The DevSecOps Company

Microsoft Partner

AZ-500T00
Microsoft Azure Security Technologies

Información general.

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.

Duración.

4 Días.

Perfil del público.

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 proporcionar seguridad para plataformas digitales basadas en Azure y desempeñar un papel integral en la protección de los datos de una organización.

Examen.

AZ-500: Microsoft Azure Security Technologies.

Temario.

Ruta de aprendizaje: Administrar la identidad y el acceso.

Domine la administración de identidades y accesos en Microsoft Entra ID, proteja a los usuarios, grupos e identidades externas, implemente controles de autenticación y autorización, y administre el acceso y la seguridad de las aplicaciones.

Módulo 1: Administración de identidades en el identificador de Microsoft Entra.

Este módulo se centra en la administración eficaz de identidades y la mejora de la seguridad en Microsoft Entra ID, lo que garantiza que los usuarios, los grupos y las identidades externas estén protegidos contra las amenazas de seguridad y el acceso no autorizado.

- ¿Qué es el ID de Microsoft Entra?
- Proteger a los usuarios de Microsoft Entra.
- Creación de un nuevo usuario en el identificador de Microsoft Entra.
- Grupos seguros de Microsoft Entra.
- Recomendar cuándo usar identidades externas.
- Protección de identidades externas.
- Implementación de la protección de identidad de Microsoft Entra.

Módulo 2: Administración de la autenticación mediante el identificador de Microsoft Entra.

Este módulo está diseñado para proporcionar a los administradores el conocimiento y las habilidades necesarias para administrar la autenticación de forma eficaz mediante el identificador de Microsoft Entra, lo que garantiza un acceso seguro a los recursos y mejora la experiencia del usuario.

- Conexión de Microsoft Entra.
- Sincronización en la nube de Microsoft Entra.
- Opciones de autenticación.
- Sincronización de hash de contraseña con el identificador de Microsoft Entra.

- Autenticación de paso a través de Microsoft Entra.
- Federación con el identificador de Microsoft Entra.
- ¿Qué es la autenticación de Microsoft Entra?
- Implementación de la autenticación multifactor (MFA).
- Opciones de autenticación sin contraseña para el identificador de Microsoft Entra.
- Implementación de la autenticación sin contraseña.
- Implementación de la protección con contraseña.
- Inicio de sesión único de Microsoft Entra ID.
- Implementación del inicio de sesión único (SSO).
- Integre el inicio de sesión único (SSO) y los proveedores de identidad.
- Introducción a Microsoft Entra Verified ID.
- Configurar el identificador verificado de Microsoft Entra.
- Recomendar y aplicar protocolos de autenticación modernos.

Módulo 3: Administración de la autorización mediante el identificador de Microsoft Entra.

Este módulo está diseñado para proporcionar a los administradores el conocimiento y las habilidades necesarias para administrar eficazmente la autorización mediante Microsoft Entra ID, lo que garantiza que los usuarios tengan el acceso adecuado a los recursos y datos.

- Grupos de administración de Azure.
- Configuración de permisos de rol de Azure para grupos de administración, suscripciones, grupos de recursos y recursos.
- Control de acceso basado en rol de Azure.
- Roles integrados de Azure.
- Asignación de permisos de rol de Azure para grupos de administración, suscripciones, grupos de recursos y recursos.
- Roles integrados de Microsoft Entra.
- Asignación de roles integrados en el identificador de Microsoft Entra.
- Control de acceso basado en roles de Microsoft Entra.
- Creación y asignación de un rol personalizado en el identificador de Microsoft Entra.
- Administración de permisos de Microsoft Entra.
- Implementar y administrar la administración de permisos de Microsoft Entra.
- Seguridad Zero Trust.
- Administración de identidades privilegiadas de Microsoft Entra.
- Configurar Privileged Identity Management.
- Gobernanza de Microsoft Entra ID.
- Gestión de derechos.
- Acceder a las reseñas.
- Gestión del ciclo de vida de las identidades.
- Flujos de trabajo del ciclo de vida.
- Delegación y funciones en la gestión de derechos.
- Configuración de la administración de roles y las revisiones de acceso mediante la gobernanza de identificadores de Microsoft Entra.
- Implementación de directivas de acceso condicional.

