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-500 / Implement end-to-end security controls for cloud and AI workloads

Este curso te prepara para diseñar, implementar y gestionar controles de seguridad integrales en entornos de Microsoft Azure y Microsoft 365, incluyendo el panorama emergente de cargas de trabajo de IA y agentes autónomos. Mediante una combinación de sesiones dirigidas por el instructor y laboratorios prácticos, desarrollarás habilidades prácticas en seguridad de identidad, protección de infraestructura en la nube, detección de amenazas y gestión de la postura de seguridad. Este curso está dirigido a ingenieros de seguridad responsables de planificar e implementar controles de seguridad en entornos de nube, híbridos y multinube utilizando tecnologías de seguridad de Microsoft.

Perfil del Público

Como candidato para este curso, usted es un ingeniero de seguridad que protege los sistemas y datos de la organización en entornos de nube e híbridos mediante la implementación de controles de seguridad integrales que previenen el acceso no autorizado y mitigan los riesgos de forma proactiva. Este rol abarca múltiples dominios de seguridad, incluyendo identidad, red, aplicación, datos y computación. Este rol también garantiza que las plataformas, los datos, las identidades y la infraestructura utilizadas por las cargas de trabajo de IA se implementen y supervisen de forma segura. Trabajará en estrecha colaboración con arquitectos, administradores, ingenieros, analistas y desarrolladores responsables de Azure, Microsoft 365, identidad y acceso, protección de la información, operaciones de seguridad, DevOps, desarrollo de aplicaciones, plataformas de bases de datos y redes. Debe tener experiencia práctica en la administración de Microsoft Azure y entornos híbridos, incluyendo computación, red y almacenamiento. Debe tener un profundo conocimiento de Microsoft Entra ID y de la administración de Microsoft 365. Sus responsabilidades para este rol incluyen:

- Protección del acceso a los recursos mediante Microsoft Entra ID y Azure Key Vault.
- Garantizar la seguridad y el cumplimiento normativo.
- Garantizar la seguridad del almacenamiento, las bases de datos y las redes.
- Garantizar la seguridad informática
- Garantizar la seguridad de las soluciones de IA
- Gestionar y supervisar la postura de seguridad

Rol de trabajo: Ingeniero de seguridad

Requisitos Previos

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

- ✓ Familiaridad con los conceptos de Microsoft Entra ID, incluidos usuarios, grupos y roles de directorio.
- ✓ Comprensión del control de acceso basado en roles (RBAC) de Azure, incluidas las asignaciones de roles y la jerarquía de ámbito de Azure (grupo de administración, suscripción, grupo de recursos, recurso).
- ✓ Experiencia básica en la navegación por el portal de Azure y el centro de administración de Microsoft Entra.
- ✓ Conocimiento de los principios de seguridad de Zero Trust, incluidos el privilegio mínimo y la presunción de violación.
- ✓ Conocimiento de los requisitos de licencia de Microsoft Entra ID P2 o Microsoft Entra ID Governance

Módulos

Gestionar e implementar métodos de autenticación en Microsoft Entra ID

Aprenda a planificar, implementar y administrar la autenticación segura en Microsoft Entra ID. Este módulo abarca los métodos de autenticación, la autenticación multifactor con acceso condicional, las opciones sin contraseña y el restablecimiento de contraseña de autoservicio.

- Introducción
- Explora los métodos de autenticación de Microsoft Entra ID.
- Configurar la autenticación multifactor en Microsoft Entra ID
- Implementar la autenticación sin contraseña en Microsoft Entra ID
- Configurar el restablecimiento de contraseña de autoservicio en Microsoft Entra ID
- Ejercicio: Configurar métodos de autenticación en Microsoft Entra ID
- Evaluación del módulo
- Resumen

Implementar y configurar la gestión de identidades privilegiadas (PIM).

Implemente el acceso privilegiado Just-in-Time mediante la administración de identidades privilegiadas (PIM) para reducir los privilegios permanentes en los roles de Microsoft Entra, los recursos de Azure y el acceso basado en grupos para entornos de nube e IA.

- Introducción
- Por qué son importantes la gestión de identidades privilegiadas y el acceso justo a tiempo.
- Capacidades básicas de la gestión de identidades privilegiadas (PIM)
- Implementar el acceso justo a tiempo para los roles de Microsoft Entra.
- Implementar el acceso justo a tiempo para los roles y recursos de Azure.
- Escalado con PIM para grupos
- Aplicación del acceso JIT a cargas de trabajo, agentes y aplicaciones de IA
- Patrones de diseño JIT y mejores prácticas
- Evaluación del módulo
- Resumen

Autentique su complemento de API para agentes declarativos con API seguras.

Al crear aplicaciones para el trabajo, normalmente se integran con API seguras. Aprenda sobre las dos formas más comunes de proteger las API: clave de API y OAuth2, y cómo integrarlas al crear un complemento de API para agentes declarativos que se ejecutan en Microsoft 365 Copilot.

- Introducción
- Integrar un plugin de API con una API protegida con una clave.
- Ejercicio: Integrar un complemento de API con una API protegida con una clave.
- Integrar un plugin de API con una API protegida con OAuth.
- Ejercicio: Integrar un complemento de API con una API protegida con OAuth.
- Evaluación del módulo
- Resumen

Configuración y protección de Azure Key Vault

Configure una Azure Key Vault protegida por la seguridad para cargas de trabajo empresariales. Aplique la eliminación temporal y la protección contra la purga, aplique el acceso RBAC con privilegios mínimos con activación Just-In-Time y proteja el perímetro de red mediante reglas de firewall y puntos de conexión privados.

