CS100 Microsoft Cybersecurity Architect (SC-100)

Kurzbeschreibung:

Der Kurs **CS100 Microsoft Cybersecurity Architect (SC-100)** vermittelt den Teilnehmern fundierte Kenntnisse und Fähigkeiten im Bereich der Cybersicherheitsarchitektur. Sie erwerben das nötige Wissen für Design und Evaluierung von Cybersicherheitsstrategien in folgenden Bereichen: Zero Trust, Governance Risk Compliance (GRC), Security Operations (SecOps) sowie Daten und Anwendungen. Außerdem lernen Sie, wie man Lösungen mithilfe von Zero-Trust-Prinzipien entwirft und Sicherheitsanforderungen für Cloudinfrastrukturen in verschiedenen Servicemodellen (SaaS, PaaS, IaaS) spezifiziert.

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:

Der Workshop **CS100 Microsoft Cybersecurity Architect (SC-100)** richtet sich an IT-Experten, die bereits umfangreiche Kenntnissein in folgenden Bereichen erworben haben:

- Identity & Access
- Plattform Protection
- Security Operations
- Securing Data
- Securing Applications

- Hybrid- und Cloud-Implementierungen

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, müssen sie sowohl die Prüfung **SC-100** als auch eine der folgenden Prüfung bestehen:

- Microsoft Certified: Security Operations Analyst Associate | Exam SC-200
- Microsoft Certified: Identity and Access Administrator Associate | Exam SC-300
- Microsoft 365 Certified Security Administrator Associate | Exam MS-500
- Microsoft Certified Azure Security Engineer Associate | Exam AZ-500

Inhalte/Agenda:

- ♦ **Entwickeln von Lösungen, die an den bewährten Sicherheitsmethoden und Prioritäten ausgerichtet sind**
  - ♦ ◊ Einführung in das Konzept "Zero Trust" und Frameworks bewährter Methoden
    ◊ Entwickeln 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
    ◊ Design einer Resilienzstrategie für Ransomware und andere Angriffe auf der Grundlage bewährter Microsoft-Sicherheitsmethoden
    ◊ Case Study: Entwerfen von Lösungen, die an den bewährten Sicherheitsmethoden und Prioritäten ausgerichtet sind

- ♦ **Entwerfen von Funktionen für Sicherheitsvorgänge, Identität und Compliance**
  - ♦ ◊ Entwickeln von Lösungen für die Einhaltung gesetzlicher Bestimmungen
    ◊ Entwerfen von Lösungen für die Identitäts- und Zugriffsverwaltung
    ◊ Entwicklung von Lösungen zum Schutz des privilegierten Zugriffs
    ◊ Design von Lösungen für Sicherheitsvorgänge
    ◊ Case Study: Entwerfen von Funktionen für Sicherheitsvorgänge, Identität und Compliance

- ♦ **Entwickeln von Sicherheitslösungen für Anwendungen und Daten**
  - ♦ ◊ Entwerfen von Lösungen zum Schutz von Microsoft 365
    ◊ Entwicklung von Lösungen zum Schutz von Anwendungen
    ◊ Entwerfen von Lösungen zum Schutz der Daten einer Organisation
    ◊ Case Study: Entwerfen von Sicherheitslösungen für Anwendungen und Daten

- ♦ **Entwerfen von Sicherheitslösungen für die Infrastruktur**
  - ♦ ◊ Entwerfen von Strategien zum Schutz von SaaS-, PaaS- und IaaS-Diensten
    ◊ Entwickeln von Lösungen für die Verwaltung des Sicherheitsstatus in Hybrid- und Multicloudumgebungen
    ◊ Design von Lösungen zum Schutz von Server- und Clientendpunkten
    ◊ Entwerfen von Lösungen für die Netzwerksicherheit
    ◊ Case Study: Entwerfen von Sicherheitslösungen für die Infrastruktur

- ♦ ◊