NETXPRESS Academy

TEMARIO

CURSO OFICIAL

SC-200

Analista de Operaciones de Seguridad de Microsoft

Investigue, busque y mitigue amenazas mediante Microsoft Sentinel, Microsoft Defender para la nube y Microsoft 365 Defender.

Microsoft Partner

SOBRE NOSOTROS

En **Netxpresss Academy** impulsamos tu crecimiento profesional con capacitación oficial de alto nivel, instructores certificados y un enfoque práctico orientado a resultados

Partners Autorizados

Instructores Oficiales

Capacitación Oficial

+5,000 alumnos

NUESTROS PARTNERS

TÓPICOS A DESARROLLAR

1. Fundamentos de las Operaciones de Seguridad

- **Rol del Security Operations Analyst**
- **Conceptos de SOC, detección y respuesta a amenazas**
- **Microsoft Defender XDR y ecosistema de seguridad Microsoft**
- **Introducción a incidentes, alertas y gestión de riesgos**

2. Administración del Entorno de Operaciones de Seguridad

- **Configuración de notificaciones y alertas**
- **Ajuste, supresión y correlación de alertas**
- **Automatización en Microsoft Defender XDR y Microsoft Sentinel**
- **Análisis de cobertura mediante MITRE ATT&CK**
- **Configuración y análisis de anomalías**

3. Investigación y Respuesta a Incidentes

- **Investigación de alertas e incidentes en Microsoft Defender XDR**
- **Investigación de amenazas en Microsoft Defender for Office 365**
- **Investigación de identidades comprometidas con Microsoft Entra ID**
- **Análisis de amenazas con Microsoft Defender for Identity**
- **Investigación de riesgos en Defender for Cloud Apps**
- **Gestión de incidentes y casos de seguridad**
- **Investigación de ataques complejos y movimientos laterales**
- **Uso de Microsoft Security Copilot en la investigación de amenazas**

TÓPICOS A DESARROLLAR

4. Protección e Investigación de Endpoints

- **Investigación de líneas de tiempo de dispositivos**
- **Análisis de evidencias y entidades**
- **Live Response y acciones de respuesta**
- **Recopilación de paquetes de investigación**
- **Investigación y mitigación mediante Automatic Attack Disruption**

5. Investigación de Actividades en Microsoft 365

- **Investigación mediante Microsoft Purview Audit**
- **Búsqueda de amenazas con Content Search y eDiscovery**
- **Análisis de actividades mediante Microsoft Graph**

6. Threat Hunting con Microsoft Defender XDR

- **Introducción a Kusto Query Language (KQL)**
- **Selección de tablas y fuentes de datos**
- **Creación de consultas de Advanced Hunting**
- **Análisis de Threat Analytics**
- **Hunting Graphs y análisis de Blast Radius**
- **Análisis de relaciones entre entidades con Sentinel Graph**

7. Threat Hunting con Microsoft Sentinel

- **Creación y monitoreo de Hunting Queries**
- **Gestión de trabajos KQL en Data Lake**
- **Summary Rule Tables para consultas**
- **Investigación de amenazas mediante Notebooks**
- **Integración con Sentinel MCP Server**

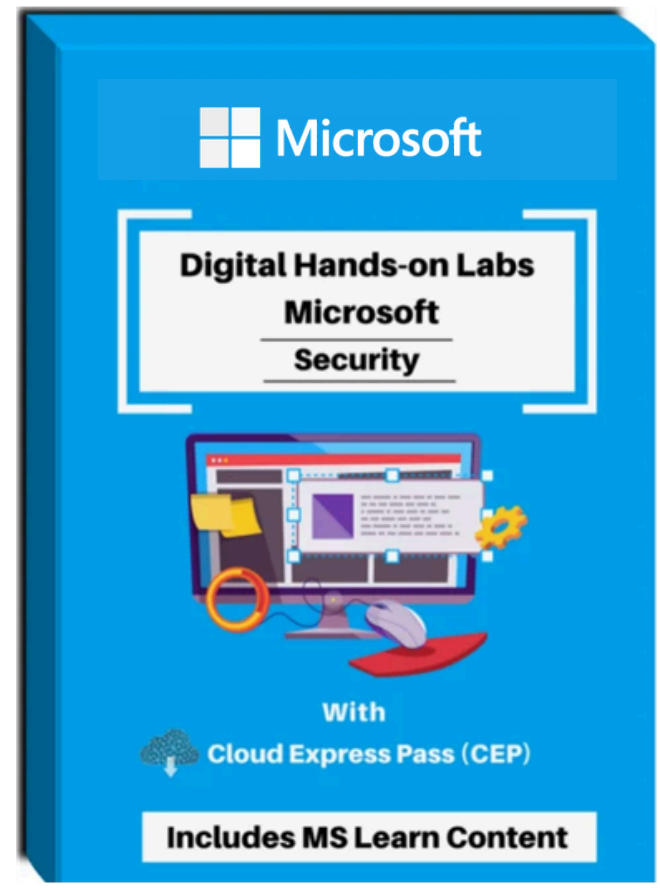
BENEFICIOS DEL CURSO

- Curso Oficial
- Clases Online En Vivo
- Grabaciones de las Clases
- Certificado de Participación
- Laboratorios oficiales
- Voucher de examen*
- Mesa de Ayuda

**El voucher de examen aplicará solo si escoge dicho paquete.*

LABORATORIOS OFICIALES

Este laboratorio incluye contenido de **Microsoft Learn**, totalmente integrado en el portal de la cuenta y en el entorno de laboratorio. Aprende a investigar, responder y realizar búsqueda de amenazas (Threat Hunting) utilizando **Microsoft Sentinel, Microsoft Defender for Cloud y Microsoft 365 Defender.**
En este laboratorio práctico oficial de Microsoft, aprenderás a mitigar ciberamenazas utilizando estas tecnologías.



Específicamente, configurarás y utilizarás **Microsoft Sentinel**, además de emplear **Kusto Query Language (KQL)** para realizar actividades de detección, análisis y generación de informes.

El laboratorio ha sido diseñado para personas que trabajan en funciones de **Operaciones de Seguridad (Security Operations)** y ayuda a los participantes a prepararse para el examen **SC-200: Microsoft Security Operations Analyst.**

CONTÁCTANOS

Sofía Rivas
+51 936 824 055 *(WhatsApp Only)*
sofia@netxpress-la.com
Ejecutiva Comercial B2C

Alonso Sal y Rosas
+51 956 347 272
alonso@netxpress-la.com
Ejecutivo Comercial B2B

Aprende con expertos, fortalece tus competencias y da el siguiente paso hacia una certificación reconocida internacionalmente.