Módulo 4: Administrar el acceso a las aplicaciones en el identificador de Microsoft Entra.

En este módulo se explica la administración del acceso a las aplicaciones en el identificador de Microsoft Entra, incluido el control del acceso a las aplicaciones empresariales, la administración de registros y permisos de aplicaciones, el uso de entidades de servicio y la configuración del proxy de aplicación de Microsoft Entra para el acceso seguro.

- Administrar el acceso a las aplicaciones empresariales en Microsoft Entra ID, incluidas las concesiones de permisos de OAuth.
- Administrar registros de aplicaciones en Microsoft Entra ID.
- Configurar ámbitos de permisos de registro de aplicaciones.
- Administrar el consentimiento de permisos de registro de aplicaciones.
- Administración y uso de entidades de servicio.
- Administración de identidades administradas para recursos de Azure.
- Recomendar cuándo usar y configurar un proxy de aplicación de Microsoft Entra, incluida la autenticación.

Ruta de aprendizaje: Redes seguras.

Domine la protección de las redes de Azure, incluidas las redes virtuales, el cifrado, la configuración de firewall, el acceso privado y la protección contra DDoS, con esta formación completa.

Módulo 5: Planeación e implementación de la seguridad de las redes virtuales.

Este módulo proporciona a los administradores los conocimientos y las habilidades necesarios para planear e implementar medidas

de seguridad sólidas para las redes virtuales de Azure, lo que garantiza la confidencialidad, integridad y disponibilidad de los recursos de red.

- ¿Qué es una red virtual de Azure?
- Planeación e implementación de grupos de seguridad de red (NSG) y grupos de seguridad de aplicaciones (ASG).
- Planificar e implementar rutas definidas por el usuario (UDR).
- Planeación e implementación de emparejamiento o puerta de enlace de red virtual.
- Planeación e implementación de una red de área amplia virtual, incluido el centro virtual seguro.
- Conectividad VPN segura, incluyendo punto a sitio y sitio a sitio.
- Azure ExpressRoute.
- Implementación del cifrado a través de ExpressRoute.
- Configuración de los ajustes de firewall en los recursos de PaaS.
- Supervisión de la seguridad de red mediante Network Watcher, incluidos los grupos de seguridad de red.

Módulo 6: Planeación e implementación de la seguridad para el acceso privado a los recursos de Azure.

Este módulo se centra en equipar a los administradores con el conocimiento y las habilidades necesarias para planear e implementar medidas de seguridad sólidas para el acceso privado a los recursos de Azure, proteger los datos confidenciales y mejorar la integridad de la red.

- Planeación e implementación de puntos de conexión de servicio de red virtual.
- Planeación e implementación de puntos de conexión privados.
- Planeación e implementación de servicios de Private Link.
- Planeación e implementación de la integración de red para Azure App Service y Azure Functions.
- Planeación e implementación de configuraciones de seguridad de red para un entorno del Servicio de aplicaciones (ASE).
- Planeación e implementación de configuraciones de seguridad de red para una instancia administrada de Azure SQL.

Módulo 7: Planeación e implementación de la seguridad para el acceso público a los recursos de Azure.

Este módulo permite a los administradores planear e implementar una seguridad sólida para los recursos de Azure, lo que garantiza la confidencialidad, la integridad y la disponibilidad de las aplicaciones y los servicios.

- Planeación e implementación de la seguridad de la capa de transporte (TLS) en aplicaciones, incluido Azure App Service y API Management.
- Planeación, implementación y administración de directivas de Azure Firewall, Azure Firewall Manager y firewall.
- Planeación e implementación de una instancia de Azure Application Gateway.
- Planificación e implementación de un firewall de aplicaciones web (WAF).
- Planeación e implementación de una instancia de Azure Front Door, incluida la red de entrega de contenido (CDN).
- Recomendar cuándo usar Azure DDoS Protection Standard.

Ruta de aprendizaje: Computación, almacenamiento y bases de datos seguras.