- Introducción
- Implementación de Azure Key Vault con controles de seguridad
- Configuración de acceso a Azure Key Vault
- Configuración del firewall y la red de Key Vault
- Comprobación de conocimiento
- Resumen

Administración de claves y secretos en Azure Key Vault

Administre el ciclo de vida de seguridad de las claves criptográficas y los secretos en Azure Key Vault. Configure las claves respaldadas por HSM, implemente Bring Your Own Key (BYOK) para escenarios normativos, configure la rotación automatizada de claves y cree una rotación de secretos sin tiempo de inactividad mediante patrones de credenciales duales.

- Introducción
- Administrar claves criptográficas en Azure Key Vault
- Administración de secretos en Azure Key Vault
- Comprobación de conocimiento
- Resumen

Administración de certificados y supervisión de Azure Key Vault

Administre el ciclo de vida de los certificados en Azure Key Vault mediante la emisión de la entidad de certificación y la renovación automática integradas. Habilite el registro de diagnóstico para crear una pista de auditoría lista para investigación, configurar reglas de alertas basadas en registros e integrar Event Grid para la automatización del ciclo de vida en tiempo real.

- Introducción
- Administración de certificados en Azure Key Vault
- Habilitación del registro de auditoría de Key Vault
- Comprobación de conocimiento
- Resumen

Protección de Azure Key Vault con Microsoft Defender para la nube

Proteja Azure Key Vault con Microsoft Defender para la nube. Utilice el examen de secretos sin agente de CSPM de Defender para detectar credenciales expuestas en máquinas virtuales (VM) e implementaciones en la nube, habilite Microsoft Defender para Key Vault para detectar patrones de acceso malintencionados y responda de manera eficaz a las alertas de seguridad de Key Vault.

- Introducción
- Análisis de secretos expuestos con Administración de la posición de seguridad en la nube (CSPM) de Defender
- Habilitar Microsoft Defender para Key Vault
- Investigar y responder a alertas de Defender para Key Vault
- Comprobación de conocimiento
- Resumen

Imponer la gobernanza con Azure Policy y bloqueos de recursos

Aplique los estándares de seguridad antes de que los recursos lleguen a producción mediante Azure Policy. Asigne definiciones e iniciativas de directivas integradas en el ámbito del grupo de administración, cree definiciones personalizadas con tareas de corrección automatizadas y proteja los recursos críticos frente a la eliminación mediante bloqueos de recursos Azure

- Introducción
- Asignar definiciones integradas de Azure Policy
- Creación e implementación de definiciones de directivas personalizadas
- Implemente bloqueos de recursos
- Comprobación de conocimiento
- Resumen

Configuración de controles de seguridad y recomendaciones de corrección en Defender for Cloud

Configurar los estándares de seguridad de Defender for Cloud en el ámbito del grupo de administración e implementar sistemáticamente controles de seguridad para remediar recomendaciones. Administre estándares de seguridad personalizados, asigne la responsabilidad de las recomendaciones mediante reglas de gobernanza y aplique correcciones a gran escala utilizando Fix, las tareas de corrección de Azure Policy y las exenciones estructuradas.

- Introducción
- Configuración de Defender for Cloud y administración de estándares de seguridad
- Implementación de controles de corrección a escala
- Comprobación de conocimiento
- Resumen

Evaluación del cumplimiento normativo en Defender for Cloud

En este módulo, usará Microsoft Defender para la nube para evaluar la posición de cumplimiento de su organización con respecto a los marcos de seguridad. Explore el panel de cumplimiento normativo, investigue brechas de control, asigne estándares normativos y genere informes listos para auditoría que comuniquen el estado de cumplimiento a las partes interesadas.

- Introducción
- Descripción de los estándares y controles de cumplimiento en Defender for Cloud
- Navegación por el panel de cumplimiento normativo e investigación de brechas de control
- Asignación de estándares y comunicación de la posición de cumplimiento
- Comprobación de conocimiento
- Resumen

Administración y asignación de roles de RBAC de tamaño adecuado para privilegios mínimos

Implemente la gobernanza del acceso con privilegios mínimos en Azure y Microsoft Entra ID. Asigne roles integrados en el ámbito adecuado, cree roles personalizados para recursos de Azure y operaciones del directorio de Microsoft Entra. A continuación, identifique y corrija el acceso con privilegios excesivos usando las revisiones de acceso de Microsoft Entra y la información sobre identidad en Defender for Cloud Security Posture Management (CSPM).

- Introducción
- Asignación y administración de roles integrados de Azure
- Crear roles personalizados de Azure y roles de Microsoft Entra
- Evaluar y remediar el acceso con exceso de privilegios
- Comprobación de conocimiento
- Resumen

Protección de datos de copia de seguridad con características de seguridad de Azure Backup

Proteja Azure Backup datos contra ransomware, eliminación accidental y administradores no autorizados. Configure la eliminación temporal mejorada, la inmutabilidad de los almacenes, la autorización multiusuario con Resource Guard y los controles RBAC para lograr una calificación de posición de seguridad excelente en los almacenes de Recovery Services.

