SC-200T00 Microsoft Security Operations Analyst

Detectar, investigar y responder a amenazas es uno de los pilares de la seguridad moderna. Este programa formativo te prepara para actuar con precisión y rapidez ante incidentes de seguridad utilizando herramientas de Microsoft.

La certificación **Microsoft Certified: Security Operations Analyst Associate** valida tu capacidad para proteger entornos híbridos mediante la integración de soluciones como **Microsoft Defender** y **Microsoft Sentinel**.

Objetivos Didácticos

- Configurar y usar Microsoft Sentinel para monitorizar y responder a incidentes.
- Implementar Microsoft Defender for Cloud, Endpoint, Identity y Office 365 en operaciones de seguridad.
- Aplicar técnicas de detección y análisis de amenazas con Kusto Query Language (KQL).
- Automatizar procesos de respuesta con playbooks e integraciones personalizadas.
- Prepararte para la certificación oficial Microsoft Certified: Security Operations Analyst Associate.

Audiencia

- Analistas SOC, técnicos en ciberseguridad y profesionales de IT encargados de operaciones de seguridad diarias.
- Empresas que buscan reforzar su equipo con perfiles especializados en detección y respuesta de amenazas.
- Profesionales que desean obtener una certificación reconocida internacionalmente y posicionarse en el ámbito de la ciberseguridad operacional.

Requisitos previos

- Conocimientos generales sobre conceptos de ciberseguridad, amenazas y protección de datos.
- Familiaridad con el entorno Microsoft 365, Azure y sus herramientas básicas.
- Deseable experiencia previa en análisis de seguridad o monitorización de eventos.

Modalidad

Aula virtual en directo.

Duración

4 días

Temario del curso

1. **Mitigación de amenazas mediante Microsoft Defender XDR**

    1.1. Introducción a la protección contra amenazas de Microsoft Defender XDR
    1.2. Mitigación de incidentes con Microsoft Defender
    1.3. Corrección de amenazas mediante Microsoft Defender
    1.4. Administrar Microsoft Entra Identity Protection
    1.5. Protección del entorno con Microsoft Defender for Identity
    1.6. Protección de aplicaciones y servicios en la nube con Microsoft Defender for Cloud Apps

2. **Mitigación de amenazas mediante Microsoft Security Copilot**

    2.1. Introducción a la inteligencia artificial y los agentes generativos
    2.2. Describir Microsoft Security Copilot
    2.3. Descripción de las características principales de Seguridad de Microsoft Copilot
    2.4. Descripción de las experiencias integradas de Microsoft Security Copilot
    2.5. Viva la experiencia de Security Copilot a través de simulaciones guiadas

3. **Mitigación de amenazas mediante Microsoft Purview**

    3.1. Investigar y responder a alertas de prevención de pérdida de datos de Microsoft Purview
    3.2. Investigación de alertas de riesgo interno y actividad relacionada
    3.3. Realizar investigaciones con Auditoría de Microsoft Purview
    3.4. Buscar contenido con eDiscovery de Microsoft Purview

4. **Mitigación de amenazas mediante Microsoft Defender para punto de conexión**

    4.1. Protección contra amenazas con Microsoft Defender para punto de conexión
    4.2. Implementación del entorno de Microsoft Defender para punto de conexión
    4.3. Implementación de mejoras de seguridad de Windows con Microsoft Defender para punto de conexión
    4.4. Realización de investigaciones de dispositivos en Microsoft Defender para punto de conexión
    4.5. Realizar acciones en un dispositivo con Microsoft Defender para punto de conexión
    4.6. Llevar a cabo investigaciones sobre evidencias y entidades con Microsoft Defender para punto de conexión
    4.7. Configuración y administración de la automatización con Microsoft Defender para punto de conexión
    4.8. Configuración de alertas y detecciones en Microsoft Defender para punto de conexiónv
    4.9. Uso de Administración de vulnerabilidades en Microsoft Defender para punto de conexión

5. **Mitigación de amenazas mediante Microsoft Defender for Cloud**

    5.1. Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender para la nube
    5.2. Conexión de recursos de Azure a Microsoft Defender para la nube
    5.3. Conexión de recursos que no son de Azure a Microsoft Defender for Cloud
    5.4. Administración de la posición de seguridad en la nube
    5.5. Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender for Cloud
    5.6. Corrección de alertas de seguridad mediante Microsoft Defender for Cloud

6. Creación de consultas para Microsoft Sentinel mediante el lenguaje de consulta Kusto (KQL)

6.1. Construcción de instrucciones KQL para Microsoft Sentinel
6.2. Uso de KQL para analizar los resultados de consultas
6.3. Uso de KQL para crear instrucciones de varias tablas
6.4. Trabajo con datos en Microsoft Sentinel mediante el lenguaje de consulta Kusto

7. Configuración del entorno de Microsoft Sentinel

7.1. Introducción a Microsoft Sentinel
7.2. Creación y administración de áreas de trabajo de Microsoft Sentinel
7.3. Registros de consulta en Microsoft Sentinel
7.4. Uso de listas de reproducción en Microsoft Sentinel
7.5. Uso de la inteligencia sobre amenazas en Microsoft Sentinel
7.6. Integración de Microsoft Defender XDR con Microsoft Sentinel

8. **Conexión de registros a Microsoft Sentinel**

8.1. Conexión de datos a Microsoft Sentinel mediante conectores de datos
8.2. Conexión de servicios Microsoft a Microsoft Sentinel
8.3. Conexión de Microsoft Defender XDR a Microsoft Sentinel
8.4. Conexión de hosts de Windows a Microsoft Sentinel
8.5. Conexión de registros de formato de eventos comunes a Microsoft Sentinel
8.6. Conexión de orígenes de datos Syslog a Microsoft Sentinel
8.7. Conexión de indicadores de amenazas a Microsoft Sentinel

9. Creación de detecciones y realización de investigaciones mediante Microsoft Sentinel

9.1. Detección de amenazas con análisis de Microsoft Sentinel
9.2. Automatización en Microsoft Sentinel
9.3. Respuesta a amenazas con cuadernos de estrategias de Microsoft Sentinel
9.4. Administración de incidentes de seguridad en Microsoft Sentinel
9.5. Identificación de amenazas con Análisis de comportamiento
9.6. Normalización de datos en Microsoft Sentinel
9.7. Consulta, visualización y supervisión de datos en Microsoft Sentinel
9.8. Administración de contenido en Microsoft Sentinel

10. Realizar la búsqueda de amenazas en Microsoft Sentinel

10.1. Explicación de los conceptos de búsqueda de amenazas en Microsoft Sentinel
10.2. Búsqueda de amenazas con Microsoft Sentinel
10.3. Uso de trabajos de búsqueda en Microsoft Sentinel
10.4. Búsqueda de amenazas con cuadernos en Microsoft Sentinel