Microsoft Security Operations Analyst (SC-200)

Detalles del curso:

Duración: 24 h.

Modalidad: Aula virtual

Certificación: Oficial

Información e inscripción:

685 457 610 - 615 844 193

formacion@laberit.com

LÄBERIT | CENTRO DE FORMACIÓN TIC.

Microsoft Security Operations Analyst (SC-200)

LÁBERIT CENTRO DE FORMACIÓN TIC

Introducción

Aprenda a investigar y buscar amenazas, y a responder a ellas, mediante Microsoft Sentinel, Microsoft Defender XDR y Microsoft Defender for Cloud. En este curso aprenderá a mitigar ciberamenazas mediante estas tecnologías. En concreto, configurará y usará Microsoft Sentinel, así como el lenguaje de consulta Kusto (KQL), para realizar la detección, el análisis y la generación de informes. El curso se diseñó para personas que desempeñan un rol de trabajo de operaciones de seguridad y ayuda a los alumnos a prepararse para el examen SC-200: Microsoft Security Operations Analyst.

¿Por qué hacer este curso?

Vivimos en una era en la que las amenazas cibernéticas evolucionan constantemente, y las organizaciones necesitan profesionales capaces de actuar con rapidez, detectar ataques y responder de forma eficaz. Este curso te prepara para asumir ese rol, brindándote las habilidades necesarias para proteger los activos y operaciones de una empresa en entornos **híbridos y multinube**.

Además, completar esta formación te capacita para obtener la certificación **Microsoft Certified: Security Operations Analyst Associate**, una credencial reconocida que puede impulsar tu carrera profesional en ciberseguridad.

¿En qué consiste la formación en Analista de operaciones de seguridad de Microsoft?

Este curso intensivo de **cuatro días** se centra en el diseño, implementación y gestión de soluciones de operaciones de seguridad utilizando herramientas de Microsoft. Aborda áreas clave como:

- **Microsoft Sentinel:** implementación, configuración y uso para detección de amenazas, investigación y respuesta.
- **Microsoft Defender XDR:** uso de Defender for Endpoint, Defender for Office 365, Defender for Identity y Defender for Cloud Apps para proteger entornos de trabajo.
- **Microsoft Defender for Cloud:** configuración de directivas de seguridad y remediación de alertas en infraestructuras cloud.
- **Kusto Query Language (KQL):** creación de consultas y detección personalizada de amenazas.

Microsoft Security Operations Analyst (SC-200)

A través de sesiones teóricas y prácticas, el curso permite a los participantes dominar las herramientas clave de Microsoft para operaciones de seguridad modernas.

¿A quién va dirigido?

El rol Analista de operaciones de seguridad de Microsoft colabora con las partes interesadas de la organización para proteger los sistemas de tecnología de la información de la organización. Su objetivo es reducir los riesgos de la organización mediante la corrección rápida de ataques activos en el entorno, el asesoramiento sobre mejoras de los procedimientos de protección contra amenazas y la comunicación de las infracciones de directivas de la organización a las partes interesadas pertinentes. Entre sus responsabilidades están la administración y la supervisión de amenazas y la respuesta a estas mediante diferentes soluciones de seguridad en el entorno. El rol se ocupa principalmente de investigar y detectar amenazas, así como de responder a ellas, mediante Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Cloud y productos de seguridad de terceros. Dado que el analista de operaciones de seguridad es quien va a hacer uso de los resultados operativos de estas herramientas, también es una parte interesada fundamental en la configuración e implementación de estas tecnologías.

Objetivos didácticos

El objetivo general es dotarte de los conocimientos y habilidades necesarios para detectar, investigar y responder a amenazas activas mediante las soluciones de seguridad de Microsoft. Al finalizar el curso, estarás capacitado para:

- Configurar y usar **Microsoft Sentinel** para detección, investigación y respuesta.
- Implementar soluciones con **Microsoft Defender for Endpoint**, **Defender for Office 365**, **Defender for Identity** y **Defender for Cloud Apps**.
- Detectar, analizar y responder a amenazas usando **Kusto Query Language (KQL)**.
- Administrar alertas de seguridad y priorizar incidentes.
- Configurar y usar **Microsoft Defender for Cloud** para proteger entornos híbridos y multinube.

