CORSO SC-500: SICUREZZA END-TO-END CLOUD E AI

Durata: 28 ore

PROGRAMMA

MODULO 1: PROTEGGERE L'ACCESSO ALLE RISORSE USANDO MICROSOFT ENTRA

- Gestire e implementare i metodi di autenticazione in Microsoft Entra ID
- Implementare e configurare Privileged Identity Management (PIM)
- Autentica il tuo plug-in API per gli agenti dichiarativi con API protette

MODULO 2: PROTEGGERE AZURE KEY VAULT CON DIFESA AVANZATA PER I CARICHI DI LAVORO CLOUD E DI INTELLIGENZA ARTIFICIALE

- Configurare e proteggere Azure Key Vault
- Gestire chiavi e segreti in Azure Key Vault
- Gestire i certificati e monitorare Azure Key Vault
- Proteggere Azure Key Vault con Microsoft Defender per il cloud

MODULO 3: APPLICARE LA GOVERNANCE DELLA SICUREZZA E LA CONFORMITÀ ALLE NORMATIVE

- Applicare la governance con blocchi di risorse e Criteri di Azure
- Configurare i controlli di sicurezza e correggere le raccomandazioni in Defender per il cloud
- Valutare la conformità alle normative in Defender per il cloud
- Gestire e adeguare le assegnazioni di ruolo RBAC a privilegi minimi
- Proteggere i dati di backup con funzionalità di sicurezza Backup di Azure
- Implementare i controlli di sicurezza nell'infrastruttura come codice

MODULO 4: IMPLEMENTARE LA SICUREZZA DI ARCHIVIAZIONE DI AZURE PER L'INGEGNERE DELLA SICUREZZA PER IL CLOUD E L'IA

- Descrivere i servizi di archiviazione di Azure
- Implementare la sicurezza e gestire l'accesso per Archiviazione di Azure
- Configurare la sicurezza di rete per Archiviazione di Azure
- Implementare Microsoft Defender per l'archiviazione

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO SC-500: SICUREZZA END-TO-END CLOUD E AI

Durata: 28 ore

MODULO 5: IMPLEMENTARE LA SICUREZZA PER I DATABASE AZURE SQL

- Configurare la sicurezza a livello di piattaforma per Azure SQL
- Configurare il controllo per database SQL di Azure e Istanza gestita di SQL
- Implementare Microsoft Defender per i database

MODULO 6: IMPLEMENTARE CONTROLLI DI SICUREZZA DI RETE IN AZURE

- Segmentare e isolare i carichi di lavoro Azure usando i controlli di sicurezza di rete
- Centralizzare e applicare l'ispezione del traffico usando Firewall di Azure
- Proteggere la connettività remota e ibrida usando gateway VPN e Accesso privato Microsoft Entra
- Eliminare l'esposizione della rete pubblica dei servizi PaaS Azure

MODULO 7: Implementare la sicurezza per l'intelligenza artificiale

- Accesso protetto per l'identità dell'agente di Microsoft Entra
- Analizzare i rischi di identità di intelligenza artificiale usando Microsoft Defender XDR
- Abilitare la protezione in tempo reale per gli agenti di Copilot Studio
- Configurare la sicurezza del gateway di intelligenza artificiale in Microsoft Foundry
- Configurare e gestire protezioni in Microsoft Foundry
- Proteggere i carichi di lavoro di intelligenza artificiale con Microsoft Defender per il cloud
- Abilitare Defender per i servizi di intelligenza artificiale protezione del carico di lavoro in Microsoft Defender per il cloud
- Gestire gli agenti usando Microsoft Agent 365
- Identificare i rischi per i dati di intelligenza artificiale usando Gestione della postura di sicurezza dei dati di Microsoft Purview

MODULO 8: IMPLEMENTARE LA SICUREZZA PER SERVER E MACCHINE VIRTUALI

- Implementare la crittografia del disco per le macchine virtuali Azure
- Configurare le funzionalità di sicurezza di avvio attendibili per Azure macchine virtuali
- Pianificare e implementare Azure Bastion
- Gestire la sicurezza per i server ibridi abilitati per Arc
- Implementare Microsoft Defender per i server
- Abilitare e applicare l'accesso just-in-time alle macchine virtuali
- Applicare la configurazione di sicurezza delle macchine virtuali con Azure Machine Configuration

CONTATTI info@nexsys.it www.nexsys.it

CORSO SC-500: SICUREZZA END-TO-END CLOUD E AI

Durata: 28 ore

MODULO 9: PROTEGGERE I SERVIZI DELLA PIATTAFORMA DELLE APPLICAZIONI AZURE PER IL TECNICO DELLA SICUREZZA CLOUD E DELL'INTELLIGENZA ARTIFICIALE

