The DevSecOps Company

Microsoft Partner

SC-200T00
Microsoft Security Operations Analyst

Información general.

En este curso aprenderá 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.

Duración.

4 Días.

Perfil del público.

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.

Examen.

SC-200: Microsoft Security Operations Analyst

Temario.

Ruta de aprendizaje: Mitigación de amenazas mediante Microsoft Defender XDR.

Analice datos sobre amenazas entre dominios y soluciónelas rápidamente con la orquestación y la automatización integradas de Microsoft Defender XDR.

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

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

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

Módulo 2: Mitigación de incidentes con Microsoft Defender.

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

- Uso del portal de Microsoft 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 Microsoft Entra.
- Información sobre la puntuación segura de Microsoft.
- Análisis de amenazas.
- Análisis de los informes.
- Configuración del portal de Microsoft Defender.

Módulo 3: Corrección de riesgos con Microsoft Defender para Office 365.

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

- Introducción a Microsoft Defender para Office 365.
- Automatize, investigue y corrija.
- Configure, proteja y detecte.

Módulo 4: Administrar Microsoft Entra Identity Protection.

La protección de la identidad de un usuario mediante la supervisión de sus patrones de uso e inicio de sesión garantiza una solución de nube segura. Explore cómo diseñar e implementar Microsoft Entra Identity Protection.

- Revisión de los conceptos básicos de Identity Protection.
- Implementación y administración de directivas de riesgo de usuario.
- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado.
- Implementación de la seguridad para las identidades de carga de trabajo.
- Explorar Microsoft Defender for Identity.

Ejercicios:

- Habilitación de una directiva de riesgo de inicio de sesión.
- Configurar la directiva de registro de autenticación multifactor de Microsoft Entra.

Módulo 5: Protección del entorno con Microsoft Defender for Identity.

Obtenga información sobre el componente Microsoft Defender for Identity de Microsoft Defender XDR.

- 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.

Módulo 6: Corrección de riesgos con Microsoft Defender para Office 365.

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

- Introducción a Microsoft Defender para Office 365.
- Automatize, investigue y corrija.
- Configure, proteja y detecte.
- Simular ataques.

Módulo 7: Protección de 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. Proporciona visibilidad enriquecida, control sobre el viaje de los datos y análisis sofisticados para identificar y combatir las ciberamenazas en todos los servicios en la nube. Aprenda a 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.

Ruta de aprendizaje: Mitigación de amenazas con Seguridad de Microsoft Copilot.

Introducción a Microsoft Security Copilot. Conocerá la terminología básica, cómo Seguridad de Microsoft Copilot procesa las solicitudes, los elementos de una solicitud eficaz y cómo habilitar la solución.

Módulo 8: Aspectos básicos de la IA generativa.

En este módulo, explorará la manera en que los modelos de lenguaje permiten a las aplicaciones y servicios de inteligencia artificial generar contenido original basado en la entrada de lenguaje natural. También aprenderá cómo la IA generativa permite la creación de copilotos que pueden ayudar a las personas en las tareas creativas.

- ¿Qué es la inteligencia artificial generativa?
- ¿Qué son los modelos de lenguaje?
- Uso de modelos de lenguaje.
- ¿Qué son los copilotos?
- Microsoft Copilot.
- Consideraciones para los mensajes de Copilot.
- Extensión y desarrollo de copilotos.

Ejercicio: Exploración de Microsoft Copilot.

Módulo 9: Descripción de Seguridad de Microsoft Copilot.

Familiarícese con Microsoft Security Copilot. Conocerás la terminología básica, cómo Microsoft Security Copilot procesa las solicitudes, los elementos de una solicitud eficaz y cómo habilitar la solución.

- Familiarícese con Microsoft Security Copilot.
- Descripción de la terminología de Seguridad de Microsoft Copilot.
- Descripción de cómo Microsoft Security Copilot procesa solicitudes de avisos.
- Describir los elementos de un mensaje eficaz.
- Descripción de cómo habilitar Microsoft Security Copilot.

Módulo 10: Descripción de las características principales de Seguridad de Microsoft Copilot.

Seguridad de Microsoft Copilot tiene un amplio conjunto de características. Conoce los complementos disponibles, los libros de solicitudes, las formas en que puedes exportar y compartir información de Copilot y mucho más.

- Descripción de las características disponibles en la experiencia independiente de Seguridad de Microsoft Copilot.
- Describir las características disponibles en una sesión de la experiencia independiente.
- Descripción de los complementos de Microsoft disponibles en Microsoft Security Copilot.
- Describir los complementos ajenos a Microsoft compatibles con Microsoft Security Copilot.
- Descripción de los libros de solicitudes personalizados.
- Descripción de las conexiones de la base de conocimiento.

Módulo 11: Descripción de experiencias integradas de Seguridad de Microsoft Copilot.

