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 / Defend against cyberthreats with Microsoft's security operations platform

Aprenda a investigar, responder y buscar amenazas 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 usar el lenguaje de consulta kusto (KQL) para realizar la detección, el análisis y los informes. El curso se diseñó para personas que trabajan en un rol de operaciones de seguridad y ayuda a los alumnos a prepararse para el examen SC-200: Analista de Operaciones de Seguridad de Microsoft.

Perfil del Público

El Analista de Operaciones de Seguridad de Microsoft colabora con las partes interesadas de la organización para proteger los sistemas de tecnologías 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 investiga principalmente, responde y busca amenazas 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.

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 Defender XDR

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

- Introducción
- Explorar casos de uso de detección y respuesta extendida (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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Explora la caza avanzada
- Investigación de los registros de inicio de sesión de Microsoft Entra
- Información sobre la puntuación segura de Microsoft
- Análisis de Analítica de Amenazas con el Agente de Información de Seguridad de Security Copilot
- Análisis de los informes
- Configuración del portal de Microsoft Defender
- Evaluación de módulos
- Resumen y recursos

Corrección de amenazas mediante Microsoft Defender

Aprenda a investigar y corregir amenazas mediante Microsoft Defender para Office 365 con herramientas automatizadas, evaluación de suplantación de identidad (phishing) y simulación de ataques.

- Introducción a Microsoft Defender para Office 365
- Automatizar, investigar y corregir
- Configurar, proteger y detectar
- Microsoft Security Copilot agente de evaluación de suplantación de identidad en Microsoft Defender
- Simular ataques
- Resumen y prueba de conocimientos

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.

- Introducción
- Repaso de los conceptos básicos de la protección de la identidad
- Implementación y administración de directivas de riesgo de usuario
- Ejercicio: Habilitación de una directiva de riesgo de inicio de sesión
- Ejercicio para configurar la directiva de registro de autenticación multifactor de Microsoft Entra
- 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

- Explorar el agente de administración de riesgos de identidad
- Evaluación de módulos
- Resumen y recursos

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
- Comprobación de conocimiento y Resumen

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen

Introducción a la inteligencia artificial y los agentes generativos

La inteligencia artificial genera aplicaciones que pueden crear contenido, responder preguntas y ayudar con tareas. En este módulo, explorará los aspectos básicos de la inteligencia artificial generativa, incluidos los modelos de lenguaje grande (LLM), las solicitudes y los agentes de IA.

- Introducción
- Modelos de lenguaje grandes (LLM)
- Mensajes
- Agentes de IA
- Ejercicio: Exploración de la inteligencia artificial generativa
- Evaluación del módulo
- Resumen

Describir Microsoft Security Copilot

Familiarícese con Microsoft Security Copilot. Se le presenta cierta terminología básica, cómo Microsoft Security Copilot procesa las indicaciones, los elementos de unas indicaciones eficaces y cómo habilitar la solución.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

Descripción de las características principales de Seguridad de Microsoft Copilot

Microsoft Security 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.

- Introducción
- Descripción de las características disponibles en la experiencia independiente de Microsoft Security Copilot
- Describir las características disponibles en una sesión de la experiencia independiente
- Describir áreas de trabajo
- 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
- Evaluación del módulo
- Resumen y recursos

Descripción de las experiencias integradas de Microsoft Security Copilot

Microsoft Security Copilot es accesible directamente desde algunos productos de seguridad de Microsoft. Esto se conoce como la experiencia insertada. Infórmese sobre los escenarios que admite la experiencia integrada de Copilot en las soluciones de seguridad de Microsoft.

- Introducción
- 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)
- Evaluación del módulo
- Resumen y recursos

Explorar casos de uso de Microsoft Copilot de Seguridad

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

- Introducción
- Explorar la experiencia de primera ejecución
- Exploración de la experiencia independiente
- Exploración de áreas de trabajo de Security Copilot
- 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
- Exploración de las funcionalidades de Copilot en Microsoft Entra
- Evaluación del módulo
- Resumen y recursos

Investigar y responder a alertas de prevención de pérdida de datos de Microsoft Purview

Microsoft Purview y XDR de Microsoft Defender ayudan a las organizaciones a detectar posibles riesgos de pérdida de datos y a responder rápidamente para proteger la información confidencial. Las actividades de investigación y respuesta incluyen revisar las alertas DLP, aplicar las acciones de corrección adecuadas y documentar los resultados de una manera estructurada y coherente

- Introducción
- Descripción de las alertas de prevención de pérdida de datos (DLP)
- Descripción del ciclo de vida de las alertas DLP

- Configuración de directivas DLP para generar alertas
- Investigar las alertas de DLP en Microsoft Purview
- Investiga las alertas DLP en Microsoft Defender XDR
- Responder a alertas DLP
- Evaluación del módulo
- Resumen

Investigación de alertas de riesgo interno y actividad relacionada

Investigue las alertas de riesgo interno y administre casos relacionados en Microsoft Purview para evaluar el comportamiento del usuario, tomar las medidas adecuadas y coordinar las revisiones más profundas en todos los equipos.

