TEMARIO DEL CURSO

Secure cloud resources with Microsoft security technologies (AZ-500)

25 horas

OBJETIVOS DEL CURSO

- Este curso tiene como objetivo principal proporcionar a los profesionales de seguridad las habilidades necesarias para:
- Implementar controles de seguridad en entornos Azure.
- Mantener la postura de seguridad de una organización en la nube.
- Identificar y remediar vulnerabilidades de seguridad en Azure.
- Asegurar la identidad y el acceso a los recursos de Azure.
- Proteger la plataforma Azure, incluyendo redes y hosts.
- Asegurar los datos y las aplicaciones desplegadas en Azure.
- Gestionar y operar las soluciones de seguridad en Azure.

A QUIÉN VA DIRIGIDO

- Este curso está dirigido a ingenieros de seguridad de Azure que planean realizar el examen de certificación asociado (AZ-500) o que realizan tareas de seguridad en su trabajo diario.
- Este curso también sería útil para un ingeniero que quiera especializarse en brindar seguridad para plataformas digitales basadas en Azure y desempeñar un papel integral en la protección de los datos de una organización.
- Nivel de experiencia
- Para aprovechar al máximo este curso, se recomienda tener la siguiente experiencia y conocimientos:
- Conocimiento de las mejores prácticas y requisitos de seguridad industrial (defensa en profundidad, acceso menos privilegiado, RBAC, MFA, responsabilidad compartida, confianza cero).
- Familiaridad con protocolos de seguridad (VPN, IPSec, SSL) y métodos de cifrado de datos/disco.
- Experiencia previa en la implementación de cargas de trabajo de Azure.
- Experiencia con sistemas operativos Windows y Linux.
- Experiencia con lenguajes de scripting (PowerShell y CLI pueden usarse en laboratorios).

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.

Administrar identidad y acceso

- Lecciones:
- Azure Active Directory
- Protección de identidad de Azure
- Gobernanza empresarial
- Administración de identidades privilegiadas de Azure AD
- Identidad híbrida
- Laboratorios:
- Control de acceso basado en roles
- Política de Azure
- Bloqueos del administrador de recursos
- MFA, acceso condicional y protección de identidad AAD
- Administración de identidades privilegiadas de Azure AD
- Implementar la sincronización de directorios

MÓDULO 02.

Implementar la protección de la plataforma

- Lecciones:
- Seguridad del perímetro
- Seguridad de la red
- Seguridad del host
- Seguridad del contenedor
- Laboratorios:
- Grupos de seguridad de red y grupos de seguridad de aplicaciones
- Azure Firewall
- Configuración y protección de ACR y AKS

MÓDULO 03.

Datos y aplicaciones seguros

- Lecciones:
- Azure Key Vault
- Seguridad de la aplicación
- Seguridad de almacenamiento
- Seguridad de la base de datos SQL
- Laboratorios:
- Key Vault (implementación de datos seguros al configurar Always Encrypted)
- Protección de la base de datos SQL de Azure
- Puntos de conexión de servicio y almacenamiento seguro

MÓDULO 04.

Gestionar operaciones de seguridad

- Lecciones:
- Azure Monitor
- Azure Security Center
- Azure Sentinel
- Laboratorios:
- Azure Monitor
- Azure Security Center
- Azure Sentinel