The DevSecOps Company

Microsoft Partner

SC-200T00
Microsoft Security Operations Analyst

Sobre este curso.

Aprenda a investigar y buscar amenazas, y a responder a ellas, mediante Microsoft Sentinel, Microsoft Defender for Cloud y Microsoft 365 Defender. 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.

Duración.

4 Días.

Perfil del público.

El rol Microsoft Security Operations Analyst 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 for Cloud, Microsoft 365 Defender 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.

Requisitos previos.

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

- Conocimientos básicos de Microsoft 365.
- Conocimientos básicos de los productos de identidad, cumplimiento normativo y seguridad de Microsoft.
- Conocimiento intermedio de Microsoft Windows.
- Conocimientos sobre los servicios de Azure, en particular Azure SQL Database y Azure Storage.
- Familiaridad con las máquinas virtuales de Azure y las redes virtuales.
- Conocimientos básicos de los conceptos de scripting.

Examen.

SC-200: Microsoft Security Operations Analyst.

Temario.

Módulo 1: Introducción a la protección contra amenazas de Microsoft 365.

En este módulo, aprenderá a usar el conjunto de protección contra amenazas integrado de Microsoft 365 Defender.

- Exploración de casos de uso de respuesta de Detección y respuesta extendidas (XDR).
- Descripción de Microsoft 365 Defender en un centro de operaciones de seguridad (SOC).
- Exploración de Microsoft Security Graph.
- Investigación de incidentes en Microsoft 365 Defender.

Ahora debería poder hacer lo siguiente:

- Descripción de la solución de Microsoft 365 Defender por dominio.
- Descripción del rol de Microsoft 365 Defender en un SOC moderno.

Módulo 2: Mitigación de incidentes con Microsoft 365 Defender.

Obtenga información sobre cómo el portal de Microsoft 365 Defender proporciona una vista unificada de los incidentes de la familia de productos de Microsoft 365 Defender.

- Uso del portal de Microsoft 365 Defender.
- Administración de incidentes.
- Investigación de incidentes.
- Administración e investigación de alertas.
- Administración de investigaciones automatizadas.
- Utilice el centro de actividades.
- Exploración de la búsqueda avanzada.
- Investigación de los registros de inicio de sesión de Azure AD.
- Información sobre la puntuación segura de Microsoft.
- Análisis de amenazas.
- Análisis de los informes.
- Configuración del portal de Microsoft 365 Defender.

Al final de este módulo, podrá hacer lo siguiente:

- Administrar incidentes en Microsoft 365 Defender
- Investigar incidentes en Microsoft 365 Defender
- Realice una búsqueda avanzada en Microsoft 365 Defender

Módulo 3: Protección de las identidades con Azure AD Identity Protection.

Use las características avanzadas de detección y corrección de amenazas basadas en identidades para proteger las aplicaciones y las identidades de Azure Active Directory de posibles riesgos.

- Información general sobre Azure AD Identity Protection.
- Detección de riesgos con directivas de Azure AD Identity Protection.
- Investigación y corrección de riesgos que Azure AD Identity Protection detecte.

Objetivos de este módulo:

- Describir las características de Azure Active Directory Identity Protection.
- Describir las características de investigación y corrección de Azure Active Directory Identity Protection.

Módulo 4: Remedia los riesgos con Microsoft Defender para Office 365.

Obtenga información sobre el componente Microsoft Defender para Office 365 de Microsoft 365 Defender.

- Automatizar, investigar y remediar.
- Configurar, proteger y detectar.
- Simular ataques.

En este módulo, aprenderás a:

- Defina las capacidades de Microsoft Defender para Office 365.
- Comprende cómo simular ataques dentro de tu red.
- Explique cómo Microsoft Defender para Office 365 puede remediar los riesgos en su entorno.

Módulo 5: Protege tu entorno con Microsoft Defender for Identity.

Conoce el componente Microsoft Defender for Identity de Microsoft 365 Defender.

- Introducción a Microsoft Defender for Identity.
- Configurar sensores de Microsoft Defender for Identity.
- Revisar las cuentas o datos comprometidos.
- Integrar con otras herramientas de Microsoft.

Una vez completado este módulo, deberías poder:

- Definir las capacidades de Microsoft Defender for Identity.
- Comprender cómo configurar los sensores de Microsoft Defender for Identity.
- Explicar cómo Microsoft Defender for Identity puede solucionar los riesgos de tu entorno.

Módulo 6: Proteger las aplicaciones y servicios en la nube con Microsoft Defender for Cloud Apps.

Microsoft Defender for Cloud Apps es un agente de seguridad de acceso a la nube (CASB) que funciona en varias nubes. Ofrece una visibilidad completa, control sobre los datos que se transmiten y análisis sofisticados para identificar y combatir las ciberamenazas en todos los servicios en la nube. Obtenga información sobre cómo usar Defender for Cloud Apps en su organización.

