Implement end-to-end security controls for cloud and AI workloads (SC-500).

Ganzheitliche Cybersecurity für Microsoft-Umgebungen strategisch gestalten.

Seminar	Zurzeit keine Termine	Teilnahmebescheinigung
Präsenz / Virtual Classroom	32 Unterrichtseinheiten	

Seminarnummer: 29555 | Herstellernummer: MOC-SC-500

Stand: 22.09.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/29555

Der Kurs vermittelt Methoden und Technologien zur Absicherung moderner Microsoft-Cloudumgebungen. Schwerpunkte sind Identitätssicherheit, Cloud-Infrastrukturschutz, Bedrohungserkennung, Sicherheitsüberwachung sowie die **Absicherung von AI-Lösungen und autonomen Agents**.

In diesem Training erwerben Sie praxisrelevante Kenntnisse zur Planung, Implementierung und Verwaltung von Sicherheitskontrollen in Cloud-, Hybrid- und Multi-Cloud-Umgebungen. Sie lernen, Identitäten, Daten, Netzwerke, Infrastrukturen und AI-Workloads mit Microsoft-Sicherheitstechnologien zu schützen sowie Sicherheitsrisiken proaktiv zu minimieren. Praktische Übungen unterstützen den Transfer in den Arbeitsalltag.

Nutzen

Nach diesem Training

- konfigurieren Sie sichere Authentifizierungs- und Autorisierungskonzepte mit Microsoft Entra ID, einschließlich Multi-Faktor-Authentifizierung, passwortloser Verfahren und Self-Service Password Reset.
- implementieren Sie Just-in-Time-Zugriffsmodelle mit Privileged Identity Management (PIM) für Microsoft Entra-Rollen, Azure-Ressourcen und Gruppen.
- sichern Sie Azure Key Vault durch rollenbasierte Zugriffssteuerung, Netzwerkisolation, Schlüsselverwaltung sowie Überwachungs- und Schutzfunktionen von Microsoft Defender for Cloud ab.
- implementieren Sie Governance-, Compliance- und Least-Privilege-Konzepte mit Azure Policy, RBAC, Defender for Cloud und Infrastructure-as-Code-Ansätzen.
- konfigurieren Sie Sicherheits- und Netzwerkschutzmechanismen für Azure Storage einschließlich Zugriffskontrolle, Private Endpoints und Microsoft Defender for Storage.

- schützen Sie Azure SQL-Datenbanken durch Authentifizierung, Verschlüsselung, Netzwerkisolation, Auditierung und Bedrohungserkennung mit Microsoft Defender for Databases.
- analysieren Sie Sicherheitsereignisse, Compliance-Abweichungen und Risikosituationen in Cloud- und AI-Umgebungen und leiten geeignete Schutzmaßnahmen ab.

Zielgruppe

- Sicherheitsingenieur*innen
- Cloud Security Engineer*innen
- Microsoft Azure Administrator*innen mit Sicherheitsverantwortung
- IT-Sicherheitsverantwortliche in Cloud- und Hybridumgebungen
- Fachkräfte, die Sicherheitskontrollen für AI-Workloads implementieren und überwachen

Voraussetzungen

- praktische Erfahrung mit Microsoft Azure
- Kenntnisse zu Compute-, Netzwerk- und Storage-Diensten in Azure
- Gute Kenntnisse von Microsoft Entra ID
- Grundlegende Erfahrung in der Administration von Microsoft 365

Abschluss

Teilnahmebescheinigung

Teilnahmebescheinigung der TÜV Rheinalnd Akademie GmbH

Inhalte des Seminars

Sicherer Zugriff auf Ressourcen mithilfe von Microsoft Entra

- Verwalten und Implementieren von Authentizifierungsmethoden der Microsoft Entra-ID
- Implementieren und Konfigurieren von Privileged Identity Management (PIM)
- Authentifizieren der API-Plugins für deklarative Agenten mit abgesicherten APIs

Sichere Azure Key Vault mit detaillieter Verteidigung für cloud- und KI-Workloads

- Konfigurieren und Sichern von Azure Key Vault
- Verwalten von Schlüsseln und geheimen Schlüssen von Azure Key Vault
- Verwalten von Zertifikaten und Überwachen von azure Key Vault
- Schützen von Azure Key Vault mit Microsoft Defender for Cloud

Durchsetzungen von Sicherheitsgovernance und Einhaltung gesetzlicher Vorschiften

- Durchsetzung der Governance mit azure Policy und Ressourcensperren
- Konfigureiren von Sicherheitskontrollen und Korrekturempfehlungen in Defender for Cloud
- Bewerten der Einhaltung gesetzlicher Vorschriften in Defender for Cloud
- Verwalren und optimieren der RBAC-Rollenzuweisung für den geringsmöglichen Berechtigungsumpfang
- Schützen von Sicherungsdaten mit Azure Backup Sicherheitsfeatures
- Implementieren von Sicherheitskontrollen in der Infrastruktur als Code

Implementieren von Sicherheit für Azure Storage für cloud- und KI-Sicherheitstechniker

- Azure-Speicheridenste beschreiben
- Implementieren von Sicherheit und Verwalten des Zugriffs für Azure Storage
- Konfigurieren der Netzwerksicherheit für Azure Storage
- Microsoft Defender for Storage implementieren

Implementieren von Sicherheit für Azure SQL Datenbanken

- Konfigurieren der Sicherheit auf Plattformebene für Azure SQL
- Konfigurieren der Überwachung für Azure SQL-Datenbanken und SQL Managed Instance
- Implementieren von Microsoft Defender für Datenbanken

Wichtige Hinweise

Dieser Kurs ersetzt den AZ-500, der von Microsoft zum 31.08.2026 aus dem Programm genommen wird.

Damit Sie von einer möglichst hohen Durchführungschance profitieren, behalten wir uns vor, bei Bedarf mit dem autorisierten Microsoft Partner ETC – Enterprise Training Center GmbH zusammenzuarbeiten.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/29555 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.