Domine el arte de proteger los recursos informáticos, el almacenamiento y las bases de datos de Azure, incluidas las medidas de seguridad avanzadas, el cifrado, el control de acceso y la protección de bases de datos.

Módulo 8: Planeación e implementación de seguridad avanzada para la informática.

Este módulo está diseñado para proporcionar a los administradores los conocimientos y las habilidades necesarios para planear e implementar medidas de seguridad avanzadas para los recursos de proceso de Azure, protegiendo las aplicaciones y los datos frente a las amenazas de seguridad en evolución.

- Planeación e implementación del acceso remoto a puntos de conexión públicos, Azure Bastion y acceso a máquinas virtuales (VM) Just-In-Time (JIT).
- ¿Qué es Azure Kubernetes Service?
- Configuración del aislamiento de red para Azure Kubernetes Service (AKS)
- Protección y supervisión de Azure Kubernetes Service.

- Configuración de la autenticación para Azure Kubernetes Service.
- Configuración de la seguridad para Azure Container Instances (ACI).
- Configuración de la seguridad para Azure Container Apps (ACA).
- Administración del acceso a Azure Container Registry (ACR).
- Configuración del cifrado de disco, Azure Disk Encryption (ADE), el cifrado como host y el cifrado de disco confidencial.
- Recomendar configuraciones de seguridad para Azure API Management.

Módulo 9: Planificación e implementación de la seguridad para el almacenamiento.

Este módulo está diseñado para proporcionar a los administradores los conocimientos y las habilidades necesarios para planear e implementar medidas de seguridad completas para los recursos de almacenamiento de Azure, salvaguardando la integridad, confidencialidad y disponibilidad de los datos.

- Almacenamiento de Azure.
- Configuración del control de acceso para cuentas de almacenamiento.
- Administración del ciclo de vida de las claves de acceso de la cuenta de almacenamiento.
- Seleccione y configure un método adecuado para el acceso a Azure Files.
- Seleccione y configure un método adecuado para el acceso a Azure Blobs.
- Seleccione y configure un método adecuado para el acceso a Azure Tables.
- Seleccione y configure un método adecuado para el acceso a las colas de Azure.
- Seleccione y configure los métodos adecuados para protegerse contra las amenazas de seguridad de los datos, incluida la eliminación temporal, las copias de seguridad, el control de versiones y el almacenamiento inmutable.
- Configurar Bring your own key (BYOK).
- Habilitación del doble cifrado en el nivel de infraestructura de Azure Storage.

Módulo 10: Planeación e implementación de la seguridad para Azure SQL Database y Azure SQL Managed Instance.

Este módulo está diseñado para dotar a los administradores de los conocimientos y las habilidades necesarios para planear e implementar medidas de seguridad sólidas para Azure SQL Database y Azure SQL Managed Instance, lo que garantiza la protección de datos y el cumplimiento normativo.

- Seguridad de Azure SQL Database y SQL Managed Instance.
- Habilitación de la autenticación de base de datos mediante el identificador de Microsoft Entra.
- Habilitación y supervisión de la auditoría de bases de datos.
- Identificación de casos de uso para el portal de gobernanza de Microsoft Purview.
- Implementación de la clasificación de datos de información confidencial mediante el portal de gobernanza de Microsoft Purview.
- Planeación e implementación de máscaras dinámicas.
- Implemente un cifrado de datos transparente.
- Se recomienda cuándo usar Azure SQL Database Always Encrypted.

Ruta de aprendizaje: Gestión de operaciones de seguridad.

Domine el arte de administrar operaciones de seguridad en Azure, desde la gobernanza y la creación de directivas hasta la seguridad de la infraestructura, la administración de claves, la posición de seguridad, la protección contra amenazas y la supervisión y automatización de seguridad avanzadas.

Módulo 11: Planear, implementar y administrar la gobernanza para la seguridad.

Este módulo se centra en permitir que los administradores planeen, implementen y administren de forma eficaz la gobernanza de seguridad en Azure, garantizando el cumplimiento de las directivas y los procedimientos recomendados de la organización.