- Definir el marco de Defender for Cloud Apps.
- Explorar sus aplicaciones en la nube con Cloud Discovery.
- Proteger los datos y aplicaciones con el control de aplicaciones de acceso condicional.
- Recorrido por la detección y el control de acceso con Microsoft Defender for Cloud Apps.
- Clasificar y proteger información confidencial.
- Detectar amenazas.

Al final de este módulo, podrás hacer lo siguiente:

- Definir el marco de Defender for Cloud Apps.
- Explicar cómo le ayuda Cloud Discovery a ver lo que pasa en su organización.
- Usar las directivas de control de aplicación de acceso condicional para controlar el acceso a las aplicaciones de su organización.

Módulo 7: Respuesta a las alertas de prevención de pérdida de datos mediante Microsoft 365.

Descubra cómo las alertas de prevención contra la pérdida de datos le ayudarán en su investigación a encontrar el ámbito completo del incidente.

- Describir las alertas de prevención de pérdida de datos.
- Investigación de las alertas de prevención de pérdida de datos en Microsoft Purview.
- Investigación de alertas de prevención de pérdida de datos en Microsoft Defender for Cloud Apps.

Al final de este módulo, podrá hacer lo siguiente:

- Describir los componentes de prevención de pérdida de datos (DLP) en Microsoft 365
- Investigación de las alertas de DLP en el portal de cumplimiento Microsoft Purview
- Investigación de alertas DLP en Microsoft Defender for Cloud Apps

Módulo 8: Gestionar el riesgo interno en Microsoft Purview.

Microsoft Purview Insider Risk Management ayuda a las organizaciones a abordar los riesgos internos, como el robo de propiedad intelectual, el fraude y el sabotaje. Aprenda sobre la gestión de riesgos internos y cómo las tecnologías de Microsoft pueden ayudarle a detectar, investigar y tomar medidas sobre actividades de riesgo en su organización.

- Visión general de la gestión de riesgos de información privilegiada.
- Introducción a la gestión de políticas de riesgo interno.
- Crear y gestionar políticas de riesgo interno.
- Verificación de conocimientos.
- Investigar alertas de riesgo de información privilegiada.
- Tomar medidas sobre las alertas de riesgo de información privilegiada a través de los casos.
- Gestionar la evidencia forense de gestión de riesgos internos.
- Crear plantillas de avisos de gestión de riesgos internos.

Al finalizar este módulo, deberías poder:

- Explique cómo Microsoft Purview Insider Risk Management puede ayudar a prevenir, detectar y contener los riesgos internos de una organización.
- Describa los tipos de plantillas de políticas integradas y predefinidas.
- Enumere los requisitos previos que deben cumplirse antes de crear políticas de riesgo interno.
- Explique los tipos de acciones que puede tomar en un caso de gestión de riesgos internos.

Módulo 9: Investigación de amenazas mediante características de auditoría en Microsoft 365 Defender y Microsoft Purview Estándar.

En este módulo se examina cómo buscar actividades auditadas mediante la solución Auditoría de Microsoft Purview (UAL), incluido cómo exportar, configurar y ver los registros del registro de auditoría recuperados de una búsqueda de registros de auditoría.

- Introducción a la investigación de amenazas con el registro de auditoría unificado (UAL).
- Exploración de soluciones Auditoría de Microsoft Purview.
- Implementación de Auditoría (Estándar) de Microsoft Purview.

- Inicio de la actividad de grabación en el registro de auditoría unificado.
- Buscar en el registro de auditoría unificado (UAL).
- Exportación, configuración y visualización de registros de auditoría.
- Uso de la búsqueda de registros de auditoría para investigar problemas comunes de soporte técnico.

Al término de este módulo, sabrá hacer lo siguiente:

- Describa las diferencias entre Auditoría (Estándar) y Auditoría (Premium).
- Inicie la grabación de la actividad de usuario y administrador en el registro de auditoría unificado (UAL).
- Identifique las características principales de la solución Auditoría (Estándar).
- Configure e implemente la búsqueda de registros de auditoría mediante la solución Auditoría (Estándar).
- Exporte, configure y vea los registros de auditoría.
- Use la búsqueda de registros de auditoría para solucionar problemas comunes de soporte técnico.

Módulo 10: Investigación de amenazas mediante auditoría en Microsoft 365 Defender y Microsoft Purview (Premium).

En este módulo se exploran las diferencias entre Auditoría de Microsoft Purview (Estándar) y Auditoría (Premium), además de la funcionalidad clave de Auditoría (Premium), incluidos los requisitos de configuración, la habilitación del registro de auditoría, la creación de directivas de retención de registros de auditoría y la realización de investigaciones forenses.