Seguridad de Microsoft Copilot es accesible directamente desde algunos productos de seguridad de Microsoft. Esto se conoce como la experiencia insertada. Obtenga información sobre los escenarios admitidos en la experiencia integrada de Copilot de las soluciones de seguridad de Microsoft.

- Describir Copilot en Microsoft Defender XDR.
- Copilot en Microsoft Purview.
- Copilot en Microsoft Entra.
- Copilot en Microsoft Intune.
- Copilot en Microsoft Defender for Cloud (versión preliminar).

Módulo 12: Exploración de casos de uso de Seguridad de Microsoft Copilot.

Explore los casos de uso de Microsoft Security Copilot en las experiencias independientes e insertadas, mediante ejercicios de laboratorio.

- Explorar la experiencia de primera ejecución.
- Exploración de la experiencia independiente.
- Configuración del complemento de Microsoft Sentinel.
- Habilitar un complemento personalizado.
- Exploración de las cargas de archivos como una base de conocimiento.
- Crear una secuencia de indicaciones personalizada.

- Exploración de las funcionalidades de Copilot en XDR de Microsoft Defender.
- Explorar las funcionalidades de Copilot en Microsoft Purview.

Ruta de aprendizaje: Mitigación de amenazas con Microsoft Purview.

En esta ruta de aprendizaje nos centramos en las soluciones de riesgo y cumplimiento de Microsoft Purview que ayudan a los analistas de operaciones de seguridad a detectar amenazas a las organizaciones e identificar, clasificar y proteger los datos confidenciales, así como supervisar e informar sobre el cumplimiento.

Módulo 13: Respuesta a las alertas de prevención de pérdida de datos mediante Microsoft 365.

Como analista de operaciones de seguridad, debe comprender la terminología y las alertas relacionadas con el cumplimiento normativo. Descubra cómo las alertas de prevención contra la pérdida de datos le ayudan 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.

Módulo 14: Administración del riesgo interno en Microsoft Purview.

La administración de riesgos internos de Microsoft Purview Insider ayuda a las organizaciones a abordar los riesgos internos, como el robo de IP, el fraude y el sabotaje. Obtenga información sobre la administración de riesgos internos y cómo las tecnologías de Microsoft pueden ayudarle a detectar e investigar actividades de riesgo en su organización y a tomar las medidas pertinentes.

- Información general sobre la administración de riesgos internos.
- Introducción a la administración de políticas de riesgo interno.
- Creación y administración de directivas de riesgo interno.
- Investigación de alertas de riesgo interno.
- Tomar medidas sobre las alertas de riesgo interno a través de casos.
- Gestione las pruebas forenses de la gestión de riesgos internos.
- Crear plantillas de avisos de administración de riesgos internos.

Módulo 15: Búsqueda e investigación con la auditoría de Microsoft Purview.

Mejore la seguridad de los datos y el cumplimiento con Microsoft Purview Audit mediante la configuración de auditorías detalladas, la administración de registros y el análisis de patrones de acceso.

- Introducción a Auditoría de Microsoft Purview.
- Configuración y administración de Auditoría de Microsoft Purview.
- Realización de búsquedas con Auditoría (Estándar).
- Auditar interacciones de Microsoft Copilot para Microsoft 365.
- Investigar actividades con Auditoría (Premium).
- Exportar datos de registro de auditoría.
- Configuración de la retención de auditoría con Auditoría (Prémium).

Módulo 16: 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 exhibición de documentos electrónicos de Microsoft Purview.
- Crear una búsqueda de contenido.
- Ver los resultados y las estadísticas de la búsqueda.
- Exportar los resultados de búsqueda y el informe de búsqueda.
- Configurar el filtrado de permisos de búsqueda.
- Buscar y eliminar mensajes de correo electrónico.

Ruta de aprendizaje: Mitigación de amenazas con Microsoft Defender for Endpoint.

Implemente la plataforma Microsoft Defender for Endpoint para detectar e investigar amenazas avanzadas, así como responder a ellas.

Módulo 17: Protección contra amenazas con Microsoft Defender para punto de conexión.

Sepa cómo Microsoft Defender para punto de conexión puede ayudar a su organización a mantenerse segura.

- Introducción a Microsoft Defender para punto de conexión.
- Práctica de la administración de la seguridad.
- Busque amenazas dentro de su red.

Módulo 18: 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.

Módulo 19: 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.

Módulo 20: 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 mediante Microsoft Defender para punto de conexión que le ayudan 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.

Módulo 21: 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.

Módulo 22: Llevar a cabo investigaciones sobre evidencias y entidades con Microsoft Defender para punto de conexión.

Obtén información sobre los artefactos de tu entorno y qué relación tienen con otros artefactos y alertas que te proporcionan conclusiones y te ayudan a comprender el impacto general sobre tu entorno.

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

Módulo 23: 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.

Módulo 24: 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.

Módulo 25: 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.

Ruta de aprendizaje: Mitigación de amenazas con Microsoft Defender for Cloud.

Use Microsoft Defender for Cloud, para la seguridad y la protección de cargas de trabajo locales, en Azure y en la nube híbrida. Esta ruta de aprendizaje se alinea con el examen SC-200: Microsoft Security Operations Analyst.

Módulo 26: 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.

Módulo 27: 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.

Módulo 28: 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.

Módulo 29: 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.

Módulo 30: 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.

Módulo 31: 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.

Ruta de aprendizaje: Creación de consultas para Microsoft Sentinel mediante el Lenguaje de consulta de Kusto (KQL).

Escriba instrucciones en Lenguaje de consulta de Kusto (KQL) para consultar los datos de registro para realizar detecciones, análisis e informes en Microsoft Sentinel. Esta ruta de aprendizaje se centrará en los operadores más usados. Las instrucciones en KQL de ejemplo mostrarán consultas de tabla relacionadas con la seguridad.

Módulo 32: Construcción de instrucciones KQL para Microsoft Sentinel.

El lenguaje de consulta Kusto (KQL) se utiliza para analizar datos con el fin de crear análisis y 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.
- Uso del operador order by.
- Uso de los operadores project.

Módulo 33: 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.

Módulo 34: 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.

Módulo 35: 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.

Ruta de aprendizaje: Configuración del entorno de Microsoft Sentinel.

Para empezar a trabajar con Microsoft Sentinel, configure correctamente el área de trabajo de Microsoft Sentinel.

Módulo 36: 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.

Módulo 37: 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.
- Administrar la configuración de Microsoft Sentinel.
- Configuración de registros.

Módulo 38: 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 Defender XDR.

Módulo 39: 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 de una lista de reproducción.
- Administración de listas de reproducción.

Módulo 40: 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.

Módulo 41: Integración de Microsoft Defender XDR con Microsoft Sentinel.

En este módulo, obtendrá información sobre la plataforma de operaciones de seguridad unificada que integra Microsoft Defender XDR con Microsoft Sentinel.

- Descripción de las ventajas de integrar Microsoft Sentinel con Defender XDR.
- Explore las diferencias de funcionalidad entre los portales de Microsoft Defender XDR y Microsoft Sentinel.
- Incorporación de Microsoft Sentinel a Microsoft Defender XDR.
- Explorar las características de Microsoft Sentinel en Microsoft Defender XDR.

Ruta de aprendizaje: Conexión de registros a Microsoft Sentinel.

Conecte datos a Microsoft Sentinel a la escala de la nube en todos los usuarios, dispositivos y aplicaciones, así como en la totalidad de la infraestructura, tanto en el entorno local como en varias nubes.

Módulo 42: 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.

Módulo 43: 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 44: Conexión de Microsoft Defender XDR a Microsoft Sentinel.

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

- Planear conectores de Microsoft Defender XDR.
- Conexión del conector de Microsoft Defender XDR.
- Conector para la conexión a Microsoft Defender for Cloud.
- Conexión de Microsoft Defender para IoT.
- Conectores heredados para la conexión a Microsoft Defender.

Módulo 45: 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 46: 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.

Módulo 47: 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.

Módulo 48: 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.

Ruta de aprendizaje: Creación de detecciones y realización de investigaciones con Microsoft Sentinel.

Detecte amenazas descubiertas anteriormente y solucionelas rápidamente con opciones de orquestación y automatización en Microsoft Sentinel.

Módulo 49: 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 50: 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 51: Respuesta a amenazas con cuadernos de estrategias de Microsoft Sentinel.

En este módulo se describe cómo crear cuadernos de estrategias de Microsoft Sentinel para responder a amenazas de seguridad.

- ¿Qué son los cuadernos de estrategias de Microsoft Sentinel?
- Desencadenamiento de un cuaderno de estrategias en tiempo real.
- Ejecución de cuadernos de estrategias a petición.

Ejercicio: Creación de un cuaderno de estrategias de Microsoft.

Módulo 52: 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.

Módulo 53: 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.

Módulo 54: Normalización de datos en Microsoft Sentinel.

Al final de este módulo, puedes usar analizadores del modelo de información de seguridad avanzada (ASIM) para identificar 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.

Módulo 55: 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.

Módulo 56: Administración de contenido en Microsoft Sentinel.

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

- Uso de soluciones desde el centro de contenido.
- Uso de repositorios para la implementación.

Ruta de aprendizaje: Búsqueda de amenazas en Microsoft Sentinel.

Busque amenazas de seguridad de forma proactiva por medio de las potentes herramientas diseñadas para tal fin de Microsoft Sentinel.

Módulo 57: 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.
- Exploración de MITRE ATT&CK.

Módulo 58: 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.

Módulo 59: 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.

Módulo 60: 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.