- Introducción
- Habilitación de la eliminación temporal y almacenes inmutables
- Configuración de la autorización multiusuario y RBAC para la copia de seguridad
- Comprobación de conocimiento
- Resumen

Implementación de controles de seguridad en la infraestructura como código

Incorpore controles de seguridad en la infraestructura como canalizaciones de código

para evitar que los recursos de Azure que no cumplan las normas lleguen a producción. Integre el examen de seguridad de IaC mediante Microsoft Defender para DevOps y la extensión de Microsoft DevOps (MSDO) y configure Azure Policy en un flujo de trabajo de directiva como código para aplicar el cumplimiento de seguridad en el momento de la implementación.

- Introducción
- Examen de plantillas de IaC mediante Microsoft Defender para DevOps
- Aplicación del cumplimiento de directivas en implementaciones de IaC
- Comprobación de conocimiento
- Resumen

Descripción de los servicios de almacenamiento de Azure

En este módulo se presenta el almacenamiento en Azure, lo que incluye aspectos como diferentes tipos de almacenamiento y cómo una infraestructura distribuida puede hacer que los datos sean más resistentes.

- Introducción
- Descripción de las cuentas de almacenamiento de Azure
- Descripción de la redundancia de almacenamiento de Azure
- Descripción de los servicios de almacenamiento de Azure
- Identificación de las opciones de migración de datos de Azure
- Identificación de las opciones de movimiento de archivos de Azure
- Evaluación de módulos
- Resumen

Implementación de la seguridad y administración del acceso para Azure Storage

Implemente controles de seguridad de nivel de cuenta y gobernanza de acceso para Azure Storage. Configure la configuración de transferencia segura, elija los modelos de autorización adecuados, aplique directivas de acceso almacenadas para la administración del ciclo de vida de SAS y aplique la deshabilitación de clave compartida mediante Azure Policy para proteger las cuentas de almacenamiento que usan los agentes de IA y las cargas de trabajo empresariales.

- Introducción
- Configuración de las opciones de seguridad de la cuenta de almacenamiento
- Selección de un modelo de autorización para Azure Storage
- Administrar el acceso con directivas de acceso almacenadas
- Deshabilitación de la autorización de clave compartida y aplicación con Azure Policy
- Comprobación de conocimiento
- Resumen

Configuración de la seguridad de red para Azure Storage

Configure los controles de acceso de nivel de red para las cuentas de Azure Storage. Aplique reglas de firewall, defina la red virtual y el acceso basado en IP, configure reglas de instancia de recursos para Servicios de Azure AI, administre excepciones de servicio de confianza e implemente puntos de conexión privados para eliminar la exposición del punto de conexión público.

- Introducción
- Describir los controles de seguridad de red de Azure Storage
- Configuración de reglas de ip y red virtual
- Configure las reglas de instancia de recursos y los servicios de confianza
- Implementación de puntos de conexión privados para cuentas de almacenamiento
- Comprobación de conocimiento
- Resumen

Implementación de Microsoft Defender para Storage

Habilite y configure Microsoft Defender para Storage para detectar amenazas contra Azure Blob Storage, Azure Files y Azure Data Lake Storage. Configure la supervisión de actividades, el examen de malware con controles de costos, la detección de amenazas de datos confidenciales y el enrutamiento de alertas para asegurarse de que las salidas de Defender lleguen al equipo de seguridad adecuado.

- Introducción
- Exploración de Microsoft Defender para funcionalidades de almacenamiento
- Habilitación e implementación de Defender para Storage
- Configuración del examen de malware y la detección de datos confidenciales
- Configuración del enrutamiento de alertas y validación de la cobertura de Defender
- Comprobación de conocimiento
- Resumen

Configuración de la seguridad de nivel de plataforma para Azure SQL

Configure la autenticación, el aislamiento de red, el cifrado y los controles de acceso para Azure SQL Database y SQL Managed Instance. Implemente la autenticación solo Microsoft Entra ID con acceso de identidad administrada para cargas de trabajo de IA, implemente puntos de conexión privados y aplique cifrado de datos transparente, enmascaramiento dinámico de datos y seguridad de nivel de fila para proteger los datos financieros confidenciales.

- Introducción
- Configuración de la autenticación y el acceso a la identidad administrada
- Implementar aislamiento de red
- Cifrado y protección de datos en tránsito y en reposo
- Aplica enmascaramiento de datos y seguridad a nivel de fila
- Comprobación de conocimiento
- Resumen

Configuración de auditoría para Azure SQL Database y SQL Managed Instance

Configure el registro de auditoría para Azure SQL Database y SQL Managed Instance para crear registros de cumplimiento resistentes a alteraciones. Configure grupos de acciones de auditoría, envíe los registros a Azure Monitor, Event Hubs y el almacenamiento de blobs inmutables, y configure la auditoría específica de SQL Managed Instance para cumplir los requisitos de auditoría de la normativa financiera.

- Introducción
- Describir las capacidades de auditoría de Azure SQL
- Configuración de destinos de auditoría para Azure SQL Database
- Configuración de la auditoría para SQL Managed Instance
- Diseño de una estrategia de auditoría compatible
- Comprobación de conocimiento
- Resumen

Implementación de Microsoft Defender para bases de datos

Active Microsoft Defender para Bases de Datos para detectar inyección de SQL, patrones de consulta anómalos y exposiciones a vulnerabilidades en los servicios de Azure SQL. Habilite la protección en el ámbito de la suscripción mediante Azure Policy, configure las líneas base de evaluación de vulnerabilidades y enrute las alertas de seguridad al equipo de operaciones de seguridad.