- Introducción a la investigación de amenazas con Auditoría (Premium) en Microsoft Purview.
- Exploración de Auditoría (Premium) en Microsoft Purview.
- Implementación de Auditoría (Premium) de Microsoft Purview.
- Administración de directivas de retención de registros de auditoría.
- Investigación de cuentas de correo electrónico en peligro mediante Auditoría (Premium) en Purview.

Al término de este módulo, sabrá hacer lo siguiente:

- Describa las diferencias entre Auditoría (Estándar) y Auditoría (Premium).
- Configurar e implementar Auditoría (Premium) en Microsoft Purview.
- Crear directivas de retención de registros de auditoría.
- Realizar investigaciones forenses de cuentas de usuario en peligro.

Módulo 11: Investigación de amenazas con búsqueda de contenido en Microsoft Purview.

En este módulo se examina cómo buscar contenido en el portal de cumplimiento de Microsoft Purview mediante la funcionalidad de búsqueda de contenido, incluido cómo ver y exportar los resultados de la búsqueda y configurar el filtrado de permisos de búsqueda.

- Soluciones de eDiscovery en Microsoft Purview.
- Creación de una búsqueda de contenido.
- Visualización de los resultados y estadísticas de la búsqueda.
- Exportar los resultados y el informe de búsqueda.
- Configurar el filtrado de permisos de búsqueda.
- Búsqueda y eliminación de mensajes de correo electrónico.

Al término de este módulo, sabrá hacer lo siguiente:

- Describir cómo usar la búsqueda de contenido en el portal de cumplimiento Microsoft Purview.
- Diseñar y crear una búsqueda de contenido.
- Vista previa de los resultados de la búsqueda.
- Visualización de las estadísticas de búsqueda.
- Exportar los resultados y el informe de búsqueda.
- Configurar el filtrado de permisos de búsqueda.

Módulo 12: Protéjase contra las amenazas con Microsoft Defender para Endpoint.

Descubra cómo Microsoft Defender para Endpoint puede ayudar a su organización a mantenerse segura.

- Introducción a Microsoft Defender para Endpoint.
- Practicar la administración de seguridad.
- Caza amenazas dentro de tu red.

En este módulo, aprenderás a:

- Defina las capacidades de Microsoft Defender para Endpoint.
- Comprende cómo cazar amenazas dentro de tu red.
- Explique cómo Microsoft Defender para Endpoint puede remediar los riesgos en su entorno.

Módulo 13: Implementación del entorno de Microsoft Defender para punto de conexión.

Aprenda a implementar el entorno de Microsoft Defender para punto de conexión, incluidas la incorporación de dispositivos y la configuración de seguridad.

- Creación del entorno.
- Descripción de la compatibilidad y las características de los sistemas operativos.
- Incorporación de dispositivos.
- Administración del acceso.
- Creación y administración de roles para el control de acceso basado en roles.
- Configuración de los grupos de dispositivos.
- Configuración de las características avanzadas del entorno.

Al final de este módulo, podrá hacer lo siguiente:

- Creación de un entorno de Microsoft Defender para punto de conexión.
- Incorporación de dispositivos que Microsoft Defender para punto de conexión debe supervisar.
- Configuración de Microsoft Defender para punto de conexión.

Módulo 14: Implementación de mejoras de seguridad de Windows con Microsoft Defender para punto de conexión.

Microsoft Defender para punto de conexión ofrece varias herramientas para eliminar riesgos al reducir el área expuesta a ataques sin bloquear la productividad de los usuarios. Obtenga información sobre la reducción de la superficie expuesta a ataques (ASR) con Microsoft Defender para punto de conexión.

- Descripción de la reducción de la superficie expuesta a ataques.
- Habilitar reglas de reducción de la superficie expuesta a ataques.

Al final de este módulo, podrá hacer lo siguiente:

- Explicar la reducción de la superficie expuesta a ataques en Windows
- Habilitar reglas de reducción de la superficie expuesta a ataques en dispositivos Windows 10
- Configurar reglas de reducción de la superficie expuesta a ataques en dispositivos con Windows 10

Módulo 15: Realización de investigaciones de dispositivos en Microsoft Defender para punto de conexión.

Microsoft Defender para punto de conexión proporciona información detallada del dispositivo, incluida información de análisis forenses. Obtenga información sobre los detalles disponibles a través de Microsoft Defender para punto de conexión que le ayudarán en sus investigaciones.

- Uso de la lista de inventario de dispositivos.
- Investigación del dispositivo.
- Uso del bloqueo de comportamiento.
- Detección de dispositivos con detección de dispositivos.

Al final de este módulo, podrá hacer lo siguiente:

- Usar la página del dispositivo de Microsoft Defender para punto de conexión.
- Describir la información de análisis forenses del dispositivo recopilada por Microsoft Defender para punto de conexión.
- Describir el bloqueo del comportamiento de Microsoft Defender para punto de conexión.

Módulo 16: Realizar acciones en un dispositivo con Microsoft Defender para punto de conexión.

