The DevSecOps Company

Microsoft Partner

SC-5009

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

Información general.

Con este curso asegura soluciones de IA en la nube configurando cargas de trabajo de IA, aplicando protecciones nativas en la nube y reforzando los resultados de seguridad con controles de identidad. Aprende cómo se autentican las cargas de trabajo de IA, cómo se establecen los límites de confianza y cómo la postura de seguridad y la protección contra cargas de trabajo reducen el riesgo usando Microsoft Defender for Cloud y Microsoft Foundry. Amplía estas protecciones utilizando Microsoft Entra para diseñar y aplicar controles de identidad y acceso que expliquen y endurezcan las decisiones de seguridad anteriores. Resultados de aprendizaje:

- Aplicar la gestión de postura de seguridad y la protección de cargas de trabajo para servicios de IA usando Microsoft Defender for Cloud.
- Configura y protege los entornos Microsoft Foundry usando controles de seguridad nativos en la nube.
- Diseña y aplica controles de identidad y acceso para cargas de trabajo de IA usando Microsoft Entra.

Duración.

1 Día.

Perfil del público.

Este curso está dirigido a profesionales responsables de asegurar y operar cargas de trabajo de IA en la nube. El público incluye ingenieros de seguridad en la nube, ingenieros de plataformas y equipos de aplicaciones que trabajan con servicios de IA y que necesitan entender cómo se aplican la protección de cargas de trabajo, la postura de seguridad y los controles de identidad en entornos de IA. Se recomienda familiarizar con Azure, conceptos de seguridad nativos en la nube y principios básicos de identidad y acceso.

Examen.

Applied Skills Assessment.

Temario.

Ruta de aprendizaje: Protege las soluciones de Microsoft Foundry usando Microsoft Defender for Cloud.

A medida que las cargas de trabajo de IA se convierten en centrales en las operaciones empresariales, introducen nuevos retos de seguridad que las herramientas tradicionales en la nube no abordan completamente. En esta ruta de aprendizaje, aprendes a:

- Comprende los riesgos de carga de trabajo de IA y cómo Microsoft Defender para la Nube identifica y protege los activos de IA.
- Habilitar el plan de cargas de trabajo de IA y utilizar la Gestión de Postura de Seguridad en la Nube (CSPM) para descubrir y corregir configuraciones erróneas.
- Utiliza la Protección de Carga de Trabajo en la Nube (CWP) para detectar amenazas en tiempo de ejecución que se

dirigen a componentes de IA.
- Investiga alertas de seguridad de IA en Microsoft Defender XDR.
- Configurar y gestionar las barreras de seguridad en Microsoft Foundry para evitar comportamientos inseguros o que violen políticas del modelo.

Módulo 1: Entiende cómo Microsoft Defender para la Nube soporta la seguridad y la gobernanza de la IA en Azure.

Microsoft Defender for Cloud desempeña un papel central en la seguridad de las cargas de trabajo de IA en todo Azure. Descubre cómo Microsoft Defender para la Nube soporta la seguridad de la IA en Azure. Explora las capas de una carga de trabajo de IA, los riesgos únicos que los sistemas de IA introducen y las barreras de seguridad que protegen las entradas y salidas de los modelos. Descubre cómo Microsoft Purview, Microsoft Entra ID y Microsoft Foundry trabajan juntos para apoyar una estrategia unificada de seguridad y gobernanza.

- Introducción.
- Entender los servicios de IA en Azure.
- Comprender los riesgos de seguridad de la IA en Azure.
- Barreras de seguridad y protecciones de IA en Azure.
- Cómo las herramientas de seguridad y gobernanza de Azure soportan las cargas de trabajo de IA.

Módulo 2: Proteger cargas de trabajo de IA con Microsoft Defender for Cloud.

Microsoft Defender for Cloud ayuda a proteger cargas de trabajo de IA combinando descubrimiento, gestión de postura y protección en tiempo de ejecución en una sola plataforma. Aprenderás a habilitar el plan de cargas de trabajo de IA, revisar información 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 capacidades trabajan conjuntamente para identificar lagunas de configuración, detectar comportamientos sospechosos y proporcionar visibilidad de extremo a extremo en tus entornos de IA.

- Habilitar el plan de cargas de trabajo de IA.
- Revisa los conocimientos en el panel de seguridad de Datos e IA.
- Evalúa y mejora la postura de seguridad de la IA con Cloud Security Posture Management (CSPM).
- Detectar amenazas de IA en tiempo de ejecución con Protección de Carga de Trabajo en la Nube (CWP).
- Investiga alertas de seguridad de IA con pruebas inmediatas en Microsoft Defender XDR.

Módulo 3: Configurar y gestionar las barreras de seguridad en Microsoft Foundry.

Las barreras de seguridad de Microsoft Foundry ayudan a proteger las cargas de trabajo de IA aplicando controles de seguridad configurables que evalúan tanto las indicaciones como las respuestas. Aprenderás a entender los modelos de seguridad integrados, probar y refinar barreras de seguridad, crear listas de bloqueo, configurar filtros de contenido y validar que las protecciones funcionan como se pretende. Estas capacidades ayudan a las organizaciones a prevenir interacciones inseguras o que violan políticas, proteger datos sensibles y mantener la confianza en las aplicaciones asistidas por IA.