- Introducción
- Exploración de Microsoft Defender para funcionalidades de bases de datos
- Habilitar Defender para bases de datos de Azure SQL en el ámbito de la suscripción
- Habilitación de Defender para bases de datos relacionales de código abierto

- Configuración de la evaluación de vulnerabilidades
- Configuración del enrutamiento de alertas y validación de la cobertura
- Comprobación de conocimiento
- Resumen

Segmentar y aislar las cargas de trabajo de Azure mediante controles de seguridad de red

Segmente las cargas de trabajo de Azure para controlar el movimiento lateral y aplicar el acceso a la red de mínima necesidad mediante grupos de seguridad de red (NSG), grupos de seguridad de aplicaciones (ASG), Azure Virtual Network Manager y la verificación con Network Watcher.

- Introducción
- Evaluación de brechas de segmentación de red
- Control del tráfico con grupos de seguridad de red (NSG)
- Simplificación de la administración de reglas con grupos de seguridad de aplicaciones
- Aplicación de una directiva coherente con Azure Virtual Network Manager
- Comprobación de las reglas de seguridad de red eficaces con Network Watcher
- Comprobación de conocimiento
- Resumen

Centralización y aplicación de la inspección del tráfico mediante Azure Firewall

Implemente Azure Firewall para centralizar la inspección del tráfico y aplicar directivas de filtrado en el entorno de Azure. Azure Firewall incluye bloqueo basado en inteligencia de amenazas y la implementación de un concentrador virtual seguro para el tráfico hub-spoke y branch.

- Introducción
- Determinar cuándo se requiere la inspección centralizada del tráfico
- Configuración de reglas y directivas de Azure Firewall
- Protección de un centro de Virtual WAN con Azure Firewall
- Comprobación de conocimiento
- Resumen

Protección de la conectividad remota e híbrida mediante puertas de enlace de VPN y Acceso privado de Microsoft Entra

Refuerce la seguridad de Azure VPN Gateway e implemente Acceso privado de Microsoft Entra para reemplazar el acceso VPN amplio con acceso basado en identidades y por aplicación que aplica los principios de conectividad de Confianza cero.

- Introducción
- Evaluación de los riesgos de seguridad en la conectividad híbrida
- Reforzar la seguridad del gateway VPN
- Reemplazo del acceso VPN amplio por Acceso privado de Microsoft Entra
- Comprobación de conocimiento
- Resumen

Eliminar la exposición a la red pública de los servicios PaaS de Azure

Elimine la exposición de red pública de los servicios de PaaS e inteligencia artificial de Azure utilizando puntos de conexión privados y Azure Private Link, y aplique a continuación la adopción a escala mediante Azure Policy y Defender for Cloud.

- Introducción
- Evalúe el riesgo de exposición de los puntos de conexión PaaS públicos
- Configuración de puntos de conexión privados para eliminar la exposición pública de PaaS
- Exposición de servicios internos de forma segura mediante Azure Private Link servicio
- Aplicación y auditoría de la adopción de puntos de conexión privados
- Comprobación de conocimiento
- Resumen

Acceso seguro para la identidad del agente de Microsoft Entra

Aplique controles de acceso condicional a las identidades de los agentes de IA en Microsoft Entra Agent Identity. Asigne cómo los agentes se autentican, configuran directivas que aplican condiciones de acceso y administran el ciclo de vida de la identidad del agente para reducir el riesgo de agentes en peligro o con privilegios excesivos.

- Introducción
- Asignación de los flujos de autenticación y el ámbito del acceso condicional
- Configuración de directivas de acceso condicional para agentes
- Gestión del acceso y del ciclo de vida del agente
- Prueba de conocimientos
- Resumen

Analizar los riesgos de identidad de IA con Microsoft Defender XDR

Use Microsoft Defender XDR para detectar agentes de inteligencia artificial que operan en su entorno, evaluar el radio de explosión de cada identidad del agente y analizar rutas de acceso a ataques que podrían provocar acceso a recursos o datos no autorizados.

- Introducción
- Detección de agentes de IA en el portal de Microsoft Defender
- Evaluar el radio de explosión y los vectores de ataque
- Comprobación de conocimiento
- Resumen

Habilitación de la protección en tiempo real para agentes de Copilot Studio

Configure Microsoft Defender for Cloud Apps para proporcionar protección en tiempo de ejecución para agentes de Copilot Studio. Habilite la protección en la configuración del portal de Defender para la inteligencia artificial, colabore con los administradores de Power Platform para la configuración del identificador de aplicación y compruebe que los datos de búsqueda avanzada, alertas y inventario de agentes aparecen en Microsoft Defender XDR.

- Introducción
- Exploración de la protección del agente de IA de Copilot Studio
- Habilitación de la protección en Microsoft Defender
- Revisión de los resultados de protección del agente de IA
- Comprobación de conocimiento
- Resumen

Configuración de la seguridad de AI Gateway en Microsoft Foundry

Use AI Gateway en Microsoft Foundry para proteger y controlar el tráfico del modelo de IA. Examine la arquitectura de la puerta de enlace, cree y configure una instancia de puerta de enlace con controles de seguridad y aplique restricciones de acceso y supervisión para aplicar la directiva y detectar el uso indebido.