Obtenga información sobre cómo Microsoft Defender para punto de conexión proporciona la capacidad remota para contener dispositivos y recopilar datos de análisis forenses.

- Explicación de las acciones del dispositivo.
- Ejecución del examen de Antivirus de Microsoft Defender en los dispositivos.
- Recopilación del paquete de investigación desde los dispositivos.
- Inicio de una sesión de respuesta dinámica.

Al final de este módulo, podrá hacer lo siguiente:

- Realizar acciones en un dispositivo con Microsoft Defender para punto de conexión
- Realizar la recopilación de datos forenses con Microsoft Defender para punto de conexión
- Acceder a dispositivos de forma remota con Microsoft Defender para punto de conexión

Módulo 17: Llevar a cabo investigaciones sobre evidencias y entidades con Microsoft Defender para punto de conexión.

Obtenga información sobre los artefactos de su entorno y qué relación tienen con otros artefactos y alertas que le proporcionarán conclusiones y le ayudarán a comprender el impacto general sobre su entorno.

- Investigar un archivo.
- Investigación de una cuenta de usuario.
- Investigar una dirección IP.
- Investigar un dominio.

Al final de este módulo, podrá hacer lo siguiente:

- Investigar archivos, dominios y direcciones IP y cuentas de usuario en Microsoft Defender para punto de conexión.

Módulo 18: Configuración y administración de la automatización con Microsoft Defender para punto de conexión.

Obtenga información sobre cómo configurar la automatización en Microsoft Defender para punto de conexión mediante la administración de la configuración del entorno.

- Configurar características avanzadas.
- Administración de la configuración de carga y carpeta de automatización.
- Configuración de las capacidades de investigación y corrección automatizadas.
- Bloqueo de dispositivos en riesgo.

Al final de este módulo, podrá hacer lo siguiente:

- Configurar características avanzadas de Microsoft Defender para punto de conexión
- Administrar la configuración de automatización en Microsoft Defender para punto de conexión

Módulo 19: Configuración de alertas y detecciones en Microsoft Defender para punto de conexión.

Obtenga información sobre cómo configurar las opciones para administrar las alertas y las notificaciones. También obtendrá información sobre cómo habilitar indicadores como parte del proceso de detección.

- Configurar características avanzadas.
- Configurar notificaciones de alerta.
- Administración de la eliminación de alertas.
- Administración de los indicadores.

Después de completar este módulo, podrá hacer lo siguiente:

- Configurar las opciones de alerta en Microsoft Defender para punto de conexión
- Administrar los indicadores en Microsoft Defender para punto de conexión

Módulo 20: Uso de Administración de vulnerabilidades en Microsoft Defender para punto de conexión.

Obtenga información sobre los puntos débiles de su entorno mediante el uso de Administración de amenazas y vulnerabilidades de Microsoft Defender para punto de conexión.

- Descripción de Administración de amenazas y vulnerabilidades.
- Exploración de las vulnerabilidades de sus dispositivos.
- Administración de la corrección.

Al final de este módulo, podrá hacer lo siguiente:

- Descripción de Administración de vulnerabilidades en Microsoft Defender para punto de conexión.
- Identificar las vulnerabilidades de sus dispositivos con Microsoft Defender para punto de conexión.
- Realizar un seguimiento de las amenazas emergentes en Microsoft Defender para punto de conexión.

Módulo 21: Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender para la nube.

Obtenga información sobre el propósito de Microsoft Defender para la nube y cómo habilitar el sistema.

- Explicación de Microsoft Defender para la nube.
- Descripción de la protección de cargas de trabajo de Microsoft Defender para la nube.
- Habilitar Microsoft Defender for Cloud.

Ejercicio: Guía interactiva de Microsoft Defender para la nube.

Al final de este módulo, podrá hacer lo siguiente:

- Descripción de Microsoft Defender para características en la nube.
- Protección de cargas de trabajo de Microsoft Defender para la nube.
- Habilitar Microsoft Defender for Cloud.

Módulo 22: Conexión de recursos de Azure a Microsoft Defender para la nube.

Aprenda a conectar los distintos recursos de Azure a Microsoft Defender para la nube a fin de detectar amenazas.

- Exploración y administración de los recursos con Asset Inventory.
- Configuración del aprovisionamiento automático.
- Aprovisionamiento manual del agente de log Analytics.

Al final de este módulo, podrá hacer lo siguiente:

- Explorar los recursos de Azure.
- Configurar el aprovisionamiento automático en Microsoft Defender para la nube.
- Describir el aprovisionamiento manual en Microsoft Defender para la nube.

Módulo 23: Conexión de recursos que no son de Azure a Microsoft Defender for Cloud.

Obtenga información sobre cómo agregar funcionalidades de Microsoft Defender for Cloud a su entorno híbrido.

- Protección de recursos que no son de Azure.
- Conexión de máquinas que no son de Azure.
- Conexión de cuentas de AWS.
- Conexión de cuentas de GCP.