Microsoft Security Operations Analyst (SC-200)

Metodología

El curso combina sesiones teóricas con prácticas, utilizando un enfoque basado en proyectos y retos reales. Se fomenta la participación de los asistentes, promoviendo el aprendizaje colaborativo y la aplicación de los conocimientos adquiridos en situaciones prácticas.

Salidas profesionales u opciones de promoción profesional

Este curso está dirigido a profesionales que quieran especializarse o avanzar en el ámbito de las operaciones de seguridad. Al completar la formación y obtener la certificación correspondiente, podrás optar a roles como:

- Security Operations Analyst (SOC Analyst)
- Especialista en respuesta ante incidentes
- Consultor de seguridad en entornos híbridos y multinube
- Especialista en Microsoft Sentinel y Microsoft Defender
- Administrador de operaciones de seguridad

Estos perfiles son cada vez más demandados en sectores estratégicos, empresas multinacionales y entornos donde la seguridad de la información es prioritaria.

Programa

1. **SC-200: Mitigación de amenazas mediante Microsoft Defender XDR**
    - Introducción a la protección contra amenazas de Microsoft Defender XDR
    - Mitigación de incidentes con Microsoft Defender
    - Corrección de incidentes con Microsoft Defender para Office 365
    - Administrar Microsoft Entra Identity Protection
    - Protección del entorno con Microsoft Defender for Identity
    - Protección de aplicaciones y servicios en la nube con Microsoft Defender for Cloud Apps
2. **SC-200: Mitigación de amenazas con Seguridad de Microsoft Copilot**
    - Introducción a la IA generativa
    - Descripción de Seguridad de Microsoft Copilot

- Descripción de las características principales de Seguridad de Microsoft Copilot
- Descripción de experiencias integradas de Seguridad de Microsoft Copilot
- Exploración de casos de uso de Seguridad de Microsoft Copilot

3. SC-200: Mitigación de amenazas con Microsoft Purview

- Respuesta a las alertas de prevención de pérdida de datos mediante Microsoft 365
- Administración del riesgo interno en Microsoft Purview
- Búsqueda e investigación con la auditoria de Microsoft Purview
- Investigación de amenazas con búsqueda de contenido en Microsoft Purview

4. SC-200: Mitigación de amenazas con Microsoft Defender for Endpoint

- Protección contra amenazas con Microsoft Defender para punto de conexión
- Implementación del entorno de Microsoft Defender para punto de conexión
- Implementación de mejoras de seguridad de Windows con Microsoft Defender para punto de conexión
- Realización de investigaciones de dispositivos en Microsoft Defender para punto de conexión
- Llevar a cabo investigaciones sobre evidencias y entidades con Microsoft Defender para punto de conexión
- Configuración y administración de la autorización con Microsoft Defender para punto de conexión
- Configuración de alertas y detecciones en Microsoft Defender para punto de conexión
- Uso de Administración de vulnerabilidades en Microsoft Defender para punto de conexión

5. SC-200: Mitigación de amenazas con Microsoft Defender for Cloud

- Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender para la nube
- Conexión de recursos de Azure a Microsoft Defender para la nube
- Conexión de recursos que no son de Azure a Microsoft Defender for Cloud
- Administración de la posición de seguridad en la nube
- Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender for Cloud
- Corrección de alertas de seguridad mediante Microsoft Defender for Cloud

LÁBERIT | CENTRO DE FORMACIÓN TIC.

Acreditado:

Microsoft Imagine Academy
Program Member

CertiProf® | Partner

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Networking Academy
CISCO

Linux Professional Institute

Microsoft
Technology Associate

Pearson VUE
Authorised
Test Centre

CERTIPORT
A PEARSON VUE BUSINESS
AUTHORIZED TESTING CENTER

Microsoft
Office Specialist
Authorized Testing Center

LABORA
Servei Valencià d'Ocupació i Formació

Avenida Cataluña, 11, bajo derecha. 46020 -Valencia
960 075 817 (Ext. 257) (Ext. 276) | formacion@laberit.com
formacion.laberit.com