- Introducción
- Examen de la arquitectura de AI Gateway
- Creación y configuración de AI Gateway
- Protección y supervisión del acceso a AI Gateway
- Comprobación de conocimiento
- 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 cargas de trabajo de INTELIGENCIA ARTIFICIAL con Microsoft Defender para la nube

Microsoft Defender para la nube 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

Habilitación de la protección de cargas de trabajo de Defender para servicios de IA en Microsoft Defender para la nube

Habilite y configure el plan de Defender para servicios de IA en Microsoft Defender para la nube para detectar amenazas destinadas a cargas de trabajo de Servicios de Azure AI. A continuación, configure los componentes del plan y supervise la posición de seguridad de la inteligencia artificial mediante el panel seguridad de datos e inteligencia artificial.

- Introducción
- Habilitación y configuración del plan de Defender para servicios de IA
- Supervisión de la seguridad de la inteligencia artificial con el panel datos e inteligencia artificial
- Comprobación de conocimiento
- Resumen

Administración de agentes mediante Microsoft Agent 365

Use Microsoft Agent 365 para controlar los agentes de inteligencia artificial en el entorno de Microsoft 365. Habilite la interfaz de administración del Agente 365, registre agentes y aplique controles de acceso, y supervise la actividad y el uso del agente para aplicar las directivas de gobernanza de inteligencia artificial de su organización.

- Introducción
- Habilitar y navegar por Microsoft Agent 365
- Registro de agentes y aplicación de controles de acceso
- Supervisión de la actividad del agente y aplicación de la gobernanza
- Prueba de conocimientos
- Resumen

Identificación de los riesgos de los datos de inteligencia artificial mediante Administración de postura de seguridad de datos de Microsoft Purview

Use Administración de postura de seguridad de datos de Microsoft Purview para IA para detectar cómo fluyen los datos confidenciales a través de herramientas de inteligencia artificial, identificar contenido SharePoint sobreexpuesto y revisar los riesgos de interacción generados por las aplicaciones de inteligencia artificial y Copilot.

- Introducción
- Configuración de la administración de la posición de seguridad de datos (DSPM) para la inteligencia artificial
- Evaluar la sobreexposición de SharePoint
- Identificación de los riesgos en las interacciones de las aplicaciones de Copilot e IA
- Prueba de conocimientos
- Resumen

Implementación del cifrado de disco para máquinas virtuales de Azure

Seleccione y configure el enfoque de cifrado de disco adecuado para Azure máquinas virtuales. Compare las opciones de cifrado de disco administrado, configure el cifrado en el host con claves administradas por el cliente mediante conjuntos de cifrado de disco, aplique el cifrado de disco confidencial a máquinas virtuales confidenciales y aplique el cumplimiento del cifrado de disco mediante Azure Policy.

- Introducción
- Elija la opción de cifrado de disco adecuada para Azure máquinas virtuales.
- Configuración del cifrado en el host con claves administradas por el cliente
- Aplicación del cifrado de disco confidencial a máquinas virtuales confidenciales
- Comprobación de conocimiento
- Resumen

Configuración de características de seguridad de inicio de confianza para máquinas virtuales de Azure

Configurar las características de seguridad de Trusted Launch para máquinas virtuales de Azure. Habilite el arranque seguro, vTPM y la supervisión de integridad para protegerse contra malware de nivel de arranque y rootkits. Actualice las máquinas virtuales Gen1 y Gen2 existentes para que usen el tipo de seguridad Trusted Launch e imponga su adopción a escala mediante Azure Policy.

- Introducción
- Identificación de componentes de inicio seguro y tipos de seguridad de máquina virtual
- Habilitación del inicio seguro en máquinas virtuales de Gen2 nuevas y existentes
- Migración de máquinas virtuales gen1 y configuración de componentes de inicio seguro
- Impulsar la adopción de Trusted Launch con Azure Policy
- Comprobación de conocimiento
- Resumen

Planear e implementar Azure Bastion

Planee e implemente Azure Bastion para proporcionar acceso SSH y RDP seguro basado en explorador a máquinas virtuales sin exponer direcciones IP públicas ni puertos de administración. Seleccione la SKU adecuada en función de los requisitos de escala y características, implemente y configure Bastion

en una red virtual de Azure y conéctese a las máquinas virtuales mediante el portal y los métodos de cliente nativos.

- Introducción
- Planeamiento de la implementación de Azure Bastion
- Implementación y configuración de Azure Bastion
- Conexión a máquinas virtuales a través de Azure Bastion
- Comprobación de conocimiento
- Resumen

Administración de la seguridad de los servidores híbridos habilitados para Arc

Administrar controles de seguridad para servidores híbridos habilitados para Azure Arc. Configure la seguridad de RBAC y de las extensiones para evitar modificaciones no autorizadas del agente. A continuación, aplique Azure Policy para aplicar líneas base de seguridad en máquinas inscritas en Arc. Por último, supervise la posición de seguridad del servidor híbrido en Microsoft Defender para la nube.

