für die Abschwächung von Bedrohungen für Anwendungen
- Festlegen eines Sicherheitsstandards für das Onboarding einer neuen Anwendung
- Festlegen einer Sicherheitsstrategie für Anwendungen und APIs

Nach Abschluss dieses Moduls werden die Studierenden in der

Lage sein:

- Festlegung von Prioritäten für die Abschwächung von Bedrohungen für Anwendungen
- Festlegen eines Sicherheitsstandards für das Onboarding einer neuen Anwendung
- Festlegen einer Sicherheitsstrategie für Anwendungen und APIs

### Modul 10: Entwurf einer Strategie zur Datensicherung

Erfahren Sie, wie Sie eine Strategie zur Datensicherung entwickeln können.

### Lektionen

- Einführung
- Prioritäten bei der Eindämmung von Bedrohungen für Daten
- Entwicklung einer Strategie zur Ermittlung und zum Schutz sensibler Daten
- Festlegung eines Verschlüsselungsstandards für ruhende und bewegte Daten

Nach Abschluss dieses Moduls werden die Studierenden in der Lage sein:

- Prioritäten bei der Eindämmung von Bedrohungen für Daten
- Entwicklung einer Strategie zur Ermittlung und zum Schutz sensibler Daten
- Festlegung eines Verschlüsselungsstandards für ruhende und bewegte Daten

# Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

## Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

## Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

## Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

**Weltweit vertreten**
mit High-End-Trainingszentren rund um den Globus

**Mehrfach ausgezeichnet**
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

**Praxiserfahrene Experten**
mit insgesamt mehr als 19.000 Zertifizierungen


**Deutschland**
**Fast Lane Institute for Knowledge Transfer GmbH**
Tel. +49 40 25334610
info@flane.de / www.flane.de

**Österreich**
**ITLS GmbH**
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

**Schweiz**
**Fast Lane Institute for Knowledge Transfer (Switzerland) AG**
Tel. +41 44 8325080
info@flane.ch / www.flane.ch