TEMARIO DEL CURSO

# Microsoft Security Operations Analyst (SC-200)

**20 horas**

El curso Microsoft Security Operations Analyst (SC-200) está orientado a profesionales de seguridad que necesitan detectar, investigar y responder a amenazas en entornos locales y en la nube mediante las soluciones de seguridad de Microsoft.

### OBJETIVOS DEL CURSO

- Detectar, investigar y responder a amenazas de seguridad en entornos locales y en la nube.
- Administrar alertas e incidentes mediante Microsoft Defender XDR y Microsoft Sentinel.
- Configurar protecciones y detecciones en las soluciones de seguridad de Microsoft.
- Investigar identidades, dispositivos, aplicaciones y cargas de trabajo comprometidas.
- Realizar búsquedas proactivas de amenazas utilizando el Lenguaje de consulta Kusto (KQL).
- Automatizar la respuesta a incidentes mediante reglas y cuadernos de estrategias.
- Mejorar la postura de seguridad y reducir el riesgo organizativo mediante operaciones de seguridad continuas.

### A QUIÉN VA DIRIGIDO

- Analistas de operaciones de seguridad (SOC).
- Ingenieros y técnicos de seguridad.
- Administradores de sistemas y cloud con responsabilidades en seguridad.
- Profesionales de TI que participan en la detección, investigación y respuesta a incidentes.
- Candidatos que deseen prepararse para el examen de certificación SC-200.

### EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

## TEMARIO

MÓDULO 01.

## Mitigación de amenazas con Microsoft 365 Defender

- Analice datos sobre amenazas en distintos dominios y responda rápidamente mediante las capacidades de orquestación, automatización y correlación de incidentes de Microsoft Defender XDR. Conozca cómo las soluciones de seguridad de Microsoft protegen identidades, dispositivos, aplicaciones y datos. Se abordan las capacidades avanzadas de detección y corrección, incluida la protección de identidades con Microsoft Entra ID, la seguridad del correo electrónico y la protección de aplicaciones en la nube.
- Lecciones
- Introducción a Microsoft Defender XDR
- Administración y mitigación de incidentes en Microsoft 365 Defender
- Protección de identidades con Microsoft Entra ID Identity Protection
- Corrección de riesgos con Microsoft Defender para Office 365
- Protección del entorno con Microsoft Defender for Identity
- Protección de aplicaciones y servicios en la nube con Microsoft Defender for Cloud Apps
- Respuesta a alertas de DLP con Microsoft Purview
- Administración del riesgo interno en Microsoft 365
- Laboratorio: Mitigación de amenazas con Microsoft 365 Defender
- Después de completar este módulo, los alumnos podrán:
- Explicar la evolución del panorama de amenazas.
- Administrar y correlacionar incidentes en Microsoft Defender XDR.
- Realizar búsquedas avanzadas e investigaciones de alertas.
- Describir las capacidades de investigación y corrección de Identity Protection.
- Explicar el uso de Cloud Discovery para identificar aplicaciones en la organización.

MÓDULO 02.

## Mitigación de amenazas con Microsoft Defender para punto de conexión

- Implemente y administre Microsoft Defender for Endpoint para detectar, investigar y responder a amenazas avanzadas. Aprenda a incorporar dispositivos, configurar protecciones, realizar investigaciones forenses y automatizar respuestas. Se cubre la administración de vulnerabilidades, la interrupción automática de ataques y la gestión avanzada del entorno.
- Lecciones
- Introducción a Microsoft Defender para punto de conexión
- Implementación y configuración del entorno
- Configuración de protecciones y reglas de reducción de superficie de ataque (ASR)
- Investigación de dispositivos, evidencias y entidades
- Acciones de respuesta en dispositivos y sesiones en directo
- Automatización e investigación y respuesta automatizadas (AIR)
- Administración de vulnerabilidades en Microsoft Defender para punto de conexión
- Laboratorio: Implementación y mitigación de ataques con Microsoft Defender para punto de conexión
- Después de completar este módulo, los alumnos podrán:
- Configurar y administrar Microsoft Defender para punto de conexión.
- Investigar incidentes y realizar análisis forense de dispositivos.
- Configurar ASR y automatizaciones de respuesta.
- Administrar indicadores y vulnerabilidades de seguridad.

MÓDULO 03.

