The DevSecOps Company

Microsoft Partner

SC-5001
Configure SIEM security operations using Microsoft Sentinel

Información general.

Empiece a trabajar con las operaciones de seguridad de Microsoft Sentinel y configure el área de trabajo de Microsoft Sentinel, conecte los servicios de Microsoft y los eventos de seguridad de Windows a Microsoft Sentinel, configure reglas de análisis de Microsoft Sentinel y responda a las amenazas con respuestas automatizadas.

Duración.

1 Día.

Requisitos previos.

Antes de asistir a este curso, los estudiantes deben tener:

- Comprensión de los aspectos básicos de Microsoft Azure.
- Conocimientos básicos de Microsoft Sentinel.
- Experiencia con el uso del Lenguaje de consulta Kusto (KQL) en Microsoft Sentinel.

Examen.

Applied Skills Assessment.

Temario.

Módulo 1: Creación y administración de áreas de trabajo de Microsoft Sentinel.

Obtenga información sobre la arquitectura de las áreas de trabajo de Microsoft Sentinel para asegurarse de que configura el sistema para satisfacer los requisitos de las operaciones de seguridad de su organización.

- Planear y crear un área de trabajo de Microsoft Sentinel.
- Administración de áreas de trabajo en los inquilinos mediante Azure Lighthouse.
- Información sobre los permisos y roles de Microsoft Sentinel.
- Administrar la configuración de Microsoft Sentinel.
- Configuración de registros.

Módulo 2: Conexión de servicios Microsoft a Microsoft Sentinel.

Vea cómo conectar registros de servicios de Microsoft 365 y Azure a Microsoft Sentinel.

- Planeamiento para usar conectores de servicios de Microsoft.
- Conexión del conector de Microsoft Office 365.
- Conectar el conector de Microsoft Entra.
- Conectar el conector de protección de Microsoft Entra ID.
- Conexión del conector de actividad de Azure.

Módulo 3: Conexión de hosts de Windows a Microsoft Sentinel.

Uno de los registros más comunes que se recopilan son los eventos de seguridad de Windows. Vea cómo Microsoft Sentinel facilita esta tarea con el conector Eventos de seguridad.

- Planeamiento para usar el conector de eventos de seguridad de hosts Windows.
- Conexión mediante eventos de seguridad de Windows a través del conector de AMA.

- Conexión mediante eventos de seguridad a través del conector del agente antiguo.
- Recopilación de registros de eventos de Sysmon.

Módulo 4: Detección de amenazas con análisis de Microsoft Sentinel.

En este módulo, ha aprendido cómo Análisis de Microsoft Sentinel puede ayudar al equipo de operaciones de seguridad a identificar y detener los ciberataques.

- ¿Qué es Análisis de Microsoft Sentinel?
- Tipos de reglas de análisis.
- Creación de una regla de análisis a partir de plantillas.
- Creación de una regla de análisis a partir del asistente.
- Administración de reglas de análisis.

Ejercicio: Detección de amenazas con análisis de Microsoft Sentinel.

Módulo 5: Automatización en Microsoft Sentinel.

Al final de este módulo, podrá usar reglas de automatización en Microsoft Sentinel para automatizar la administración de incidentes.

- Descripción de las opciones de automatización.
- Creación de reglas de automatización.

Módulo 6: Configuración de operaciones de seguridad de SIEM mediante Microsoft Sentinel.

En este módulo, ha aprendido a configurar operaciones de seguridad de SIEM mediante Microsoft Sentinel.

Ejercicios:

- Configuración de operaciones SIEM con Microsoft Sentinel.
- Instalación de soluciones y conectores de datos del Centro de contenido de Microsoft Sentinel.
- Configuración de una regla de recopilación de datos para un conector de datos.
- Realizar un ataque simulado para validar las reglas analíticas y de automatización.