Al final de este módulo, podrá hacer lo siguiente:

- Conexión de máquinas que no son de Azure a Microsoft Defender para la nube.
- Conexión de cuentas de AWS a Microsoft Defender para la nube.
- Conexión de cuentas de GCP a Microsoft Defender para la nube.

Módulo 24: Administración de la posición de seguridad en la nube.

En Microsoft Defender for Cloud, la administración de la posición de seguridad en la nube (CSPM) proporciona visibilidad sobre los recursos vulnerables y proporciona instrucciones de protección.

- Exploración de la puntuación de seguridad.
- Explorar recomendaciones.
- Medición y aplicación del cumplimiento normativo.
- Descripción de Workbooks.

Cuando haya terminado, podrá hacer lo siguiente:

- Describir las características de Microsoft Defender for Cloud.
- Explicar las protecciones de administración de la posición de seguridad de Microsoft Defender for Cloud para los recursos.

Módulo 25: Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender for Cloud.

Obtenga información sobre las protecciones y detecciones que proporciona Microsoft Defender for Cloud con cada carga de trabajo en la nube.

- Información sobre Microsoft Defender para servidores.
- Información sobre Microsoft Defender para App Service.
- Información sobre Microsoft Defender para Storage.
- Información sobre Microsoft Defender para SQL.
- Información sobre Microsoft Defender para bases de datos de código abierto.
- Información sobre Microsoft Defender para Key Vault.
- Información sobre Microsoft Defender para Resource Manager.
- Información sobre Microsoft Defender para DNS.
- Descripción de Microsoft Defender para contenedores.
- Información sobre las protecciones adicionales de Microsoft Defender.

Al final de este módulo, podrá hacer lo siguiente:

- Explicación de qué cargas de trabajo están protegidas por Microsoft Defender for Cloud.
- Descripción de las ventajas de las protecciones que ofrece Microsoft Defender for Cloud.
- Explicación del funcionamiento de las protecciones de Microsoft Defender for Cloud.

Módulo 26: Corrección de alertas de seguridad mediante Microsoft Defender for Cloud.

Descubra cómo corregir las alertas de seguridad de Microsoft Defender for Cloud.

- Descripción de las alertas de seguridad.
- Corrección de alertas y automatización de respuestas.
- Supresión de alertas de Defender for Cloud.
- Generación de informes de inteligencia sobre amenazas.
- Respuesta a alertas desde recursos de Azure.

Al final de este módulo, podrá hacer lo siguiente:

- Descripción de alertas en Microsoft Defender for Cloud.
- Corrección de alertas en Microsoft Defender for Cloud.
- Automatización de respuestas en Microsoft Defender for Cloud.

Módulo 27: Construcción de instrucciones KQL para Microsoft Sentinel.

KQL es el lenguaje de consulta que se usa para analizar datos con el fin de crear análisis, libros y realizar búsquedas en Microsoft Sentinel. Obtenga información sobre cómo la estructura de instrucciones KQL básica proporciona la base para crear instrucciones más complejas.

- Descripción de la estructura de instrucciones del lenguaje de consulta Kusto.
- Uso del operador de búsqueda.
- Uso del operador where.
- Uso de la instrucción Let.
- Uso del operador extend y order by.
- Uso de los operadores project.

Al final de este módulo, podrá hacer lo siguiente:

- Construir instrucciones KQL
- Buscar eventos de seguridad en archivos de registro con KQL
- Filtrar búsquedas en función de la hora del evento, la gravedad, el dominio y otros datos relevantes mediante KQL

Módulo 28: Uso de KQL para analizar los resultados de consultas.

Aprender a resumir y visualizar datos con una instrucción KQL proporciona la base para crear detecciones en Microsoft Sentinel.

- Uso del operador summarize.
- Uso del operador summarize para filtrar resultados.
- Uso del operador summarize para preparar los datos.
- Uso del operador render para crear visualizaciones.

Al final de este módulo, podrá hacer lo siguiente:

- Resumir datos usando instrucciones KQL.
- Representar visualizaciones con instrucciones KQL.

Módulo 29: Uso de KQL para crear instrucciones de varias tablas.

Vea cómo se trabaja con varias tablas usando KQL.

- Uso del operador union.
- Uso del operador join.

Al final de este módulo, podrá hacer lo siguiente:

- Usar KQL para crear consultas mediante uniones para ver los resultados de varias tablas.
- Usar KQL para combinar dos tablas con el operador join.

Módulo 30: Trabajo con datos en Microsoft Sentinel mediante el lenguaje de consulta Kusto.

Aprenda a usar el lenguaje de consulta Kusto (KQL) para manipular los datos de cadena ingeridos de los orígenes de registros.

- Extracción de datos de campos de cadena no estructurados.
- Extracción de datos de datos de cadena estructurados.
- Integración de datos externos.
- Creación de analizadores con funciones.

