Hands-On Productivo
Microsoft Sentinel

Onboarding a Microsoft Sentinel mediante curso práctico distribuido en 5 módulos con transferencia de conocimiento, participación práctica, recomendaciones, configuración y puesta en producción del producto.

MÓDULOS

1 — **2 Horas**

Introducción
Que es Microsoft Sentinel
¿Por qué es importante?
Diseño de Workspaces
Hands-On : Habilitar Microsoft Sentinel
Resumen

2 — **2 Horas**

Introducción
Tipos de conectores Microsoft Sentinel
Hands-On : Conectar a Azure AD
Hands-On : Conectar a Office 365
Hands-On : Conectar a Azure AD
Hands-On : Conectar a Azure Activity
Hands-On : Microsoft Sentinel Workbooks

3 — **2 Horas**

Introducción
Threat Detection Using Analytics
KQL
Hands-On : KQL refresher
Entendiendo Analytic rules
Hands-on : Creando incidentes desde Security Alerts
Hands-on: Creando schedule rules y detección de amenazas
Resumen

5 — **4 Horas**

Que es SOAR
Hands-On: Logic App Refresh
¿Que son Security playbooks?
Automatización en tiempo real
Automatización bajo demanda
Microsoft Sentinel API
Hands-On: incidentes
Hands-On: Ingestando datos
Resumen

4 — **2 Horas**

Introducción
Comprender incidentes y ciclo de vida
Hands-On: incidentes
Hands-On: Threat hunting e investigación con bookmark
Resumen

“Obtén conocimiento dinámico del producto entrenamiento e implementación en vivo”

ALCANCES:

- 5 Módulos prácticos de 12 horas total
- Implementación del producto Microsoft Sentinel
- Audiencia por módulo 5 usuarios

RESUMEN ACTIVIDADES

1) Visión General
2) Introducción a Microsoft Sentinel
3) Introducción de datos en Microsoft Sentinel y uso de workbooks
4) Detección de amenazas
5) Gestión e investigación de incidentes
6)Integración y automatización

Nebulan
SOLUCIONES QUE TRANSFORMAN TU NEGOCIO

Nebulan - ¡Contáctenos hoy para comenzar!

contacto@nebulan.cl / (+56) 226113660 www.nebulan.cl