The DevSecOps Company

Microsoft Partner

SC-5002

Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Información general.

Este curso le guía en la protección de los servicios y cargas de trabajo de Azure mediante los controles de Microsoft Cloud Security Benchmark en Microsoft Defender for Cloud a través de Azure Portal.

Duración.

1 Día.

Examen.

Applied Skills Assessment.

Temario.

Módulo 1: Examinar los estándares de cumplimiento normativo de Defender para Cloud.

En este módulo, nos centraremos en el uso de Microsoft Defender for Cloud para simplificar el cumplimiento normativo mediante la identificación y resolución de incidencias que dificultan el cumplimiento de los estándares de cumplimiento y las certificaciones.

- Normas de cumplimiento normativo en Defender for Cloud.
- Microsoft Cloud Security Benchmark en Defender for Cloud.
- Mejora del cumplimiento normativo en Defender for Cloud.

Módulo 1: Habilitación de Defender for Cloud en una suscripción de Azure.

En este módulo, nos centraremos en habilitar Microsoft Defender for Cloud en su suscripción de Azure para mejorar la supervisión de la seguridad, la administración del cumplimiento y la protección contra amenazas para las aplicaciones basadas en la nube.

- Conexión de las suscripciones de Azure.

Ejercicio: Configuración de Microsoft Defender for Cloud para la protección mejorada.

Módulo 3: Filtrado del tráfico de red con un grupo de seguridad de red mediante Azure Portal.

En este módulo, nos centraremos en filtrar el tráfico de red mediante grupos de seguridad de red de Azure Portal. Aprenda a crear, configurar y aplicar grupos de seguridad de red para mejorar la seguridad de red.

- Grupo de recursos de Azure.
- Azure Virtual Network.
- Cómo filtran el tráfico de red los grupos de seguridad de red.
- Grupos de seguridad de aplicaciones.

Ejercicio: Creación de una infraestructura de red virtual.

Módulo 4: Creación de un área de trabajo de Log Analytics.

En este módulo, descubrirá cómo crear un área de trabajo de Log Analytics en Azure Portal para Microsoft Defender for Cloud, y así mejorar la recopilación de datos y el análisis de seguridad.

- Área de trabajo de Log Analytics.

Ejercicio: Creación de un área de trabajo de Log Analytics.

Módulo 5: Recopilación de datos de supervisión del sistema operativo invitado de Azure y máquinas virtuales híbridas mediante el agente de Azure Monitor.

Este módulo le guiará sobre cómo implementar y administrar el agente de Azure Monitor, configurar reglas de recopilación de datos e integrarlo con Microsoft Defender for Cloud para mejorar la seguridad.

- Implementación del agente de Azure Monitor.
- Recopilación de datos con el agente de Azure Monitor.
- Recopilación de datos de las cargas de trabajo con el agente de Log Analytics.
- Configuración del agente y el área de trabajo de Log Analytics.

Ejercicios:

- Creación y edición de reglas de recopilación de datos y asociaciones en Azure Monitor.
- Creación de una regla de recopilación de datos e Instalación del agente de Azure Monitor.

Módulo 6: Exploración del acceso JIT a la máquina virtual.

En este módulo, nos centraremos en el riesgo de puertos de administración abiertos en máquinas virtuales y cómo el acceso a máquinas virtuales JIT en Microsoft Defender for Cloud mitiga esta amenaza.

- Descripción del acceso a máquinas virtuales Just-In-Time.
- Habilitación del acceso Just-In-Time en máquinas virtuales.

Ejercicio: Habilitación del acceso Just-In-Time en máquinas virtuales.

Módulo 7: Configuración de las redes de Azure Key Vault.

En este módulo, aprenderá a configurar las opciones de red de Azure Key Vault mediante Azure Portal para garantizar un acceso seguro y controlado a los secretos almacenados.

- Conceptos básicos de Azure Key Vault.
- Procedimientos recomendados para Azure Key Vault.
- Seguridad de red de Azure Key Vault.
- Configuración de firewalls y redes virtuales de Azure Key Vault.
- Introducción a la eliminación temporal de Azure Key Vault.
- Puntos de conexión de servicio de red virtual para Azure Key Vault.

Ejercicios:

- Configuración de las opciones de red de Key Vault.
- Habilitación de la eliminación temporal en Azure Key Vault.

Módulo 8: Conexión a un servidor de Azure SQL mediante un punto de conexión privado de Azure a través de Azure Portal.

Este módulo le guiará en la conexión segura de un servidor de Azure SQL mediante un punto de conexión privado de Azure en Azure Portal, lo cual mejora la seguridad de la comunicación de datos.

- Punto de conexión privado de Azure.
- Azure Private Link.

Ejercicio: Conexión a un servidor de Azure SQL mediante un punto de conexión privado de Azure con Azure Portal.