Al final de este módulo, podrá hacer lo siguiente:

- Extraer datos de campos de cadena no estructurados usando KQL.
- Extraer datos de datos de cadena estructurados usando KQL.
- Crear funciones con KQL.

Módulo 31: Introducción a Microsoft Sentinel.

Los sistemas tradicionales de administración de eventos e información de seguridad (SIEM) suelen tardar mucho tiempo en instalarse y configurarse. Tampoco están diseñados de forma específica para cargas de trabajo en la nube. Microsoft Sentinel

permite empezar a obtener conclusiones valiosas sobre la seguridad de los datos en la nube y locales en muy poco tiempo. Este módulo lo ayuda a empezar.

- ¿Qué es Microsoft Sentinel?
- Funcionamiento de Microsoft Sentinel.
- Cuándo usar Microsoft Sentinel.

Al término de este módulo, sabrá hacer lo siguiente:

- Identificar los distintos componentes y la funcionalidad de Microsoft Sentinel.
- Identificar los casos de uso en los que Microsoft Sentinel sería una buena solución.

Módulo 32: 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.

- Plan para el área de trabajo de Microsoft Sentinel.
- Creación de 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.
- Administración de la configuración de Microsoft Sentinel.
- Configuración de registros.

Al final de este módulo, podrá hacer lo siguiente:

- Describir la arquitectura de un área de trabajo de Sentinel
- Instalar un área de trabajo de Microsoft Sentinel
- Administrar un área de trabajo de Microsoft Sentinel

Módulo 33: Registros de consulta en Microsoft Sentinel.

Como analista de operaciones de seguridad, debe comprender las tablas, los campos y los datos ingeridos en el área de trabajo. Descubra cómo consultar las tablas de datos más utilizadas en Microsoft Sentinel.

- Consulta de registros en la página de registros.
- Información sobre las tablas de Microsoft Sentinel.
- Descripción de las tablas comunes.
- Descripción de las tablas de Microsoft 365 Defender.

Al final de este módulo, podrá hacer lo siguiente:

- Usar la página de registros para ver tablas de datos en Microsoft Sentinel.
- Consultar las tablas más utilizadas con Microsoft Sentinel.

Módulo 34: Uso de listas de reproducción en Microsoft Sentinel.

Aprenda a crear listas de reproducción de Microsoft Sentinel que son una lista con nombre de datos importados. Una vez creadas, puede usar fácilmente la lista reproducción con nombre en las consultas de KQL.

- Planear listas de reproducción.
- Creación y Administración de listas de reproducción.

Al final de este módulo, podrá hacer lo siguiente:

- Creación de una lista de reproducción en Microsoft Sentinel.
- Uso de KQL para acceder a la lista de reproducción en Microsoft Sentinel.

Módulo 35: Uso de la inteligencia sobre amenazas en Microsoft Sentinel.

Aprenda cómo la página de inteligencia sobre amenazas de Microsoft Sentinel le permite administrar los indicadores de amenazas.

- Definición de Inteligencia sobre amenazas.
- Administrar los indicadores de amenazas.
- Visualización de los indicadores de amenazas con KQL.

Al final de este módulo, podrá hacer lo siguiente:

- Administrar indicadores de amenazas en Microsoft Sentinel
- Usar KQL para acceder a los indicadores de amenazas en Microsoft Sentinel

Módulo 36: Conexión de datos a Microsoft Sentinel mediante conectores de datos.

El enfoque principal para conectar datos de registro es usar los conectores de datos proporcionados de Microsoft Sentinel.

En este módulo, se proporciona información general sobre los conectores de datos disponibles.

- Ingesta de datos de registro con conectores de datos.
- Descripción de los proveedores de conectores de datos.
- Visualización de hosts conectados.
-
- Al final de este módulo, podrá hacer lo siguiente:
- Describir cómo instalar soluciones de Centro de contenido para aprovisionar conectores de datos de Microsoft Sentinel.
- Explicar el uso de los conectores de datos en Microsoft Sentinel.
- Describir a los proveedores de conectores de datos de Microsoft Sentinel.
- Explicar las diferencias entre el formato de evento común y el conector Syslog en Microsoft Sentinel.

Módulo 37: Conexión de servicios Microsoft a Microsoft Sentinel.

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

- Conectar conectores de servicios de Microsoft.
- Explicar el modo en el que los conectores crean incidentes automáticamente en Microsoft Sentinel.

Al final de este módulo, podrá hacer lo siguiente:

- Conectar conectores de servicios de Microsoft.
- Explicar el modo en el que los conectores crean incidentes automáticamente en Microsoft Sentinel.

Módulo 38: Conexión de Microsoft 365 Defender a Microsoft Sentinel.

Conozca las opciones de configuración y los datos que proporcionan los conectores de Microsoft Sentinel para Microsoft 365 Defender.