## Mitigación de amenazas con Microsoft Defender for Cloud

- Utilice Microsoft Defender for Cloud para proteger cargas de trabajo locales, en Azure y en entornos híbridos. Aprenda a administrar la posición de seguridad, detectar recursos no protegidos y responder a alertas de seguridad en cargas de trabajo cloud.
- Lecciones
- Introducción a Microsoft Defender for Cloud
- Protección de cargas de trabajo en la nube
- Conexión de recursos de Azure y no Azure
- Administración de la postura de seguridad en la nube
- Corrección y automatización de respuestas ante alertas
- Laboratorio: Mitigación de amenazas con Microsoft Defender for Cloud
- Después de completar este módulo, los alumnos podrán:
- Explicar las capacidades de protección de Microsoft Defender for Cloud.
- Configurar el aprovisionamiento automático.
- Identificar y corregir alertas de seguridad.

- Automatizar respuestas ante incidentes en la nube.

MÓDULO 04.

## Creación de consultas para Microsoft Sentinel mediante el Lenguaje de consulta Kusto (KQL)

- Aprenda a crear consultas KQL para detección, investigación, búsqueda de amenazas e informes en Microsoft Sentinel. Se cubren operadores, visualización de datos y uso de KQL en escenarios de seguridad reales.
- Lecciones
- Construcción de consultas KQL para Microsoft Sentinel
- Análisis de resultados y consultas multitabla
- Trabajo con datos estructurados y no estructurados
- Visualización y resumen de datos
- Laboratorio: Creación de consultas KQL para Microsoft Sentinel
- Después de completar este módulo, los alumnos podrán:
- Construir consultas KQL para escenarios de seguridad.
- Filtrar y analizar eventos de seguridad.

- Crear visualizaciones y funciones con KQL.

MÓDULO 05.

## Configuración del entorno de Microsoft Sentinel

- Configure correctamente un área de trabajo de Microsoft Sentinel para operaciones de seguridad a escala cloud. Aprenda la arquitectura, los roles, el almacenamiento de datos y el uso de inteligencia sobre amenazas.
- Lecciones
- Introducción a Microsoft Sentinel
- Creación y administración de áreas de trabajo
- Arquitectura, tablas y datos de Sentinel
- Uso de listas de reproducción e inteligencia sobre amenazas
- Laboratorio: Configuración del entorno de Microsoft Sentinel
- Después de completar este módulo, los alumnos podrán:
- Diseñar e implementar un área de trabajo de Microsoft Sentinel.
- Administrar roles y recursos.
- Gestionar listas de reproducción e indicadores de amenazas.

MÓDULO 06.

## Conexión de registros a Microsoft Sentinel

- Conecte orígenes de datos a Microsoft Sentinel mediante conectores nativos, Syslog, CEF, WEF y TAXII. Aprenda a planificar, optimizar y supervisar la ingesta de datos.
- Lecciones
- Conectores de datos de Microsoft Sentinel
- Conexión de Microsoft Defender y servicios de Azure
- Conexión de hosts Windows y Linux
- Ingesta de Syslog, CEF y eventos de Windows
- Inteligencia sobre amenazas y conectores TAXII
- Laboratorio: Conexión de registros a Microsoft Sentinel
- Después de completar este módulo, los alumnos podrán:
- Configurar conectores de datos correctamente.
- Diferenciar CEF, Syslog y otros métodos de ingesta.
- Supervisar y optimizar la recopilación de datos.

MÓDULO 07.

## Creación de detecciones y realización de investigaciones con Microsoft Sentinel

- Detecte amenazas mediante reglas de análisis, ASIM, análisis de comportamiento y automatización SOAR. Aprenda a investigar incidentes y responder mediante cuadernos de estrategias.
- Lecciones
- Detecciones y reglas de análisis en Microsoft Sentinel
- Automatización y cuadernos de estrategias
- Investigación y administración de incidentes
- Análisis de comportamiento de entidades
- Normalización de datos y ASIM
- Visualización y libros de Microsoft Sentinel
- Laboratorio: Detecciones e investigaciones con Microsoft Sentinel

- Después de completar este módulo, los alumnos podrán:
- Crear y administrar reglas de detección.
- Automatizar respuestas a incidentes.
- Investigar y resolver incidentes de seguridad.

MÓDULO 08.

## Búsqueda de amenazas en Microsoft Sentinel

- Identifique amenazas de forma proactiva mediante búsqueda avanzada, KQL, marcadores, streaming en vivo y cuadernos.
- Lecciones
- Conceptos de búsqueda de amenazas
- Búsqueda proactiva con Microsoft Sentinel
- Uso de trabajos de búsqueda y marcadores
- Búsqueda avanzada con cuadernos
- Laboratorio: Búsqueda de amenazas en Microsoft Sentinel
- Después de completar este módulo, los alumnos podrán:
- Definir hipótesis de búsqueda de amenazas.
- Realizar búsquedas avanzadas con KQL.
- Analizar amenazas a lo largo del tiempo.
- Crear y utilizar cuadernos para hunting