Microsoft Cybersecurity Architect (SC-100T00)

Dieser Kurs vermittelt Ihnen das nötige Wissen für das Design und die Evaluierung von Cybersecuritystrategien in folgenden Bereichen: Zero Trust, Governance Risk Compliance (GRC), Security Operations (SecOps) sowie Daten und Anwendungen. Sie lernen außerdem, Lösungen mithilfe von Zero-Trust-Prinzipien zu entwerfen und Sicherheitsanforderungen für Cloudinfrastrukturen in verschiedenen Servicemodellen (SaaS, PaaS, IaaS) zu spezifizieren.

INHALTE

Einführung in Zero Trust und Frameworks bewährter Methoden

- Einführung in Zero Trust
- Zero Trust-Initiativen
- Zero Trust-Technologiepfeiler

Design von Lösungen, die am Cloud Adoption Framework (CAF) und dem Well-Architected Framework (WAF) ausgerichtet sind

- Definieren einer Sicherheitsstrategie
- Einführung in Cloud Adoption Framework
- Sichere Methodik: Cloud Adoption Framework
- Einführung in Azure-Zielzonen
- Entwurfssicherheit mit Azure-Zielzonen
- Einführung in Well-Architected Framework
- Well-Architected Framework – Sicherheitspfeiler

Design von Lösungen, die an der Microsoft Cybersecurity Reference Architecture (MCRA) und dem Microsoft Cloud Security Benchmark (MCSB) ausgerichtet sind

- Einführung in die Microsoft Cybersecurity Reference Architecture und in die Cloud Security Benchmark
- Entwerfen von Lösungen mit Best Practices für Funktionen und Kontrollen
- Entwerfen von Lösungen mit Best Practices für den Schutz vor Angriffen

Design einer Resilienzstrategie für gängige Cyberbedrohungen wie Ransomware

- Häufige Cyberbedrohungen und Angriffsmuster

PREIS P. P.

€ 2390,- (zzgl. MwSt.)

DAUER

4 Tage (09:00 - 17:00 Uhr)

SIE HABEN FRAGEN?

+43 50 4510-0

E-Mail Anfrage: office@tectrain.at

https://www.tectrain.at/seminare/microsoft-technisch/microsoft-security/microsoft-cybersecurity-architect

- Unterstützung von Geschäftsresilienz
- Ransomware-Schutz
- Konfigurationen für sichere Sicherungs- und Wiederherstellungsvorgänge
- Sicherheitsupdates

Entwerfen von Lösungen für die Einhaltung gesetzlicher Bestimmungen

- Einführung in die Einhaltung gesetzlicher Bestimmungen
- Übersetzen von Complianceanforderungen in eine Sicherheitslösung
- Erfüllen von Complianceanforderungen mit Microsoft Purview
- Erfüllen von Datenschutzanforderungen mit Microsoft Priva
- Erfüllen von Sicherheits- und Complianceanforderungen mit Azure Policy
- Beurteilen der Infrastrukturcompliance mit Defender for Cloud

Erstellen von Lösungen für die Identitäts- und Zugriffsverwaltung

- Einführung in die Identitäts- und Zugriffsverwaltung
- Entwerfen von Cloud-, Hybrid- und Multicloudzugriffsstrategien (einschließlich Azure AD)
- Entwerfen einer Lösung für externe Identitäten
- Entwerfen einer modernen Strategie für die Authentifizierung und Autorisierung
- Ausrichten von bedingtem Zugriff und Zero Trust
- Festlegen von Anforderungen zum Schutz von Active Directory Domain Services (AD DS)
- Entwerfen einer Lösung zum Verwalten von Geheimnissen, Schlüsseln und Zertifikaten

Entwerfen von Lösungen zum Schutz des privilegierten Zugriffs

- Einführung in den privilegierten Zugriff
- Das Enterprise-Zugriffsmodell
- Entwerfen von Lösungen zur Identitätsgovernance
- Entwerfen einer Lösung zum Sichern der Mandantenverwaltung
- Entwerfen einer Lösung für die Berechtigungsverwaltung der Cloudinfrastruktur (CIEM)
- Entwerfen einer Lösung für Arbeitsstationen mit privilegiertem Zugriff und Bastion-Dienste

Entwerfen von Lösungen für Sicherheitsvorgänge

- Einführung in Sicherheitsvorgänge (SecOps)

- Entwerfen von Sicherheitsbetriebsfunktionen in Hybrid- und Multicloudumgebungen
- Entwerfen einer zentralen Protokollierung und Überwachung
- Entwerfen von Lösungen für Security Information and Event Management (SIEM)
- Entwerfen von Lösungen für Erkennung und Reaktion
- Entwerfen einer Lösung für Security Orchestration, Automation und Response (SOAR)
- Entwerfen von Sicherheitsworkflows
- Entwerfen einer Bedrohungserkennungsabdeckung