- Gobernanza de Azure.
- Creación, asignación e interpretación de directivas e iniciativas de seguridad en Azure Policy.
- Configuración de las opciones de seguridad mediante Azure Blueprint.
- Despliegue de infraestructuras seguras mediante el uso de una zona de aterrizaje.

- Azure Key Vault.
- Seguridad de Azure Key Vault.
- Autenticación de Azure Key Vault.
- Creación y configuración de una instancia de Azure Key Vault.
- Se recomienda cuándo usar un módulo de seguridad de hardware (HSM) dedicado.
- Configuración del acceso a Key Vault, incluidas las directivas de acceso al almacén y el control de acceso basado en roles de Azure.
- Administrar certificados, secretos y claves.
- Configurar la rotación de teclas.
- Configurar la copia de seguridad y la recuperación de certificados, secretos y claves.

Módulo 12: Administración de la posición de seguridad mediante Microsoft Defender for Cloud.

Este módulo enseña a los administradores a administrar y mejorar la seguridad en la nube mediante Microsoft Defender for Cloud, centrándose en la identificación y corrección proactivas de riesgos.

- Implementación de Microsoft Defender for Cloud.
- Identificación y corrección de riesgos de seguridad mediante la puntuación de seguridad y el inventario de Microsoft Defender for Cloud.
- Evalúe el cumplimiento con respecto a los marcos de seguridad y Microsoft Defender for Cloud.
- Incorporación de estándares normativos y del sector a Microsoft Defender for Cloud.
- Adición de iniciativas personalizadas a Microsoft Defender for Cloud.
- Conexión de entornos de nube híbrida y multinube a Microsoft Defender for Cloud.
- Identificación y supervisión de recursos externos mediante la administración de la superficie expuesta a ataques externos de Microsoft Defender.

Módulo 13: Configuración y administración de la protección contra amenazas mediante Microsoft Defender for Cloud.

Este módulo se centra en las técnicas esenciales para configurar y administrar la protección contra amenazas exclusivamente con Microsoft Defender for Cloud, lo que permite a los especialistas en ciberseguridad reforzar la posición de seguridad de sus entornos en la nube.

- Habilitación de los servicios de protección de cargas de trabajo en Microsoft Defender for Cloud.
- Configuración de Microsoft Defender para servidores.
- Configuración de Microsoft Defender para Azure SQL Database.
- Seguridad de contenedores en Microsoft Defender.
- Factores de amenaza de Kubernetes gestionado.
- Arquitectura de Defender para contenedores.
- Configuración de los componentes de Microsoft Defender para contenedores.
- Evaluaciones de vulnerabilidades para Azure.
- Defender para almacenamiento.
- Examen de malware en Defender para almacenamiento.
- Detección de amenazas a datos confidenciales.
- Implementación de Microsoft Defender para almacenamiento.
- Habilitación de la configuración de la directiva integrada de Azure.
- Seguridad de Microsoft Defender for Cloud DevOps.
- Compatibilidad y requisitos previos de DevOps Security.
- Postura de seguridad del entorno de DevOps.
- Conexión del entorno de laboratorio de GitHub a Microsoft Defender for Cloud.
- Configuración de la acción de GitHub de Microsoft Security DevOps.
- Administración y respuesta a alertas de seguridad en Microsoft Defender for Cloud.
- Configuración de la automatización del flujo de trabajo mediante Microsoft Defender for Cloud.
- Evaluación de exámenes de vulnerabilidades de Microsoft Defender para Server.

Módulo 14: Configure y administre soluciones de automatización y monitoreo de seguridad.

En este módulo se enseña a configurar y administrar herramientas de seguridad con Azure Monitor y Microsoft Sentinel. Ayuda a las organizaciones a encontrar y tratar rápidamente los problemas de seguridad en su configuración en la nube.

- Supervisión de eventos de seguridad mediante Azure Monitor.
- Configuración de conectores de datos en Microsoft Sentinel.
- Creación y personalización de reglas de análisis en Microsoft Sentinel.
- Evaluación de alertas e incidentes de Microsoft Sentinel.
- Configuración de la automatización en Microsoft Sentinel.