- Entiende las barreras de seguridad y la seguridad de contenidos de Microsoft.
- Entiende los controles de seguridad en Microsoft Foundry.
- Prueba barandillas integradas.
- Crea y gestiona listas de bloqueo en Microsoft Foundry.
- Configurar y aplicar barreras de seguridad en Microsoft Foundry.
- Elige y refina las barreras adecuadas para tus cargas de trabajo de IA.

Módulo 4: Entornos seguros de Microsoft Foundry.

Para proteger los entornos Microsoft Foundry se requieren protecciones en capas que controlen el acceso, salvaguarden las credenciales, aíslen la comunicación en red y mantengan la visibilidad entre los recursos conectados. El enfoque incluye definir los límites de acceso con Microsoft Entra ID y roles de proyecto, e integrar Key Vault para la gestión de secretos. También utiliza redes virtuales gestionadas, enlace privado y registro de diagnóstico para mantener la privacidad, visibilidad y cumplimiento. Estas prácticas crean entornos de IA seguros y rastreables que apoyan la colaboración sin comprometer la protección.

- Controla el acceso a Microsoft Foundry con Microsoft Entra ID.
- Gestionar el acceso dentro de los proyectos de Microsoft Foundry.
- Secure Microsoft Foundry secrets with Azure Key Vault (preview).
- Aislar redes con red virtual gestionada y enlace privado.
- Activar el registro de diagnóstico en Microsoft Foundry.

Ruta de aprendizaje: Infraestructura de identidad segura de IA con Microsoft Entra.

Aprende cómo proteger las identidades utilizadas por las cargas de trabajo de IA en Azure. Comprende la arquitectura de identidad de carga de trabajo, configura el acceso a los recursos de Azure, aplica políticas de Acceso Condicional e investiga el riesgo de identidad utilizando Microsoft Entra.

Módulo 5: Entender la arquitectura de identidad para cargas de trabajo de IA.

La arquitectura de identidad define quién puede desplegar, invocar y gestionar cargas de trabajo de IA en Azure. Microsoft Entra ID regula el acceso a través de planos de gestión y datos, los flujos de autenticación establecen los límites de confianza para los endpoints de IA y las decisiones sobre el alcance de roles determinan el radio de explosión. Los tipos de identidad, asignaciones de roles y límites de alcance moldean los resultados de seguridad de la IA mucho antes de que se apliquen los controles de aplicación.

- Identidad como capa de control para soluciones de IA.
- Acceso a planos de gestión y planos de datos en cargas de trabajo de IA.
- Flujos de autenticación para endpoints de IA en Microsoft Foundry.
- Identidades humanas y de carga de trabajo en cargas de trabajo de IA.
- Asignación de roles y alcance en entornos de IA.
- Configuraciones erróneas comunes de identidad en despliegues de IA.

Módulo 6: Implementar access management for Azure resources.

Explora cómo usar roles integrados en Azure, identidades gestionadas y la política RBAC para controlar el acceso a los recursos de Azure. La identidad es la clave para soluciones seguras.

- Assign Azure roles.
- Configurar roles personalizados en Azure.
- Crear y configurar identidades gestionadas.
- Access Azure resources with managed identities.
- Analyze Azure role permissions.
- Configurar las políticas RBAC de Azure Key Vault.
- Recuperar objetos de Azure Key Vault.

Módulo 7: Planificar, implementar y administrar el Acceso Condicional.

El Acceso Condicional proporciona una fina granularidad de control sobre qué usuarios e identidades pueden realizar actividades específicas, acceder a qué recursos y cómo garantizar la seguridad de los datos y sistemas, incluyendo las identidades de agentes de IA gestionadas mediante el ID de Agente Microsoft Entra.

- Incumplimientos de seguridad del plan.
- Políticas de Acceso Condicional de Planes.
- Implementar controles y asignaciones de políticas de acceso condicional.
- Probar y solucionar problemas de políticas de Acceso Condicional.
- Implementar controles de aplicación.
- Implementar la gestión de sesiones y la evaluación de acceso continuo.
- Agente de Optimización de Acceso Condicional Microsoft Entra.

Ejercicios:

- Trabajar con valores predeterminados de seguridad.
- Implementar políticas de acceso condicional roles y asignaciones.
- Configurar los controles de sesión de autenticación.

Módulo 8: Gestionar la protección de identidad de Microsoft Entra.

Proteger la identidad del usuario monitorizando su uso y los patrones de inicio de sesión garantiza una solución segura en la nube. Explora cómo diseñar e implementar la protección de identidad Microsoft Entra.

- Revisa los conceptos básicos de protección de identidad.
- Implementar y gestionar la política de riesgo de usuario.
- Política de riesgo de inicio de sesión que habilite el ejercicio.
- Política de registro de autenticación multifactor de Microsoft Entra.
- Monitorizar, investigar y remediar a usuarios con mayor riesgo.
- Implementar seguridad para las identidades de carga de trabajo.
- Explora Microsoft Defender para la identidad.
- Explora el Agente de Gestión de Riesgos de Identidad.