MS-500T00 Microsoft 365 Security Administrator

Introducción

El Microsoft 365 Security Administrator colabora con el Microsoft 365 Enterprise Administrator, las partes interesadas de negocios y otros administradores de cargas de trabajo para planificar e implementar estrategias de seguridad y garantiza que las soluciones cumplan con las directivas y regulaciones de la organización.

Este rol asegura proactivamente los entornos empresariales de Microsoft 365. Las responsabilidades incluyen responder a amenazas, implementar, administrar y monitorear soluciones de seguridad y cumplimiento para el entorno de Microsoft 365. Responden a incidentes, investigaciones y aplicación de la gobernanza de datos

El administrador de seguridad de Microsoft 365 está familiarizado con las cargas de trabajo de Microsoft 365 y los entornos híbridos. Este rol tiene fuertes habilidades y experiencia con protección de identidad, protección de información, protección contra amenazas, gestión de seguridad y gobierno de datos.

Objetivos

- Administrar el acceso de usuarios y grupos en Microsoft 365.
- Explicar y administrar Azure Identity Protection.
- Planificar e implementar Azure AD Connect.
- Administrar identidades de usuario sincronizadas.
- Explicar y usar el acceso condicional.
- Describir los vectores de amenazas de ciberataques.
- Explicar soluciones de seguridad para Microsoft 365.
- Usar la puntuación segura de Microsoft para evaluar y mejorar su posición de seguridad.
- Configurar varios servicios avanzados de protección contra amenazas para Microsoft 365.
- Planear e implementar dispositivos móviles seguros.
- Implementar la gestión de derechos de información.
- Mensajes seguros en Office 365.
- Configurar directivas de prevención de pérdida de datos.
- Implementar y administrar Cloud App Security.
- Implementar la protección de información de Windows para dispositivos.
- Planificar e implementar un sistema de archivo y retención de datos.

- Crear y gestionar una investigación de descubrimiento electrónico.
- Gestionar solicitudes de sujetos de datos GDPR.
- Explicar y usar etiquetas de confidencialidad.

Temario

Módulo 1: Administración de usuarios y grupos

- Conceptos de administración de identidades y acceso
- Modelo de confianza cero
- Planeamiento de la solución de identidad y autenticación
- Roles y cuentas de usuario
- Administración de contraseñas

Módulo 2: Sincronización y protección de identidades

- Planeamiento de la sincronización de directorios
- Configuración y administración de identidades sincronizadas
- Azure AD Identity Protection

Módulo 3: Administración de identidades y acceso

- Administración de aplicaciones
- Identity Governance
- Administración del acceso al dispositivo
- Control de acceso basado en roles (RBAC)
- Soluciones de acceso externo
- Privileged Identity Management

Módulo 4: Seguridad en Microsoft 365

- Vectores de amenazas e infracciones de datos
- Estrategia y principios de seguridad
- Soluciones de seguridad de Microsoft
- Puntuación segura

Módulo 5: Protección contra amenazas

- Exchange Online Protection (EOP)
- Microsoft Defender para Office 365
- Administración de datos adjuntos seguros
- Administración de vínculos seguros
- Microsoft Defender for Identity
- Microsoft Defender para punto de conexión

Módulo 6: Administración de amenazas

- Panel de seguridad
- Investigación de amenazas y respuesta a ellas
- Azure Sentinel
- Advanced Threat Analytics

Módulo 7: Seguridad de la aplicación Microsoft Cloud

- Implementación de Cloud Application Security
- Uso de información de Cloud Application Security

Módulo 8: Movilidad

- Administración de aplicaciones móviles (MAM)
- Administración de dispositivos móviles (MDM)
- Implementación de servicios para dispositivos móviles
- Registro de dispositivos en la administración de dispositivos móviles

Módulo 9: Protección y gobernanza de la información

- Conceptos de la protección de la información
- Gobernanza y administración de registros
- Etiquetas de confidencialidad
- Archivo en Microsoft 365
- Retención en Microsoft 365
- Directivas de retención en el Centro de cumplimiento de Microsoft 365
- Archivo y retención en Exchange
- Administración de registros locales en SharePoint

Módulo 10: Rights Management y cifrado

- Information Rights Management (IRM)
- Extensión segura de correo multipropósito de Internet (S-MIME)
- Cifrado de mensajes de Office 365

Módulo 11: Prevención de pérdida de datos

- Aspectos básicos de la prevención de la pérdida de datos
- Crear una directiva DLP
- Personalización de una directiva DLP
- Creación de una directiva DLP para proteger documentos
- Consejos de directiva

Módulo 12: Administración del cumplimiento

- Centro de cumplimiento

Módulo 13: Administración de riesgos internos

- Riesgo interno
- Acceso con privilegios
- Barreras de información
- Construcción de muros éticos en Exchange Online

Módulo 14: Detección y respuesta

- Búsqueda de contenido
- Auditoría de las investigaciones del registro
- eDiscovery avanzado

Duración y Desarrollo

25 horas teórico-practicas
Del 10 al 14 de junio de 9 a 14 horas
Modalidad presencial-virtual