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: 7 horas

SC-5001 / Configure SIEM security operations using Microsoft Sentinel

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

Perfil del Público

Este curso es ideal para aquellos que buscan profundizar en la configuración y gestión de operaciones de seguridad utilizando Microsoft Sentinel, con un enfoque práctico y orientado a la implementación en entornos reales.

Requisitos Previos

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

- ✓ Experiencia en monitoreo y respuesta a amenazas de seguridad.
- ✓ Comprensión general de la administración y configuración de infraestructuras de TI, incluyendo redes, servidores y servicios en la nube.
- ✓ Experiencia básica con servicios y soluciones de Microsoft Azure, incluyendo la administración de recursos y la configuración de servicios en la nube.
- ✓ Familiaridad con herramientas y tecnologías de gestión de información y eventos de seguridad (SIEM) es beneficioso pero no estrictamente necesario.
- ✓ Habilidades técnicas generales, incluyendo la capacidad de trabajar con scripts y automatización en un entorno de TI.

Módulos

Creación y administración de áreas de trabajo de Microsoft Sentinel

- 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.
- Administrar la configuración de Microsoft Sentinel.
- Configuración de registros.
- Prueba de conocimientos.
- Resumen y recursos

ExecuTrain
Impulsamos tu talento tecnológico

Conexión de servicios Microsoft a Microsoft Sentinel

- Introducción.
- 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
- Prueba de conocimientos
- Resumen y recursos

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.

- Introducción
- 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
- Prueba de conocimientos
- 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.

- Introducción3 min.
- Ejercicio: Detección de amenazas con análisis de Microsoft Sentinel20 min.
- ¿Qué es Análisis de Microsoft Sentinel?5 min.
- Tipos de reglas de análisis5 min.
- Creación de una regla de análisis a partir de plantillas8 min.
- Creación de una regla de análisis a partir del asistente8 min.
- Administración de reglas de análisis4 min.
- Ejercicio: Detección de amenazas con análisis de Microsoft Sentinel12 min.
- Resumen5 min.

Automatización en Microsoft Sentinel

Al final de este módulo, podrá 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
- Prueba de conocimientos
- Resumen y recursos

Configuración de operaciones de seguridad de SIEM mediante Microsoft Sentinel

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

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