- Introducción
- Control de acceso y seguridad de las extensiones para servidores habilitados para Arc
- Aplicación de Azure Policy a servidores habilitados para Arc
- Supervisión de la posición de seguridad del servidor de Arc en Defender for Cloud
- Comprobación de conocimiento
- Resumen

Implementación de Microsoft Defender para servidores

Incorpore las máquinas virtuales de Azure y los servidores híbridos conectados mediante Arc a Microsoft Defender for Servers. Seleccione el Plan 1 o el Plan 2 en función de los requisitos de capacidades y configure el análisis de vulnerabilidades sin agente y basado en agente mediante Administración de vulnerabilidades de Defender. A continuación, integre Microsoft Defender para punto de conexión y administre funcionalidades de análisis sin agente para el inventario de software, los secretos, la detección de malware y la supervisión de la integridad de los archivos.

- Introducción
- Incorporar servidores a Defender para servidores
- Configuración del examen de vulnerabilidades con Administración de vulnerabilidades de Defender
- Configuración de Defender para la integración de puntos de conexión, el examen sin agente y la supervisión de la integridad de los archivos
- Comprobación de conocimiento
- Resumen

Habilitar y forzar el acceso Just-In-Time a máquinas virtuales

Habilite y configure el acceso a máquinas virtuales Just-In-Time en Microsoft Defender para la nube para eliminar los puertos RDP y SSH abiertos permanentemente. Configure directivas de acceso por puerto, solicite acceso limitado a tiempo a las máquinas virtuales, audite la actividad de acceso y aplique la adopción jiT en todo el patrimonio de máquinas virtuales mediante Azure Policy.

- Introducción
- Examinar los requisitos de acceso justo a tiempo a máquinas virtuales y la elegibilidad de las máquinas virtuales.
- Habilitación y configuración de directivas de acceso JIT
- Solicitar acceso Just-In-Time (JIT) y auditar la actividad de acceso
- Comprobación de conocimiento
- Resumen

Aplicación de la configuración de seguridad de la máquina virtual con Azure Machine Configuration

Audite y aplique la configuración de seguridad del sistema operativo en Azure máquinas

virtuales y servidores habilitados para Arc mediante Azure Machine Configuration. Aplique directivas de línea de base de seguridad integradas Windows y Linux, configure los modos de auditoría y aplicación, y cree configuraciones de máquina personalizadas para requisitos de seguridad específicos de la organización.

- Introducción
- Explorar las funcionalidades y modos de extensión de configuración de máquinas de Azure
- Aplica las políticas de línea de base de seguridad integradas
- Creación y asignación de configuraciones de máquina personalizadas
- Comprobación de conocimiento
- Resumen

Detección de riesgos de contenedor mediante Microsoft Defender para contenedores

Detecte errores de configuración y riesgos en tiempo de ejecución en las cargas de trabajo de contenedor mediante Microsoft Defender para contenedores. Habilite y configure la Defender para el plan de contenedores y evalúe las vulnerabilidades de la imagen de contenedor en Azure Container Registry. A continuación, responda a las alertas de amenazas en tiempo de ejecución y las recomendaciones de posición de seguridad para los clústeres de Azure Kubernetes Service (AKS).

- Introducción
- Exploración de Microsoft Defender para contenedores
- Habilitación y configuración de Defender para contenedores
- Evaluación de vulnerabilidades de la imagen de contenedor
- Detección de amenazas en tiempo de ejecución de contenedor y configuraciones incorrectas
- Comprobación de conocimiento
- Resumen

Implementación de controles de seguridad para Azure Kubernetes Service

Implemente controles de seguridad para Azure Kubernetes Service. Configurar la integración con Microsoft Entra y RBAC de Kubernetes para la autenticación y autorización del servidor API, aplicar directivas de red y acceso privado al clúster. A continuación, aplique los estándares de identidad de las cargas de trabajo y de seguridad de los pods para reforzar las cargas de trabajo en contenedores en Azure Kubernetes Service (AKS).

- Introducción
- Control del acceso al clúster de AKS con Microsoft Entra ID y RBAC
- Protección del acceso a la red de AKS
- Implementación de identidad de carga de trabajo y administración de secretos para AKS
- Aplicar la seguridad de pods y contenedores
- Comprobación de conocimiento
- Resumen

Implementar controles de seguridad para Azure Container Registry, Container Instances y Container Apps

Implemente controles de seguridad en Azure Container Registry, Azure Container Instances y Azure Container Apps. Configure RBAC, puntos de conexión privados y confianza de contenido para ACR; aplique identidades administradas e integración de red virtual para Container Instances y aplique controles de entrada, identidades administradas y administración de secretos para entornos de Container Apps.

- Introducción
- Proteja Azure Container Registry
- Implementación de controles de seguridad para Azure Container Instances
- Implementación de controles de seguridad para Azure Container Apps
- Comprobación de conocimiento
- Resumen

Implementación de controles de seguridad para aplicaciones de función y aplicaciones lógicas de Azure

Implemente controles de seguridad para Azure aplicaciones de funciones y aplicaciones lógicas. Configure la autenticación y autorización, las identidades administradas, la integración de red virtual y los puntos de conexión privados para las aplicaciones de Function y aplique la identidad administrada, la seguridad del conector y el aislamiento de red para aplicaciones lógicas.

- Introducción
- Configuración de la autenticación y autorización para aplicaciones de funciones
- Protección del acceso a la red para aplicaciones de funciones
- Implementación de controles de seguridad para aplicaciones lógicas
- Comprobación de conocimiento
- Resumen

Implementar controles de seguridad para App de Azure Services y Web Application Firewall

Implemente controles de seguridad para App de Azure Services y Web Application Firewall. Configure la autenticación, las identidades administradas, la integración de red virtual y los puntos de conexión privados para App Service e implemente directivas de WAF en Azure Application Gateway para proteger las cargas de trabajo web en el perímetro de la red.

