>> Microsoft 365

Cybersecurity Architect

EGOS! the education company

Die Microsoft Cloud Lösungen haben ein vielfältiges Portfolio im Sicherheitsumfeld für Compliance, Identity, Risikomanagement und Detection.

Ihr Nutzen

In diesem Seminar erlernen Sie Cybersicherheitsstrategien in den folgenden Bereichen zu entwerfen und zu bewerten: Zero Trust, Governance Risk Compliance (GRC), Security Operations (SecOps) sowie Daten und Anwendungen. Außerdem lernen Sie, wie man Lösungen unter Verwendung von Zero-Trust-Prinzipien entwirft und gestaltet und Sicherheitsanforderungen für Cloud-Infrastrukturen in verschiedenen Servicemodellen (SaaS, PaaS, IaaS) spezifiziert.

Preis pro Teilnehmer

EUR 2550,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Voraussetzungen

Microsoft 365, Administration~9868

Hinweise

SC-100T00, Dieses Seminar dient zu Vorbereitung zur Zertifizierung Microsoft Certified: Cybersecurity Architect Expert

Version: 365

Seminarinhalte

1. Tag
* Aufbau einer Sicherheitsstrategie und -architektur
- Überblick über Zero Trust
- Integrationspunkte in einer Architektur
- Sicherheitsanforderungen auf der Grundlage von Geschäftszielen
- Umsetzen von Sicherheitsanforderungen in technische Möglichkeiten
- Sicherheit für eine Resilienz-Strategie entwickeln
- Sicherheitsstrategie für hybride und multi-tenant Umgebungen
- Strategiepläne für Technik und Governance zur Filterung und Segmentierung des Datenverkehrs
- Sicherheit von Protokollen

* Strategie für Security Operations
- Frameworks, Prozesse und Verfahren für Security Operations
- Entwurf einer Sicherheitsstrategie für Protokollierung und Auditing
- Entwicklung von Security Operations für hybride und Multi-Cloud-Umgebungen
- Strategie für Security Information and Event Management (SIEM) und Security Orchestration
- Bewertung von Security Workflows
- Überprüfung von Sicherheitsstrategien für das Incident Management
- Bewertung der Security Operations-Strategie für den Austausch technischer Bedrohungsdaten
- Monitoring von Quellen für Insights zu Gefahren und Gegenmaßnahmen

2. Tag
* Strategie für Identity Security
- Sicherer Zugriff auf Cloud-Ressourcen
- Einen Identity Store für Sicherheit empfehlen
- Empfehlen von Strategien zur sicheren Authentifizierung und Sicherheitsautorisierung
- Secure Conditional Access
- Entwicklung einer Strategie für die Rollenzuordnung und -delegation
- Definition von Identity Governance für Access Reviews und Entitlement Management
- Entwurf einer Sicherheitsstrategie für den Zugriff bevorzugter Rollen auf die Infrastruktur
- Entwurf einer Sicherheitsstrategie für bevorzugte Aktivitäten
- Verstehen der Sicherheit von Protokollen

* Strategie zur Einhaltung gesetzlicher Vorschriften
- Compliance-Anforderungen und ihre technischen Möglichkeiten
- Compliance-Scores und empfohlene Maßnahmen zur Behebung von
- Sicherheitsvorkehrungen mit Hilfe von Benchmarks
- Sicherheitsvorkehrungen mithilfe von Microsoft Defender for Cloud
- Sicherheitsvorkehrungen mit Secure Scores
- Sicherheitsvorkehrungen für Cloud Workloads
- Security für eine Azure Landing Zone
- Technische Threat Intelligence und Vorschläge zur Risikominimierung
- Sicherheitsfunktionen oder -kontrollen zur Minderung der identifizierten Risiken

* Best Practices in der Architektur und wie sie sich durch die Cloud verändern
- Planen und Implementieren einer teamübergreifenden Sicherheitsstrategie
- Festlegung einer Strategie und eines Prozesses für die proaktive und kontinuierliche Weiterentwicklung einer Sicherheitsstrategie
- Verstehen von Netzwerkprotokollen und Best Practices für Netzwerksegmentierung und Traffic-Filterung

* Strategie zur Sicherung von Server- und Client-Endpunkten
- Sicherheitsgrundlagen für Server- und Client-Endpoints
- Sicherheitsanforderungen für Server
- Sicherheitsanforderungen für mobile Geräte und Clients
- Anforderungen für die Sicherung von Active Directory-Domänendiensten
- Strategie zur Verwaltung von Secrets, Keys und Zertifikaten
- Strategie für den sicheren Remote-Zugriff
- Security Operations Frameworks, Prozesse und Methoden
- Detaillierte forensische Verfahren nach Ressourcentyp

4. Tag
* Strategie zur Sicherung von PaaS-, IaaS- und SaaS-Diensten
- Sicherheitsgrundlagen für PaaS-Dienste
- Sicherheitsgrundlagen für IaaS-Dienste
- Sicherheitsgrundlagen für SaaS-Dienste
- Sicherheitsanforderungen für IoT-Workloads
- Sicherheitsanforderungen für Daten-Workloads
- Sicherheitsanforderungen für Web-Workloads
- Sicherheitsanforderungen für Speicher-Workloads
- Sicherheitsanforderungen für Container
- Sicherheitsanforderungen für die Container-Orchestrierung

* Sicherheitsanforderungen für Anwendungen
- Application Threat Modeling
- Sicherheitsstandard für das Onboarding einer neuen Anwendung