Microsoft Azure Security Technologies

AZ-500T00

Detalles del Curso

Audiencia(s):	Profesional de TI(s)
Tecnología:	Microsoft Azure
Duración:	32 Horas
Material Didáctico:	Oficial (Ingles)

Sobre este Curso

Este curso proporciona a los profesionales de seguridad de TI el conocimiento y las habilidades necesarias para implementar controles de seguridad, mantener la postura de seguridad de una organización e identificar y remediar las vulnerabilidades de seguridad. Este curso incluye seguridad para la identidad y el acceso, protección de la plataforma, datos y aplicaciones, y operaciones de seguridad.

Perfil de Audiencia

Este curso está dirigido a ingenieros de seguridad de Azure que planean realizar el examen de certificación asociado 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.

Contenido del Curso

Módulo 1: Administrar identidad y acceso

Este módulo cubre Azure Active Directory, Azure Identity Protection, Enterprise Governance, Azure AD PIM e Hybrid Identity.

Lecciones

- Azure Active Directory
- Protección de identidad de Azure
- Gobernanza empresarial
- Administración de identidades privilegiadas de Azure AD
- Identidad híbrida

Laboratorio: Control de acceso basado en roles
Laboratorio: Política de Azure
Laboratorio: Bloqueos del administrador de recursos
Laboratorio: MFA, acceso condicional y protección de identidad AAD
Laboratorio: Administración de identidades privilegiadas de Azure AD
Laboratorio: Implementar la sincronización de directorios

Módulo 2: Implementar la protección de la plataforma

Este módulo cubre la seguridad del perímetro, la red, el host y el contenedor.

Lecciones

- Seguridad del perímetro
- Seguridad de la red
- Seguridad del host
- Seguridad del contenedor

Laboratorio: Grupos de seguridad de red y grupos de seguridad de aplicaciones
Laboratorio: Azure Firewall
Laboratorio: Configuración y protección de ACR y AKS

Módulo 3: Datos y aplicaciones seguros

Este módulo cubre Azure Key Vault, seguridad de aplicaciones, seguridad de almacenamiento y seguridad de base de datos SQL.

Lecciones

- Azure Key Vault
- Seguridad de la aplicación

- Seguridad de almacenamiento
- Seguridad de la base de datos SQL

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

Módulo 4: Gestionar operaciones de seguridad

Este módulo cubre Azure Monitor, Azure Security Center y Azure Sentinel.

Lecciones

- Azure Monitor
- Azure Security Center
- Azure Sentinel

Laboratorio: Azure Monitor
Laboratorio: Azure Security Center
Laboratorio: Azure Sentinel

Al Finalizar este Curso

Después de completar este curso, los estudiantes podrán:

- Implementar estrategias de gobierno empresarial que incluyen control de acceso basado en roles, políticas de Azure y bloqueos de recursos.
- Implementar una infraestructura de Azure AD que incluya usuarios, grupos y autenticación multifactor.
- Implementar Azure AD Identity Protection, incluidas las políticas de riesgo, el acceso condicional y las revisiones de acceso.
- Implementar Azure AD Privileged Identity Management, incluidos los roles de Azure AD y los recursos de Azure.
- Implementar Azure AD Connect, incluidos los métodos de autenticación y la sincronización de directorios local.
- Implementar estrategias de seguridad perimetral, incluido Azure Firewall.
- Implementar estrategias de seguridad de red, incluidos grupos de seguridad de red y grupos de seguridad de aplicaciones.
- Implementar estrategias de seguridad del host, incluida la protección de terminales, la administración de acceso remoto, la administración de actualizaciones y el cifrado de disco.

- Implementar estrategias de seguridad de contenedores, incluidas Azure Container Instances, Azure Container Registry y Azure Kubernetes.
- Implementar Azure Key Vault, incluidos certificados, claves y secretos.
- Implementar estrategias de seguridad de aplicaciones, incluido el registro de aplicaciones, identidades administradas y puntos de conexión de servicio.
- Implementar estrategias de seguridad de almacenamiento, incluidas firmas de acceso compartido, políticas de retención de blobs y autenticación de Azure Files.
- Implementar estrategias de seguridad de bases de datos que incluyen autenticación, clasificación de datos, enmascaramiento dinámico de datos y siempre cifrado.
- Implementar Azure Monitor, incluidas fuentes conectadas, análisis de registros y alertas.
- Implementar Azure Security Center, incluidas políticas, recomendaciones y acceso justo a tiempo a la máquina virtual.
- Implementar Azure Sentinel, incluidos libros, incidentes y cuadernos de estrategias.