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-5004 / Defend against cyberthreats with Microsoft Defender XDR

Implemente el entorno de Microsoft Defender para punto de conexión para administrar dispositivos, realizar investigaciones en puntos de conexión, administrar incidentes en Defender XDR y usar la búsqueda avanzada con lenguaje de consulta Kusto (KQL) para detectar amenazas únicas.

Perfil del Público

El curso SC-5004: Defiende contra ciberamenazas con Microsoft Defender XDR está dirigido a profesionales de ciberseguridad, analistas de seguridad y administradores de TI que buscan proteger sus entornos empresariales contra amenazas avanzadas. Es ideal para quienes desean aprender a implementar, configurar y gestionar Microsoft Defender XDR para detectar, investigar y responder a incidentes de seguridad de manera efectiva. Se recomienda contar con conocimientos básicos de seguridad informática y herramientas de gestión de amenazas.

Requisitos Previos

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

- ✓ Experiencia con el portal de Microsoft Defender
- ✓ Conocimientos básicos de Microsoft Defender para punto de conexión
- ✓ Conocimientos básicos de Microsoft Sentinel
- ✓ Experiencia con el uso del Lenguaje de consulta Kusto (KQL) en Microsoft Sentinel

Módulos

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
- 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
- Prueba de conocimientos
- Resumen y recursos

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
- 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
- Prueba de conocimientos
- 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
- Prueba de conocimientos
- 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
- Prueba de conocimientos
- 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
- Prueba de conocimientos
- Resumen y recursos

Defensa contra ciberamenazas con ejercicios de laboratorio de XDR de Microsoft Defender

En este módulo, ha aprendido a configurar XDR de Microsoft Defender, a implementar Microsoft Defender para punto de conexión e incorporar dispositivos. También ha configurado directivas, amenazas mitigadas y respondido a incidentes con Defender XDR.

- Introducción
- Configuración del entorno de Microsoft Defender XDR
- Implementación de Microsoft Defender para punto de conexión
- Mitigación de ataques con Microsoft Defender para punto de conexión
- Resumen