- Introducción
- Comprender las alertas de riesgo corporativo interno y las investigaciones
- Administración del volumen de alertas en la administración de riesgos internos
- Investigación y evaluación de alertas de riesgo interno en Microsoft Purview
- Investigación de alertas de riesgo interno con Security Copilot y agentes de Inteligencia Artificial
- Análisis del contexto de alerta con la pestaña Todos los factores de riesgo
- Investigar los detalles de la actividad con la pestaña Explorador de actividades
- Revisión de patrones a lo largo del tiempo con la pestaña Actividad de usuario
- Investigar alertas de riesgo interno en Microsoft Defender XDR
- Administración y toma de medidas en casos de riesgo interno
- Ejercicio: Investigación del posible robo de datos mediante la administración de riesgos internos
- Evaluación del módulo
- Resumen

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
- 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)
- Evaluación de módulos
- Resumen

Buscar contenido con eDiscovery de Microsoft Purview

Use eDiscovery de Microsoft Purview para buscar contenido en Microsoft 365. En este módulo se explica cómo configurar casos, definir criterios de búsqueda y buscar mensajes, archivos y otros datos de la organización.

- Introducción
- Descripción de las funcionalidades de búsqueda de contenido y eDiscovery
- Requisitos previos para usar eDiscovery en Microsoft Purview
- Creación de una búsqueda de eDiscovery
- Realización de una búsqueda de eDiscovery
- Exportación de resultados de búsqueda de eDiscovery
- Evaluación del módulo
- Resumen y recursos

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
- Practique la administración de la seguridad
- Buscar amenazas en la red
- Resumen y prueba de conocimientos

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.

- Introducción
- Creación del entorno
- Descripción de la compatibilidad y las características de los sistemas operativos
- Incorporación de dispositivos
- Administrar 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Descripción de la reducción de la superficie expuesta a ataques
- Habilitar reglas de reducción de la superficie expuesta a ataques
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Uso de la lista de inventario de dispositivos
- Investigación del dispositivo
- Uso del bloqueo de comportamiento
- Detección de dispositivos con detección de dispositivos
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Investigar un archivo
- Investigación de una cuenta de usuario
- Investigar una dirección IP
- Investigar un dominio
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Configurar características avanzadas
- Configurar notificaciones de alerta
- Administración de la eliminación de alertas
- Administración de los indicadores
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Descripción de Administración de amenazas y vulnerabilidades
- Exploración de las vulnerabilidades de sus dispositivos
- Administración de la corrección
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Explicación de Microsoft Defender for Cloud
- Descripción de las protecciones de cargas de trabajo de Microsoft Defender for Cloud
- Ejercicio: Guía interactiva de Microsoft Defender for Cloud
- Habilitación de Microsoft Defender for Cloud
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Exploración y administración de los recursos con Asset Inventory
- Configuración del aprovisionamiento automático
- Aprovisionamiento manual de agentes
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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.

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

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

Corrección de alertas de seguridad mediante Microsoft Defender for Cloud

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

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Descripción de la estructura de instrucciones del lenguaje de consulta Kusto
- Uso del operador de búsqueda
- Uso del operador where
- Usar la instrucción Let
- Uso del operador extend
- Uso del operador order by
- Uso de los operadores project
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

Uso de KQL para crear instrucciones de varias tablas

Vea cómo se trabaja con varias tablas usando KQL.

- Introducción
- Uso del operador union
- Uso del operador join
- Evaluación del módulo
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación del módulo
- Resumen y recursos

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.

- Introducción
- ¿Qué es Microsoft Sentinel?
- Funcionamiento de Microsoft Sentinel
- Cuándo usar Microsoft Sentinel
- Evaluación del módulo
- Resumen

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación del módulo
- Resumen y recursos

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.

- Introducción
- Planear listas de reproducción
- Creación de una lista de reproducción
- Administrar listas de seguimiento
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Definición de Inteligencia sobre amenazas
- Administrar los indicadores de amenazas
- Visualización de los indicadores de amenazas con KQL
- Evaluación de módulos
- Resumen y recursos

Integración de Microsoft Defender XDR con Microsoft Sentinel

En este módulo, aprenderá cómo el portal de Microsoft Defender integra XDR de Microsoft Defender con Microsoft Sentinel.

- Introducción
- Comprender las ventajas de integrar Microsoft Sentinel con XDR de Defender
- Exploración de las diferencias de funcionalidad entre los portales de Microsoft Defender XDR y Microsoft Sentinel
- Incorporación de Microsoft Sentinel a XDR de Microsoft Defender
- Exploración de las características de Microsoft Sentinel en XDR de Microsoft Defender
- Ejercicio: Conexión de Microsoft Sentinel a XDR de Microsoft Defender
- Evaluación del módulo
- Resumen

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.

- Introducción
- Ingesta de datos de registro con conectores de datos
- Descripción de los proveedores de conectores de datos
- Visualización de hosts conectados
- Evaluación de módulos
- Resumen y recursos

Conexión de servicios Microsoft a Microsoft Sentinel

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

- Introducción
- Planeamiento para usar conectores de servicios de Microsoft
- Conexión del conector de Microsoft 365
- Conectar el conector de Microsoft Entra
- Conectar el conector de protección de Microsoft Entra ID
- Conexión del conector de actividad de Azure
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

Conexión de hosts de Windows a Microsoft Sentinel

Dos de los registros más comunes que se van a recopilar son eventos de seguridad de Windows y Sysmon. Obtenga información sobre cómo Microsoft Sentinel facilita esto con los conectores de datos de eventos de Microsoft Windows.

- Introducción
- Planeamiento para usar el conector de eventos de seguridad de hosts Windows
- Conéctate utilizando los 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
- Evaluación de módulos
- Resumen y recursos

Conexión de registros de formato de eventos comunes 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).

- Introducción
- Planeamiento para usar el conector de formato de evento común
- Conexión de una solución externa mediante el conector de formato de evento común
- Evaluación de módulos
- Resumen y recursos

Conexión de hosts de Windows a Microsoft Sentinel

Dos de los registros más comunes que se van a recopilar son eventos de seguridad de Windows y Sysmon. Obtenga información sobre cómo Microsoft Sentinel facilita esto con los conectores de datos de eventos de Microsoft Windows.

- Introducción
- Planeamiento para usar el conector de eventos de seguridad de hosts Windows
- Conéctate utilizando los 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- Planeamiento para usar conectores de inteligencia sobre amenazas
- Conexión del conector de inteligencia sobre amenazas de Defender
- Conexión del conector TAXII de inteligencia sobre amenazas
- Conexión del conector de API de carga de inteligencia sobre amenazas
- Visualización de los indicadores de amenazas con KQL
- Evaluación del módulo
- Resumen y recursos

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.

- Introducción
- Ejercicio: Detección de amenazas con análisis de Microsoft Sentinel
- ¿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
- Administrar reglas de análisis
- Ejercicio: Detección de amenazas con análisis de Microsoft Sentinel
- Resumen

Automatización en Microsoft Sentinel

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

- Introducción
- Descripción de las opciones de automatización
- Creación de reglas de automatización
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción

- Ejercicio: Creación de un cuaderno de estrategias de Microsoft Sentinel
- ¿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 Sentinel
- Resumen

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.

- Introducción
- Ejercicio: Configuración del entorno de Azure
- Descripción de incidentes
- Evidencia y entidades de un incidente
- Administración de incidentes
- Ejercicio: Investigación de un incidente
- Resumen

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.

- Introducción
- Descripción del análisis de comportamiento
- Exploración de entidades
- Mostrar información de comportamiento de entidad
- Uso de plantillas de reglas analíticas de detección de anomalías
- Evaluación de módulos
- Resumen y recursos

Normalización de datos en Microsoft Sentinel

Al final de este módulo, puede usar analizadores del modelo de información de seguridad avanzada (ASIM) para identificar amenazas dentro de la organización.

- Introducción
- 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
- Evaluación del módulo
- Resumen y recursos

Consulta, visualización y supervisión de datos en Microsoft Sentinel

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

- Introducción
- Ejercicio: Consulta y visualización de datos con los libros de trabajo de 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
- Ejercicio: Visualización de datos mediante libros de Microsoft Sentinel
- Resumen

Administración de contenido en Microsoft Sentinel

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

- Introducción3 min
- Uso de soluciones desde el centro de contenido3 min

- Uso de repositorios para la implementación3 min
- Evaluación del módulo3 min
- Resumen y recursos

Explicación de los conceptos de búsqueda de amenazas en Microsoft Sentinel

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

- Introducción
- Concepto de búsqueda de amenazas de ciberseguridad
- Desarrollo de una hipótesis
- Exploración de MITRE ATT&CK
- Evaluación de módulos
- Resumen y recursos

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.

- Introducción
- 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
- Resumen

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.

- Introducción
- Búsqueda con un trabajo de búsqueda
- Restauración de datos históricos
- Evaluación del módulo
- Resumen y recursos

Búsqueda de amenazas con cuadernos en Microsoft Sentinel

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

- Introducción
- Acceso a los datos de Azure Sentinel con herramientas externas
- Búsqueda con cuadernos
- Creación de un cuaderno
- Exploración del código del cuaderno
- Evaluación del módulo
- Resumen y recursos