Entwerfen von Lösungen zum Schutz von Microsoft 365

- Bewerten des Sicherheitsstatus für Zusammenarbeits- und Produktivitätsworkloads
- Entwerfen einer Microsoft 365 Defender-Lösung
- Entwurfskonfigurationen und Betriebspraktiken für Microsoft 365

Entwerfen von Lösungen zum Schutz von Anwendungen

- Einführung in die Anwendungssicherheit
- Entwerfen und Implementieren von Standards für die sichere Anwendungsentwicklung
- Bewerten des Sicherheitsstatus vorhandener Anwendungsportfolios
- Bewerten von Anwendungsbedrohungen mit Bedrohungsmodellierung
- Entwerfen einer Sicherheitsstrategie für den Lebenszyklus von Anwendungen
- Sicherer Zugriff für Workloadidentitäten
- Entwerfen einer Lösung für API Management und Sicherheit
- Entwerfen einer Lösung für sicheren Zugriff auf Anwendungen

Entwerfen von Lösungen zum Schutz der Daten einer Organisation

- Einführung in die Datensicherheit
- Entwerfen einer Lösung für die Datenermittlung und -klassifizierung mithilfe von Microsoft Purview
- Entwerfen einer Lösung für den Schutz von Daten
- Entwerfen der Datensicherheit für Azure-Workloads
- Entwerfen der Sicherheit für Azure Storage
- Entwerfen einer Sicherheitslösung, die Microsoft Defender for SQL und Microsoft Defender for Storage umfasst

Entwerfen einer Strategie zum Schutz von SaaS-, PaaS- und IaaS-Diensten

- Einführung in die Sicherheit für SaaS, PaaS und IaaS
- Angeben von Sicherheitsbaselines für SaaS-, PaaS- und IaaS-Dienste
- Angeben von Sicherheitsanforderungen für Webworkloads
- Angeben von Sicherheitsanforderungen für Container und Containerorchestrierung

Entwerfen von Lösungen für die Verwaltung des Sicherheitsstatus in Hybrid- und Multicloudumgebungen

- Einführung in die Verwaltung des Sicherheitsstatus in Hybrid- und Multicloudumgebungen
- Bewerten des Sicherheitsstatus mithilfe von Microsoft Cloud Security Benchmark
- Entwerfen der integrierten Verwaltung des Sicherheitsstatus und des Workloadschutzes
- Bewerten des Sicherheitsstatus mithilfe von Microsoft Defender for Cloud
- Statusauswertung mit der Sicherheitsbewertung in Microsoft Defender for Cloud
- Entwerfen des Cloudworkloadschutzes mit Microsoft Defender for Cloud
- Integrieren von Hybrid- und Multicloudumgebungen in Azure Arc
- Entwerfen einer Lösung für External Attack Surface Management

Entwerfen von Lösungen zum Schutz von Server- und Clientendpunkten

- Einführung in die Endpunktsicherheit
- Angeben von Sicherheitsanforderungen für Server
- Angeben von Anforderungen für mobile Geräte und Clients
- Angeben von Sicherheitsanforderungen für das Internet der Dinge (IoT) und eingebettete Geräte
- Schutz von operativer Technologie (OT) und industriellen Steuerungssystemen (ICS) mit Microsoft Defender for IoT
- Angeben von Sicherheitsbaselines für Server- und Clientendpunkte
- Entwerfen einer Lösung für sicheren Remotezugriff

Entwerfen von Lösungen für die Netzwerksicherheit

- Einführung
- Entwerfen von Lösungen für die Netzwerksegmentierung
- Entwerfen von Lösungen für die Datenverkehrsfilterung mit Netzwerksicherheitsgruppen
- Entwerfen von Lösungen für die Verwaltung des

Netzwerkstatus
- Entwerfen von Lösungen für die Netzwerküberwachung

ZIELGRUPPE

Security Architect, Solution Archtiect

VORAUSSETZUNGEN

Erfahrung mit Hybrid- und Cloudimplementierungen sowie Wissen in den Bereichen Identität und Zugriff, Plattformschutz, Sicherheitsvorgänge sowie Absicherung von Daten und Anwendungen

ZERTIFIZIERUNG

Dieser Kurs bereitet auf folgende Prüfung vor: SC-100

ABSCHLUSS

Nach Seminarabschluss erhalten Sie ein tecTrain-Teilnahmezertifikat.