Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

SC-100T00A Microsoft Cybersecurity Architect

This course is designed for students who are planning to take the corresponding certification exam, or students who are performing Cybersecurity Architect tasks in their daily job.

Both the certification exam and the courseware are based on the Microsoft Cybersecurity Architect role.
The Microsoft Cybersecurity Architect has subject matter expertise in designing and evolving cybersecurity solutions that protect an organization's mission and business processes across all aspects of the enterprise architecture. Responsibilities include designing reference models, integrating security into architectures, designing security architectures, and ensuring the resiliency of the organization.

The Cybersecurity Architect gathers the client's business and security requirements, selects appropriate security capabilities, and translates the requirements into architectural specifications that minimize risk, meet compliance and privacy requirements, adhere to best practices, and ensure appropriate levels of confidentiality, integrity, availability, and safety for critical business assets. The Cybersecurity Architect ensures successful deployments and the ongoing technical viability of solutions and through assessments and reviews of the security posture.

The Cybersecurity Architect continuously collaborates with Security Engineers, Security Operations Analysts, Identity and Access Management Admins, Information Protection Admins, Cloud Security (Azure/M365) Administrator/Engineers, privacy officers, governance, compliance, and risk roles, and solution providers to plan and implement a cybersecurity strategy that meets the business needs of an organization.

The Cybersecurity Architect must be familiar with Microsoft security and identity technologies, hybrid cloud and workload security configurations, and cloud application development solutions. The Cybersecurity Architect must have skills and experience in applying cybersecurity concepts and practices,information security, application security, incident response and recovery techniques, and security standards, policies, and governance frameworks.

Détails

- Code : SC-100T00A
- Durée : 4 jours (28 heures)

Public
- Administrateurs de Cloud
- Administrateurs systèmes
- Architectes de Système
- Architectes techniques
- Cloud Solution Architects
- Developers IT
- Développeurs Cloud
- Ingénieurs Sécurité
- Responsable Sécurité

Pré-requis
- Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications + Experience with hybrid and cloud implementations.

Objectifs
- Design a Zero Trust strategy and architecture
- Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies
- Design security for infrastructure
- Design a strategy for data and applications
- Recommend security best practices

Programme

1. Design a Zero Trust strategy and architecture
- Build overall security strategy and architecture
- Design a security operations strategy
- Design an identity security strategy

2. Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies
- Evaluate a regulatory compliance strategy
- Evaluate security posture and recommend technical strategies to manage risk

3. Design security for infrastructure
- Understand architecture best practices and how they are changing with the Cloud
- Designing a strategy for securing server and client endpoints
- Design a strategy for securing PaaS, IaaS and SaaS

services

4. Design a strategy for data and applications

- Specify security requirements for applications
- Design a strategy for securing data

5. Recommend security best practices

- Recommend security best practices using Microsoft Cybersecurity Reference Architectures (MCRA) and Microsoft Cloud Security Benchmarks
- Recommend a secure methodology using the Cloud Adoption Framework (CAF)
- Recommend a ransomware strategy by using Microsoft Security Best Practices

Modalités

- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages