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-5009 / Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra

Proteja las soluciones de inteligencia artificial en la nube mediante la configuración de cargas de trabajo de inteligencia artificial, la aplicación de protecciones nativas de la nube y el refuerzo de los resultados de seguridad con controles de identidad. Obtenga información sobre cómo se autentican las cargas de trabajo de inteligencia artificial, cómo se establecen los límites de confianza y cómo la postura de seguridad y la protección de cargas de trabajo reducen el riesgo con Microsoft Defender for Cloud y Microsoft Foundry. Amplíe estas protecciones mediante Microsoft Entra para diseñar y aplicar controles de identidad y acceso que expliquen y protejan las decisiones de seguridad anteriores. Resultados de aprendizaje:

- Aplicación de la administración de la posición de seguridad y la protección de cargas de trabajo para los servicios de inteligencia artificial mediante Microsoft Defender for Cloud
- Configuración y protección de entornos de Microsoft Foundry mediante controles de seguridad nativos de la nube
- Diseñar y aplicar controles de identidad y acceso para cargas de trabajo de IA mediante Microsoft Entra

Perfil del Público

Este curso está diseñado para profesionales responsables de proteger y operar cargas de trabajo de inteligencia artificial en la nube. El público incluye ingenieros de seguridad en la nube, ingenieros de plataforma y equipos de aplicaciones que trabajan con servicios de inteligencia artificial que necesitan comprender cómo se aplican la protección de cargas de trabajo, la posición de seguridad y los controles de identidad a los entornos de inteligencia artificial. Se recomienda estar familiarizado con Azure, los conceptos de seguridad nativos de la nube y los principios básicos de identidad y acceso.

Requisitos Previos

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

- ✓ Experiencia en la administración de suscripciones, cargas de trabajo y planes de Defender for Cloud de Azure
- ✓ Familiaridad con Microsoft Foundry y cómo se implementan las cargas de trabajo de inteligencia artificial en Azure
- ✓ Descripción de los principios básicos de seguridad en la nube, incluida la administración de la posición, el control de acceso y la investigación de incidentes

Módulos

Comprender cómo Microsoft Defender para la Nube apoya la seguridad y gobernanza de la IA en Azure

Microsoft Defender for Cloud desempeña un papel central en la protección de cargas de trabajo de inteligencia artificial en Azure. Obtenga información acerca de cómo Microsoft Defender for Cloud admite la seguridad de la inteligencia artificial en Azure. Explora las capas de una carga de trabajo de IA, los riesgos únicos que introducen los sistemas de inteligencia artificial y las barreras de seguridad que protegen las entradas y salidas del modelo. Vea cómo Microsoft Purview, Microsoft Entra ID y Microsoft Foundry funcionan conjuntamente para respaldar una estrategia unificada de seguridad y gobernanza.

- Introducción
- Descripción de los servicios de inteligencia artificial en Azure
- Descripción de los riesgos de seguridad de la inteligencia artificial en Azure
- Salvaguardias y protecciones de inteligencia artificial en Azure
- Cómo admiten las herramientas de seguridad y gobernanza de Azure las cargas de trabajo de inteligencia artificial
- Evaluación del módulo
- Resumen

Protección de cargas de trabajo de INTELIGENCIA ARTIFICIAL con Microsoft Defender for Cloud

Microsoft Defender for Cloud ayuda a proteger las cargas de trabajo de inteligencia artificial mediante la combinación de la detección, la administración de la posición y la protección en tiempo de ejecución en una plataforma. Aprenderá a habilitar la planificación de cargas de trabajo de IA, revisar los análisis en el panel de seguridad de Datos e IA, evaluar la postura usando Cloud Security Posture Management (CSPM), detectar amenazas en tiempo de ejecución con Cloud Workload Protection (CWP) e investigar incidentes en Microsoft Defender XDR. Estas funcionalidades funcionan conjuntamente para identificar brechas de configuración, detectar comportamientos sospechosos y proporcionar visibilidad de un extremo a otro en los entornos de inteligencia artificial.

- Introducción
- Habilitación del plan de cargas de trabajo de IA
- Revisión de la información en el panel de seguridad de datos e inteligencia artificial
- Evaluación y mejora de la posición de seguridad de la inteligencia artificial con Cloud Security Posture Management (CSPM)
- Detección de amenazas de inteligencia artificial en tiempo de ejecución con Cloud Workload Protection (CWP)
- Investigue alertas de seguridad de inteligencia artificial con pruebas rápidas en Microsoft Defender XDR
- Evaluación del módulo
- Resumen

Configuración y administración de límites de protección en Microsoft Foundry

Los límites de protección de Microsoft Foundry ayudan a proteger las cargas de trabajo de inteligencia artificial mediante la aplicación de controles de seguridad configurables que evalúan las solicitudes y las respuestas. Aprenderá a comprender los modelos de seguridad integrados, probar y refinar los límites de protección, crear listas de bloqueos, configurar filtros de contenido y validar que las protecciones funcionan según lo previsto. Estas funcionalidades ayudan a las organizaciones a evitar interacciones no seguras o que infringen directivas, proteger los datos confidenciales y mantener la confianza en las aplicaciones asistidas por IA.

- Introducción
- Descripción de los límites de protección y la seguridad del contenido de Microsoft
- Descripción de los controles de seguridad en Microsoft Foundry
- Prueba de barreras de protección integradas
- Creación y administración de listas de bloqueados en Microsoft Foundry

- Configurar y aplicar límites de protección en Microsoft Foundry
- Elección y refinación de los límites de protección adecuados para las cargas de trabajo de IA
- Evaluación del módulo
- Resumen

Protección de entornos de Microsoft Foundry

Para proteger los entornos de Microsoft Foundry, se requieren protecciones superpuestas que controlan el acceso, protegen las credenciales, aíslan la comunicación de red y mantienen la visibilidad de los recursos conectados. El enfoque incluye definir límites de acceso con Microsoft Entra ID y los roles de proyecto, e integrar Key Vault para la gestión de secretos. También usa redes virtuales administradas, Private Link y registro de diagnóstico para mantener la privacidad, la visibilidad y el cumplimiento. Estos procedimientos crean entornos de inteligencia artificial seguros y rastreables que admiten la colaboración sin poner en peligro la protección.

- Introducción
- Control del acceso a Microsoft Foundry con el identificador de Entra de Microsoft
- Administrar el acceso en proyectos de Microsoft Foundry
- Protección de secretos de Microsoft Foundry con Azure Key Vault (versión preliminar)
- Aislamiento de redes con red virtual administrada y Private Link
- Habilitación del registro de diagnóstico en Microsoft Foundry
- Evaluación del módulo
- Resumen

Descripción de la arquitectura de identidad para cargas de trabajo de IA

La arquitectura de identidad define quién puede implementar, invocar y administrar cargas de trabajo de IA en Azure. El identificador de Entra de Microsoft rige el acceso entre planos de administración y datos, los flujos de autenticación establecen límites de confianza para los puntos de conexión de IA y las decisiones de ámbito de rol determinan el radio de explosión. Los tipos de identidad, las asignaciones de roles y los límites de ámbito dan forma a los resultados de seguridad de inteligencia artificial mucho antes de aplicar los controles de cumplimiento.

- Introducción
- Identidad como capa de control para soluciones de inteligencia artificial
- Acceso a los planos de gestión y de datos en las cargas de trabajo de la IA
- Flujos de autenticación para puntos de conexión de IA en Microsoft Foundry
- Identidades humanas y de carga de trabajo en entornos de IA
- Asignaciones de roles y ámbito en entornos de IA
- Configuraciones incorrectas de identidad comunes en implementaciones de IA
- Evaluación del módulo
- Resumen

Implementación de la administración de acceso para recursos de Azure

Explore cómo usar roles integrados de Azure, identidades administradas y directivas de RBAC para controlar el acceso a los recursos de Azure. La identidad es la clave para proteger las soluciones.

- Introducción
- Asignación de roles de Azure
- Configuración de roles personalizados de Azure
- Creación y configuración de identidades administradas
- Acceso a recursos de Azure con identidades administradas
- Análisis de permisos de rol de Azure
- Configuración de directivas de RBAC de Azure Key Vault
- Recuperación de objetos de Azure Key Vault
- Explorar la Administración de permisos de Microsoft Entra
- Prueba de conocimientos
- Resumen y recursos

Planear, implementar y administrar el acceso condicional

El acceso condicional proporciona una granularidad fina de control sobre qué usuarios e identidades pueden realizar actividades específicas, acceder a

los recursos y cómo garantizar que los datos y los sistemas sean seguros, incluidas las identidades de agente de IA administradas a través del identificador de Microsoft Entra Agent.

- Introducción
- Configurar valores predeterminados de seguridad
- Ejercicio: uso de los valores predeterminados de seguridad
- Planificación de directivas de acceso condicional
- Implementación de controles y asignaciones de directivas de acceso condicional
- Ejercicio: implementación de roles y asignaciones de directivas de acceso condicional
- Prueba de las directivas de acceso condicional y solución de problemas relacionados
- Implementación de controles de aplicación
- Implementación de la administración de sesiones y la evaluación continua de acceso
- Ejercicio: configuración de los controles de sesión de autenticación
- Agente de optimización de acceso condicional de Microsoft Entra
- Evaluación de módulos
- Resumen y recursos

Administración de 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 segura en la nube. 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