- Planeamiento para usar los conectores de Microsoft 365 Defender.
- Conexión del conector de Microsoft 365 Defender.
- Conexión del conector de Microsoft Defender for Cloud.
- Conexión de Microsoft Defender para IoT.
- Conexión de los conectores heredados de Microsoft Defender.

Al final de este módulo, podrá hacer lo siguiente:

- Activación del conector de Microsoft 365 Defender en Microsoft Sentinel.
- Activación del conector de Microsoft Defender for Cloud y Microsoft Defender para IoT en Microsoft Sentinel.

Módulo 39: 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 AMA.
- Conexión mediante eventos de seguridad a través del conector del agente antiguo.
- Recopilación de registros de eventos de Sysmon.

Al final de este módulo, podrá hacer lo siguiente:

- Conectar Azure Windows Virtual Machines a Microsoft Sentinel.
- Conectar hosts Windows que no son de Azure a Microsoft Sentinel.
- Configurar el agente de Log Analytics para recopilar eventos de Sysmon.

Módulo 40: Conexión de registros de formato de evento común a Microsoft Sentinel.

La mayoría de los conectores proporcionados por los proveedores utilizan el conector CEF. Conozca las opciones de configuración del conector CEF (formato de evento común).

- Planeamiento para usar el conector de formato de evento común.
- Conexión de una solución externa mediante el conector de formato de evento común.

Al final de este módulo, podrá hacer lo siguiente:

- Explicar las opciones de implementación del conector de formato de evento común en Microsoft Sentinel.
- Ejecutar el script de implementación para el conector de formato de evento común.

Módulo 41: Conexión de orígenes de datos Syslog a Microsoft Sentinel.

Obtenga información sobre las opciones de configuración de la regla de recopilación de datos de Syslog del agente de Azure Monitor en Linux, que le permiten analizar los datos de Syslog.

- Planeamiento de la recopilación de datos de Syslog.
- Recopilación de datos de orígenes basados en Linux mediante Syslog.
- Configuración de la regla de recopilación de datos para orígenes de datos de Syslog.
- Análisis de los datos de syslog con KQL.

Al final de este módulo, el alumno podrá hacer lo siguiente:

- Describir la regla de recopilación de datos del agente de Azure Monitor para Syslog.
- Instalar y configurar la extensión del agente Linux de Azure Monitor con la regla de recopilación de datos de Syslog.
- Ejecutar los scripts de conexión e implementación de Linux de Azure Arc.
- Comprobar que los datos de registro de Syslog están disponibles en Microsoft Sentinel.
- Crear un analizador mediante KQL en Microsoft Sentinel.

Módulo 42: Conexión de indicadores de amenazas a Microsoft Sentinel.

Vea cómo conectar indicadores de inteligencia sobre amenazas al área de trabajo de Microsoft Sentinel mediante los conectores de datos proporcionados.

- Planeamiento para usar conectores de inteligencia sobre amenazas.
- Conexión del conector TAXII de inteligencia sobre amenazas.
- Conexión del conector de plataformas de inteligencia sobre amenazas.
- Visualización de los indicadores de amenazas con KQL.

Al final de este módulo, podrá hacer lo siguiente:

- Configuración del conector TAXII en Microsoft Sentinel
- Configurar el conector de plataformas de inteligencia sobre amenazas en Microsoft Sentinel.
- Visualización de indicadores de amenazas en Microsoft Sentinel

Módulo 43: 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.

Objetivos de este módulo:

- Explicar la importancia de Análisis de Microsoft Sentinel.
- Explicar los distintos tipos de reglas de análisis.
- Crear reglas a partir de plantillas.
- Crear reglas y consultas de análisis mediante el Asistente para reglas de análisis.
- Administrar reglas con modificaciones.

Módulo 44: 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.

Después de completar este módulo, podrá:

- Explicación de las opciones de automatización en Microsoft Sentinel
- Creación de reglas de automatización en Microsoft Sentinel

Módulo 45: Administración de incidentes de seguridad en Microsoft Sentinel.

Obtenga información sobre los incidentes de seguridad, la evidencia y las entidades de un incidente, la administración de incidentes y cómo usar Microsoft Sentinel para tratar incidentes.

- Descripción de incidentes.
- Evidencia y entidades de un incidente.
- Administración de incidentes.

Ejercicios:

- Configuración del entorno de Azure.
- Investigación de un incidente.

Al final de este módulo, podrá hacer lo siguiente:

- Obtenga información sobre los incidentes de seguridad y la administración de incidentes de Microsoft Sentinel.
- Explore la evidencia y las entidades de un incidente de Microsoft Sentinel.
- Use Microsoft Sentinel para investigar incidentes de seguridad y administrar la resolución de incidentes.

Módulo 46: Identificación de amenazas con Análisis de comportamiento.