- Rilevare i rischi dei contenitori usando Microsoft Defender per i contenitori
- Implementare i controlli di sicurezza per servizio Azure Kubernetes
- Implementare controlli di sicurezza per Registro Azure Container, Istanze di Container e app contenitore
- Implementare controlli di sicurezza per le app per le funzioni Azure e le app per la logica
- Implementare controlli di sicurezza per app Azure Services e Web application firewall
- Implementare la sicurezza back-end dell'API usando Gestione API di Azure

MODULO 10: GESTIRE LA POSTURA DI SICUREZZA USANDO MICROSOFT DEFENDER PER IL CLOUD

- Connettere ambienti ibridi e multicloud a Microsoft Defender for Cloud
- Identificare i rischi per la sicurezza usando la gestione del comportamento di sicurezza cloud
- Individuare asset e vulnerabilità non protetti usando Microsoft Defender External Attack Surface Management
- Valutare la conformità alle normative in Defender for Cloud
- Abilitare e configurare i piani di protezione del carico di lavoro in Microsoft Defender for Cloud
- Configurare le impostazioni di Microsoft Defender Vulnerability Management per le macchine virtuali Azure

MODULO 11: IMPLEMENTAZIONE DELLA RACCOLTA DI ATTIVITÀ ED EVENTI IN MICROSOFT SENTINEL

- Creare e gestire le aree di lavoro di Microsoft Sentinel
- Gestire il contenuto in Microsoft Sentinel
- Connettere i servizi Microsoft a Microsoft Sentinel
- Connettere origini dati Syslog a Microsoft Sentinel
- Connettere i log Common Event Format a Microsoft Sentinel
- Connettere host Microsoft a Microsoft Sentinel
- Implementare regole e playbook di automazione in Microsoft Sentinel
- Gestire l'archiviazione dei dati e i registri di controllo delle query in Microsoft Sentinel

MODULO 12: DISTRIBUIRE E GESTIRE MICROSOFT SECURITY COPILOT

- Descrivi Microsoft Security Copilot
- Configurare le aree di lavoro per Microsoft Security Copilot
- Gestione di plug-in e agenti in Microsoft Security Copilot

CONTATTI info@nexsys.it www.nexsys.it

CORSO SC-500: SICUREZZA END-TO-END CLOUD E AI

Durata: 28 ore

OVERVIEW DEL CORSO

La sicurezza cloud non si ferma più a rete, identità e dati: oggi comprende anche gli agenti AI che operano nei tuoi ambienti Microsoft. Con la diffusione di agenti autonomi, copiloti e workload basati su intelligenza artificiale, il perimetro da proteggere si è allargato — e con esso le competenze richieste a chi se ne occupa.

Il corso SC-500 forma security engineer capaci di progettare, implementare e gestire controlli di sicurezza end-to-end su Microsoft Azure e Microsoft 365, in ambienti ibridi e multicloud. Il percorso copre l'intero spettro della disciplina: governance degli accessi e delle identità con Microsoft Entra ID, protezione di storage, database e infrastrutture di rete, rilevamento e risposta alle minacce con Microsoft Defender XDR, fino alla protezione specifica dei carichi di lavoro AI — inclusi gli agenti autonomi in Copilot Studio, la gestione dell'identità con Microsoft Entra Agent ID e l'analisi del rischio ad essi collegato.

Il corso prepara all'esame Microsoft SC-500, propedeutico alla certificazione Microsoft Certified: Cloud and AI Security Engineer Associate, ed è pensato per chi lavora già a stretto contatto con architetti, amministratori e sviluppatori su Azure, Microsoft 365, identità e infrastrutture — e vuole presidiare in prima persona la sicurezza dei sistemi che oggi includono anche l'intelligenza artificiale.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Security engineer responsabili della sicurezza di sistemi e dati su ambienti cloud, ibridi e multicloud
- Professionisti con un ruolo trasversale su identità, rete, applicazioni, dati e infrastrutture
- Chi presidia la sicurezza dei carichi di lavoro AI
- Chi ha esperienza con SC-200, SC-300 o SC-100 e vuole una visione end-to-end che includa anche l'AI

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Gestire identità, accessi e governance in ambienti cloud e ibridi con Microsoft Entra ID
- Proteggere storage, database e infrastrutture di rete secondo i principi Zero Trust
- Rilevare e rispondere alle minacce con Microsoft Defender XDR, Defender for Servers e Defender for Containers
- Implementare controlli di sicurezza specifici per i carichi di lavoro AI: agenti Copilot Studio, Microsoft Entra Agent ID, analisi del "blast radius" dei rischi legati agli agenti
- Applicare configurazioni di sicurezza e compliance trasversali su Azure, Microsoft 365 e ambienti multicloud

CONTATTI

info@nexsys.it

www.nexsys.it