CORSO MOC SC-100:
MICROSOFT CYBERSECURITY ARCHITECT

Durata: 4 giorni

★ *TopSelection*

PROGRAMMA

MODULO 1: BUILD AN OVERALL SECURITY STRATEGY AND ARCHITECTURE

- Zero Trust overview
- Develop Integration points in an architecture
- Design security for a resiliency strategy
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- 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

MODULO 2: 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

MODULO 3: 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

CONTATTI

info@nexsys.it

www.nexsys.it

MODULO 4: 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

MODULO 5: EVALUATE SECURITY POSTURE AND RECOMMEND TECHNICAL STRATEGIES TO MANAGE RISK

- Evaluate security postures by using benchmarks, Microsoft Defender for Cloud, and 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

MODULO 6: 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

MODULO 7: DESIGN A STRATEGY FOR SECURING SERVER AND CLIENT ENDPOINTS

- Specify security baselines for server and client endpoints and 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

MODULO 8: DESIGN A STRATEGY FOR SECURING PAAS, IAAS, AND SAAS SERVICES

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

MODULO 9: SPECIFY SECURITY REQUIREMENTS FOR APPLICATIONS

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

MODULO 10: 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

Scopri di più sul Corso MOC SC-100: Microsoft Cybersecurity Architect.

CORSO MOC SC-100:
MICROSOFT CYBERSECURITY ARCHITECT

Durata: 4 giorni

NEXSYS
LEARN IT, TRANSFORM IT

★ *TopSelection*

OVERVIEW DEL CORSO

Il corso MOC SC-100 – Microsoft Cybersecurity Architect prepara i partecipanti a progettare e valutare strategie di cybersecurity in ambito Zero Trust, Governance Risk Compliance (GRC), operazioni di sicurezza (SecOps), dati e applicazioni. I partecipanti impareranno, inoltre, a progettare e ad architettare soluzioni che utilizzano i principi dello Zero Trust e a specificare i requisiti di sicurezza per le infrastrutture cloud in diversi modelli di servizio (SaaS, PaaS, IaaS).

A CHI È RIVOLTO IL CORSO?

Il corso MOC SC-100 è rivolto a professionisti IT con esperienza e conoscenze avanzate in un'ampia gamma di aree di security engineering, tra cui identità e accesso, protezione delle piattaforme, operazioni di sicurezza, protezione dei dati e protezione delle applicazioni. Si raccomanda inoltre di avere esperienza nelle implementazioni ibride e nel cloud.

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- progettare una strategia e un'architettura Zero Trust;
- valutare le strategie tecniche di Governance Risk Compliance (GRC) e le strategie operative di sicurezza;
- progettare la sicurezza per l'infrastruttura;
- progettare una strategia per i dati e le applicazioni.

CONTATTI

info@nexsys.it

www.nexsys.it