Microsoft Cybersecurity Architect (4 Days)

Course Overview

This course prepares students with the background to design and evaluate cybersecurity strategies in the following areas: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications. Students will also learn how to design and architect solutions using zero trust principles and specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS).
IT professionals with advanced experience and knowledge in a wide range of security engineering areas, including identity and access, platform protection, security operations, securing data, and securing applications. They should also have experience with hybrid and cloud implementations.

Course Benefits

- 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.

Class Prerequisites

Experience in the following *is required* for this Microsoft Security class:

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

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Course Outline

Build an overall security strategy and architecture

- Zero Trust overview
- Develop Integration points in an architecture
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- Design security for a resiliency strategy
- Design a security strategy for hybrid and multi-tenant environments
- Design technical and governance strategies for traffic filtering and segmentation
- Understand security for protocols
- Exercise: Build an overall security strategy and architecture
- Knowledge check

Design a security operations strategy

- Understand security operations frameworks, processes, and procedures
- Design a logging and auditing security strategy
- Develop security operations for hybrid and multi-cloud environments
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration,
- Evaluate security workflows
- Review security strategies for incident management
- Evaluate security operations strategy for sharing technical threat intelligence
- Monitor sources for insights on threats and mitigations

Design an identity security strategy

- Secure access to cloud resources
- Recommend an identity store for security
- Recommend secure authentication and security authorization strategies
- Secure conditional access
- Design a strategy for role assignment and delegation
- Define Identity governance for access reviews and entitlement management
- Design a security strategy for privileged role access to infrastructure
- Design a security strategy for privileged activities
- Understand security for protocols

Evaluate a regulatory compliance strategy

- Interpret compliance requirements and their technical capabilities
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security
- Design and validate implementation of Azure Policy
- Design for data residency Requirements
- Translate privacy requirements into requirements for security solutions

Evaluate security posture and recommend technical strategies to manage risk

- Evaluate security postures by using benchmarks
- Evaluate security postures by using Microsoft Defender for Cloud
- Evaluate security postures by using Secure Scores
- Evaluate security hygiene of Cloud Workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

Understand architecture best practices and how they are changing with the Cloud

- Plan and implement a security strategy across teams
- Establish a strategy and process for proactive and continuous evolution of a security strategy
- Understand network protocols and best practices for network segmentation and traffic filtering

Design a strategy for securing server and client endpoints

- Specify security baselines for server and client endpoints
- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify requirements for securing Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access
- Understand security operations frameworks, processes, and procedures
- Understand deep forensics procedures by resource type

Design a strategy for securing PaaS, IaaS, and SaaS services

- Specify security baselines for PaaS services
- Specify security baselines for IaaS services
- Specify security baselines for SaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads
- Specify security requirements for web workloads
- Specify security requirements for storage workloads
- Specify security requirements for containers
- Specify security requirements for container orchestration

Specify security requirements for applications

- Understand application threat modeling
- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application
- Specify a security strategy for applications and APIs

Design a strategy for securing data

- Prioritize mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion