ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT	RED HAT	VIRTUALIZACIÓN
CIBERSEGURIDAD	DESARROLLO	OFFICE
BIG DATA	BLOCK CHAIN	BASES DE DATOS
GESTIÓN DE SERVICIOS IT	CLOUD COMPUTING	METODOLOGÍAS EN PROYECTOS
SISTEMAS OPERATIVOS	Y MÁS...	

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 28 horas

SC-200 / Microsoft Security Operations Analyst

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 y ayuda a los alumnos a prepararse para el examen SC-200: Microsoft Security Operations Analyst.

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.

Rol de trabajo: Ingeniero de Seguridad
Preparación para el examen: SC-200

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.

Módulos

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.

Objetivos de aprendizaje

En este módulo, aprendió el papel que desempeña Microsoft 365 Defender en un SOC moderno. 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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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.

Corrija los riesgos con Microsoft Defender para Office 365

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

Objetivos de aprendizaje

En este módulo, aprenderá cómo:

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

Protege tu entorno con Microsoft Defender for Identity

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

Objetivos de aprendizaje

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.

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.

Objetivos de aprendizaje

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
- Entender cómo usar las directivas de control de aplicación de acceso condicional para controlar el acceso a las aplicaciones de su organización

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 ayudarán en su investigación a encontrar el ámbito completo del incidente.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

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

Administrar 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. Obtenga información sobre la administración de riesgos internos y cómo las tecnologías de Microsoft pueden ayudarlo a detectar, investigar y tomar medidas sobre las actividades de riesgo en su organización.

Objetivos de aprendizaje

Al finalizar este módulo, usted debería ser capaz de:

- Explicar cómo Microsoft Purview Insider Risk Management puede ayudar a prevenir, detectar y contener riesgos internos en una organización.
- Describir los tipos de plantillas de políticas predefinidas e integradas.
- 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 de información privilegiada.

Protégete contra las amenazas con Microsoft Defender para Endpoint

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

Objetivos de aprendizaje

En este módulo, aprenderá cómo:

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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 en Microsoft Defender para punto de conexión

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Describir la capacidad de Administración de amenazas y 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

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.

Objetivos de aprendizaje

- 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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

- En este módulo, aprenderá cómo Microsoft Defender for Cloud proporciona administración de la posición de seguridad. 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.

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.

Objetivos de aprendizaje

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

Corrección de alertas de seguridad mediante Microsoft Defender for Cloud

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

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

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

Uso de KQL para crear instrucciones de varias tablas

Vea cómo se trabaja con varias tablas usando KQL.

Objetivos de aprendizaje

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.

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.

Objetivos de aprendizaje

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.

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.

Objetivos de aprendizaje

Al final de este módulo, podrá:

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

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.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- 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.

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.

Objetivos de aprendizaje

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 para punto de conexión en Microsoft Sentinel
- Activación del conector de Microsoft Defender para Office 365 en Microsoft Sentinel

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.

Objetivos de aprendizaje

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.

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).

Objetivos de aprendizaje

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.

Conexión de orígenes de datos Syslog a Microsoft Sentinel

Conozca las opciones de configuración del conector Syslog, que le permitirá analizar datos de Syslog.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Describir las opciones de implementación del conector Syslog en Microsoft Sentinel
- Ejecutar el script de implementación del conector para enviar datos a Microsoft Sentinel
- Configurar la integración del agente de Log Analytics para Microsoft Sentinel
- Crear un análisis mediante KQL en Microsoft Sentinel

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.

Objetivos de aprendizaje

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

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.

Objetivos de aprendizaje

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

Automatización en Microsoft Sentinel

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

Objetivos de aprendizaje

Después de completar este módulo, podrá:

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

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.

Objetivos de aprendizaje

Objetivos de este módulo:

- Explicar las funcionalidades de SOAR de Microsoft Sentinel.
- Explorar el conector de Microsoft Sentinel en Logic Apps.
- Crear un cuaderno de estrategias para automatizar la respuesta a incidentes.
- Ejecutar un cuaderno de estrategias a petición en respuesta a un incidente.

Administración de incidentes de seguridad en Microsoft Sentinel

En este módulo, investigará la administración de incidentes de Microsoft Sentinel, obtendrá información sobre los eventos y las entidades de Microsoft Sentinel, y verá maneras de resolver los incidentes.

Objetivos de aprendizaje

Objetivos de este módulo:

- Entender la administración de incidentes de Microsoft Sentinel
- Explorar la administración de evidencias y entidades de Microsoft Sentinel
- Investigar y administrar la resolución de incidentes

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.

Objetivos de aprendizaje

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

Normalización de datos en Microsoft Sentinel

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

Objetivos de aprendizaje

Tras finalizar este módulo, podrá:

- Uso de analizadores de ASIM
- Creación del analizador de ASIM
- Creación de funciones KQL parametrizadas

Consulta, visualización y supervisión de datos en Microsoft Sentinel

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

Objetivos de aprendizaje

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.

Administración de contenido en Microsoft Sentinel

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

Objetivos de aprendizaje

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

Explicación de los conceptos de búsqueda de amenazas en Microsoft Sentinel

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

Objetivos de aprendizaje

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.

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.

Objetivos de aprendizaje

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.

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.

Objetivos de aprendizaje

Después de completar este módulo, podrá:

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

Búsqueda de amenazas con cuadernos en Microsoft Sentinel

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

Objetivos de aprendizaje

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