- Introducción
- Implementación de controles de seguridad para Azure App Service
- Configuración de directivas de Web Application Firewall
- Proteja App Service con Web Application Firewall
- Comprobación de conocimiento
- Resumen

Implementación de la seguridad de back-end de API mediante Azure API Management

Implemente directivas de seguridad para la protección de api de back-end mediante Azure API Management. Configure la administración de claves de suscripción, la validación de JSON Web Token (JWT) y las directivas de OAuth 2.0 y aplique el filtrado ip y la limitación de velocidad. A continuación, aplique la seguridad mutua de la capa de transporte (mTLS) para proteger las conexiones de API de back-end y configure AI Gateway para proteger y controlar los puntos de conexión del modelo de IA.

- Introducción
- Configuración de directivas de autenticación y autorización de API
- Implementación de la seguridad de red de API y protección contra amenazas
- Protección de las conexiones del backend de API Management
- Configuración de AI Gateway en API Management para Fundición de IA de Azure
- Comprobación de conocimiento
- Resumen

Conexión de entornos híbridos y multinube a Microsoft Defender for Cloud

En este módulo, conectará servidores locales, cuentas de AWS y proyectos de GCP a Microsoft Defender for Cloud para ampliar la cobertura de seguridad unificada para toda su infraestructura híbrida y multinube. Obtenga información sobre cómo la autenticación federada protege el acceso del conector sin almacenar credenciales de larga duración. A continuación, planee el ámbito de conector adecuado para cada tipo de entorno y configure conectores nativos para AWS y GCP. El módulo cubre tanto la extensión de cobertura CSPM (sin agente) como la CWPP (habilitada con Azure Arc), y cierra verificando que la postura unificada y la protección de carga de trabajo estén activas en todos los entornos conectados.

- Introducción
- Exploración del modelo de conectividad multinube de Defender for Cloud
- Planeamiento de una estrategia de conector para entornos híbridos y multinube
- Conexión de máquinas locales mediante Azure Arc
- Conexión de cuentas de AWS a Defender for Cloud
- Conexión de proyectos de GCP a Defender for Cloud
- Comprobación de la cobertura multinube y validación de la protección
- Comprobación de conocimiento
- Resumen

Identificación de los riesgos de seguridad mediante cloud Security Posture Management

En este módulo, usará Cloud Security Posture Management (CSPM) en Microsoft Defender for Cloud para identificar, priorizar y realizar un seguimiento de los riesgos de seguridad en entornos de Azure, incluidas las cargas de trabajo de inteligencia artificial generativas. Compare las funcionalidades fundamentales y del plan de Defender CSPM, interprete la puntuación de seguridad en la nube basada en riesgos, investigue rutas de acceso de ataque dirigidas a recursos de inteligencia artificial y de nube y ejecute consultas basadas en grafos en Cloud Security Explorer para detectar de forma proactiva riesgos ocultos.

- Introducción
- Explore los planes y la visibilidad de la postura de CSPM
- Análisis de recomendaciones de seguridad con priorización de riesgos
- Identificación de rutas de acceso de ataque y puntos de ahogamiento
- Búsqueda de riesgos con el Explorador de seguridad en la nube
- Comprobación de conocimiento
- Resumen

Detección de recursos y vulnerabilidades no protegidos mediante Microsoft Defender External Attack Surface Management

En este módulo, usará Microsoft Defender External Attack Surface Management (EASM) para detectar y proteger la superficie expuesta a ataques externos. Aprendes cómo el descubrimiento externo de Microsoft Defender External Attack Surface Management (EASM) complementa otras herramientas de Defender. EASM usa la detección recursiva para buscar recursos desconocidos accesibles desde Internet en toda la organización, analizar paneles para priorizar las vulnerabilidades y los riesgos de higiene de la seguridad e integrar los hallazgos de EASM con Defender CSPM para el análisis de rutas de acceso a ataques.

- Introducción
- Exploración de las características y funcionalidades de EASM
- Detección de recursos mediante la detección recursiva
- Analiza tu superficie de ataque con paneles de control
- Integración de EASM Insights con Defender for Cloud
- Comprobación de conocimiento
- Resumen

Evaluación del cumplimiento normativo en Defender for Cloud

En este módulo, usará Microsoft Defender for Cloud para evaluar la posición de cumplimiento de su organización con respecto a los marcos de seguridad. Explore el panel de cumplimiento normativo, investigue brechas de control, asigne estándares normativos y genere informes listos para auditoría que comuniquen el estado de cumplimiento a las partes interesadas.

- Introducción
- Descripción de los estándares y controles de cumplimiento en Defender for Cloud
- Navegación por el panel de cumplimiento normativo e investigación de brechas de control

- Asignación de estándares y comunicación de la posición de cumplimiento
- Comprobación de conocimiento
- Resumen

Habilitación y configuración de planes de protección de cargas de trabajo en Microsoft Defender for Cloud

Habilite los planes de Cloud Workload Protection Platform (CWPP) en Microsoft Defender for Cloud para defender servidores, almacenamiento, bases de datos y cargas de trabajo de inteligencia artificial frente a amenazas activas. Puede identificar el plan adecuado para cada tipo de carga de trabajo, incluidos Defender for AI Services y Defender para API, configurar opciones específicas del plan, como la distinción de nivel P1/P2 de Defender para servidores y el análisis de malware de Defender para almacenamiento, e implementar la protección en el ámbito de suscripción o grupo de administración. El módulo concluye comprobando la cobertura mediante el libro de cobertura.