Aprenda a usar el análisis de comportamiento de entidades en Microsoft Sentinel para identificar amenazas dentro de su organización.

- Descripción del análisis de comportamiento.
- Exploración de entidades.
- Visualización de información de comportamiento de entidades.
- Uso de plantillas de reglas analíticas de detección de anomalías.

Al final de este módulo, podrá hacer lo siguiente:

- Explicar el análisis de comportamiento de entidades y usuarios en Azure Sentinel.
- Explorar entidades en Microsoft Sentinel.

Módulo 47: Normalización de datos en Microsoft Sentinel.

Al final de este módulo, podrá usar analizadores ASIM para identificar las amenazas dentro de la organización.

- Descripción de la normalización de datos.
- Uso de analizadores de ASIM.
- Descripción de las funciones KQL parametrizadas.
- Creación de un analizador de ASIM.
- Configuración de reglas de recopilación de datos de Azure Monitor.

Tras finalizar este módulo, usted será capaz de:

- Usar analizadores de ASIM.
- Crear un analizador de ASIM.
- Crear funciones KQL parametrizadas.

Módulo 48: Consulta, visualización y supervisión de datos en Microsoft Sentinel.

En este módulo se describe cómo consultar, visualizar y supervisar datos en Microsoft Sentinel.

- Supervisión y visualización de datos.
- Consulta de datos mediante el lenguaje de consulta Kusto.
- Uso de libros predeterminados de Microsoft Sentinel.
- Creación de un libro de Microsoft Sentinel.

Ejercicios:

- Consulta y visualización de datos con libros de Microsoft Sentinel.
- Visualización de datos mediante libros de Microsoft Sentinel.

Objetivos de este módulo:

- Visualizar datos de seguridad con libros de Microsoft Sentinel.
- Comprender cómo funcionan las consultas.
- Explorar las funciones de los libros.
- Crear un libro de Microsoft Sentinel.

Módulo 49: Administración de contenido en Microsoft Sentinel.

Al final de este módulo, podrá administrar el contenido en Microsoft Sentinel.

- Instalación de una solución de centro de contenido en Microsoft Sentinel.
- Conexión de un repositorio de GitHub a Microsoft Sentinel.

Después de completar este módulo, podrá:

- Instalación de una solución de centro de contenido en Microsoft Sentinel
- Conexión de un repositorio de GitHub a Microsoft Sentinel

Módulo 50: Explicación de los conceptos de búsqueda de amenazas en Microsoft Sentinel.

Obtenga información sobre el proceso de búsqueda de amenazas en Microsoft Sentinel.

- Concepto de búsqueda de amenazas de ciberseguridad.
- Desarrollo de una hipótesis.
- Explorar MITRE ATT&CK.

Al final de este módulo, podrá hacer lo siguiente:

- Describir los conceptos de búsqueda de amenazas para usarlos con Microsoft Sentinel.
- Definir una hipótesis de búsqueda de amenazas para usarla en Microsoft Sentinel.

Módulo 51: Búsqueda de amenazas con Microsoft Sentinel.

En este módulo obtendrá información sobre cómo identificar de forma proactiva comportamientos de amenaza mediante consultas de Microsoft Sentinel. También va a aprender a usar marcadores y streaming en vivo para la búsqueda de amenazas.

- Configuración del ejercicio.
- Exploración de la creación y administración de consultas de búsqueda de amenazas.
- Conservación de hallazgos importantes con marcadores.
- Observación de amenazas a lo largo del tiempo con streaming en vivo.

Ejercicio: Búsqueda de amenazas mediante Microsoft Sentinel

En este módulo, aprenderá a:

- Usar consultas para buscar amenazas.
- Guardar hallazgos importantes con marcadores.
- Observar amenazas a lo largo del tiempo con streaming en vivo.

Módulo 52: Uso de trabajos de búsqueda en Microsoft Sentinel.

En Microsoft Sentinel, puede buscar en largos períodos de tiempo en conjuntos de datos grandes mediante un trabajo de búsqueda.

- Búsqueda con un trabajo de búsqueda.
- Restauración de datos históricos.

Después de completar este módulo, podrá:

- Uso de trabajos de búsqueda en Microsoft Sentinel.
- Restauración de registros de archivo en Microsoft Sentinel.

Módulo 53: Búsqueda de amenazas con cuadernos en Microsoft Sentinel.

Aprenda a usar cuadernos en Microsoft Sentinel para realizar búsquedas avanzadas.

- Acceso a los datos de Azure Sentinel con herramientas externas.
- Búsqueda con cuadernos.
- Creación de un cuaderno.
- Exploración del código del cuaderno.

Al final de este módulo, podrá hacer lo siguiente:

- Explorar las bibliotecas de API para la búsqueda avanzada de amenazas en Microsoft Sentinel.
- Describir cuadernos en Microsoft Sentinel.
- Crear y usar cuadernos en Microsoft Sentinel.