CORSO PLANNING AND IMPLEMENTING MICROSOFT SENTINEL (SIEM & SOAR)

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: PANORAMICA DI MICROSOFT SENTINEL

- Panoramica di Microsoft Sentinel;
- Metodi di immissione dei dati;
- Microsoft Sentinel per MSSP;
- Analisi del comportamento degli utenti e delle entità;
- Fusion;
- Notebooks;
- Strumenti di gestione e automazione;
- Registri e costi;

MODULO 2: KQL

- Importanza di KQL in Azure;
- L'interfaccia utente;
- La struttura KQL standard;
- Comandi KQL comuni;

MODULO 3: DATA CONNECTORS

- Gestisci il contenuto in Microsoft Sentinel;
- Connetti i dati a Microsoft Sentinel utilizzando i connettori dati;
- Connetti i servizi Microsoft a Microsoft Sentinel;
- Connetti Microsoft 365 Defender a Microsoft Sentinel;
- Connetti gli host Windows a Microsoft Sentinel;
- Connetti i registri del formato eventi comune a Microsoft Sentinel;
- Connetti le origini dati syslog a Microsoft Sentinel;
- Connetti gli indicatori di minaccia a Microsoft Sentinel;

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO PLANNING AND IMPLEMENTING MICROSOFT SENTINEL (SIEM & SOAR)

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

MODULO 4: REGOLE DI ANALISI

- Rilevamento delle minacce con l'analisi Microsoft Sentinel;
- Automazione in Microsoft Sentinel;
- Risposta alle minacce con i playbook Microsoft Sentinel;

MODULO 5: INCIDENT MANAGEMENT

- Panoramica sulla gestione degli incidenti;
- Analisi del comportamento degli utenti e delle entità;
- Normalizzazione dei dati in Microsoft Sentinel;
- Interrogare, visualizzare e monitorare i dati;

MODULO 6: HUNTING

- Concetti di caccia alla minaccia;
- Caccia alle minacce con Microsoft Sentinel;
- Utilizzare i processi di ricerca in Microsoft Sentinel;
- Caccia alle minacce utilizzando i notebook;

MODULO 7: LISTE DI CONTROLLO

- Dare priorità agli incidenti;
- Importa dati aziendali;
- Ridurre l'affaticamento da allerta;
- Arricchisci i dati degli event;

MODULO 8: THREAT INTELLIGENCE

- Panoramica sulla Threat Intelligence;
- Threat Intelligence in Microsoft Sentinel;

Scopri di più sul Corso Planning and Implementing Microsoft Sentinel.

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO PLANNING AND IMPLEMENTING MICROSOFT SENTINEL (SIEM & SOAR)

Durata: 3 giorni

NEXSYS
LEARN IT, TRANSFORM IT

OVERVIEW DEL CORSO

Il Corso Planning and Implementing Microsoft Sentinel offre un percorso tecnico e pratico che permette di comprendere e gestire in profondità le logiche operative della soluzione SIEM & SOAR di Microsoft. Attraverso esercitazioni e simulazioni, i partecipanti apprendono come integrare dati provenienti da fonti diverse, configurare connettori e regole, analizzare avvisi e monitorare in tempo reale la sicurezza aziendale. Microsoft Sentinel, piattaforma cloud-native, unisce funzionalità avanzate di gestione eventi e informazioni di sicurezza (SIEM) con strumenti di orchestrazione, automazione e risposta (SOAR), sfruttando anche l'intelligenza artificiale per rilevare, investigare e neutralizzare le minacce in modo rapido ed efficace.
La formazione consente di acquisire competenze pratiche per implementare e ottimizzare Sentinel, migliorando la scalabilità e riducendo la complessità rispetto alle soluzioni tradizionali. Guidati da trainer certificati Microsoft, i partecipanti esplorano architettura, configurazione e gestione degli incidenti, approfondendo le tecniche di ricerca proattiva e l'automazione dei processi di risposta, con l'obiettivo di sviluppare una visione completa e strategica della sicurezza in ambiente cloud.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Professionisti IT.
- System Admin Esperti.
- Amministratori Azure.
- Amministratori di sicurezza.
- Esperti del settore che desiderano ampliare le proprie competenze nella gestione delle minacce e nell'implementazione di soluzioni avanzate di sicurezza.

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Esaminare gli elementi essenziali dell'intelligence sulle minacce.
- Raccogliere e monitorare i dati di log dagli avvisi dei servizi e dagli endpoint.
- Creare e convalidare regole di analisi per generare casi investigativi.
- Ricercare in modo proattivo le minacce per prevenire e affrontare gli attacchi.

CONTATTI

info@nexsys.it

www.nexsys.it