- Introducción
- Descripción del catálogo de planes de CWPP de Defender for Cloud
- Habilitar los planes de protección de cargas de trabajo en Configuración del entorno
- Configuración de Defender para almacenamiento y Defender para bases de datos
- Implementación de planes a escala y comprobación de la cobertura
- Comprobación de conocimiento
- Resumen

Configuración de Microsoft Defender Vulnerability Management para máquinas virtuales de Azure

Configura Microsoft Defender Vulnerability Management para las máquinas virtuales de Azure seleccionando el método de escaneo adecuado para tu nivel de plan de Defender for Servers, habilitando la evaluación de vulnerabilidades en el ámbito de suscripción y máquina, y revisando los hallazgos en el portal Microsoft Defender. Aplique Defender para las funcionalidades premium del plan 2 de servidores(evaluación de líneas base de seguridad y bloqueo de aplicaciones vulnerables) para aplicar el cumplimiento continuo y reducir el riesgo de explotación.

- Introducción
- Exploración de la integración de Microsoft Defender Vulnerability Management (MDVM) con Defender para servidores
- Configuración del examen de vulnerabilidades para máquinas virtuales de Azure
- Revisión y administración de los resultados de vulnerabilidades
- Aplicación de las funcionalidades de MDVM premium del plan 2
- Comprobación de conocimiento
- 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

Administración de contenido en Microsoft Sentinel

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

- Introducción
- Uso de soluciones desde el centro de contenido
- Uso de repositorios para la implementación
- Evaluación del módulo
- 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 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

Conectar registros de Common Event Format 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

Implementación de reglas de automatización y cuadernos de estrategias en Microsoft Sentinel

Automatice la administración de incidentes en Microsoft Sentinel mediante reglas de automatización y cuadernos de estrategias de Logic Apps. Cree reglas de automatización para evaluar y enrutar incidentes, activar un

cuaderno de estrategias de respuesta precompilado desde el centro de contenido y crear un cuaderno de estrategias personalizado. El proceso implementa un flujo de trabajo automatizado de notificación y respuesta.

- Introducción
- Descripción de las opciones de automatización de Microsoft Sentinel
- Creación de reglas de automatización en Microsoft Sentinel
- Configurar y activar una guía de procedimientos de Content Hub
- Creación de un cuaderno de estrategias personalizado con Azure Logic Apps
- Comprobación de conocimiento
- Resumen

Administración del almacenamiento de datos y consulta de registros de auditoría en Microsoft Sentinel

Administre el almacenamiento de datos en Microsoft Sentinel mediante la creación de tablas de registro personalizadas, la configuración de niveles de retención y directivas de archivo y la integración de Auditoría de Microsoft Purview. Cree tablas para orígenes de datos no estándar, aplique niveles de retención de análisis y de archivo para cumplir los requisitos de cumplimiento y consulte los registros de auditoría de Purview en el portal de Microsoft Defender XDR.

- Introducción
- Creación de tablas de registro personalizadas en Microsoft Sentinel
- Implementación de la retención de datos en Microsoft Sentinel
- Conexión de Auditoría de Microsoft Purview a Microsoft Sentinel
- Consulta de registros de auditoría de Purview en Microsoft Defender XDR
- Comprobación de conocimiento
- 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

Configuración de áreas de trabajo para Microsoft Security Copilot

En este módulo, planifica y configura las áreas de trabajo de Security Copilot para la segmentación empresarial. Aprenderá a establecer la capacidad con unidades de cómputo de seguridad (SCU) y a seleccionar ubicaciones de almacenamiento de datos para cumplir con las normativas. Luego, asigne roles de área de trabajo, configure los complementos específicos del área de trabajo y las configuraciones del propietario, asigne áreas de trabajo para agentes integrados de Microsoft Security Copilot y monitoree el uso de capacidad.

- Introducción
- Planificar un despliegue del espacio de trabajo
- Creación de un área de trabajo de Security Copilot
- Configuración del acceso y la configuración del área de trabajo
- Asignación de áreas de trabajo para agentes integrados

- Supervisión y administración de la capacidad del área de trabajo
- Comprobación de conocimiento
- Resumen

Administración de complementos y agentes en Microsoft Security Copilot

En este módulo, configurará las opciones de gobernanza del complemento y administrará el ciclo de vida de seguridad agente de Copilot. Aprenderá cómo la configuración de los complementos a nivel de propietario determina quién puede agregar y publicar complementos personalizados. A continuación, explorar cómo restringir el acceso de complementos preinstalados a través de áreas de trabajo y cómo descubrir, configurar y administrar tanto agentes creados por Microsoft como agentes de los socios de Security Store.

- Introducción
- Configuración de los valores del complemento en Security Copilot
- Detección y configuración de agentes creados por Microsoft
- Adquisición y configuración de agentes asociados de Security Store
- Administración de agentes de Security Copilot
- Comprobación de conocimiento
- Resumen