The DevSecOps Company

Microsoft Partner

SC-900T00
Microsoft Security, Compliance, and Identity Fundamentals

Información general.

Este curso proporciona conocimientos de nivel básico sobre los conceptos de seguridad, cumplimiento e identidad y las soluciones de Microsoft relacionadas basadas en la nube.

Duración.

1 Día.

Perfil del público.

El público de este curso busca familiarizarse con los aspectos básicos de la seguridad, el cumplimiento y la identidad (SCI) en los entornos basados en la nube y servicios de Microsoft relacionados. Esta curso va dirigido a aquellos que buscan familiarizarse con los fundamentos de seguridad, cumplimiento e identidad (SCI) a través de los servicios basados en cloud y relacionados con Microsoft 365. Antes de asistir a este curso, los estudiantes deben tener:

- Descripción general de los conceptos relativos a la informática en la nube y las redes.
- Conocimientos generales de TI o experiencia general trabajando en un entorno de TI.
- Descripción general de Microsoft Azure y Microsoft 365.

Examen.

SC-900: Microsoft Security, Compliance, and Identity Fundamentals.

Temario.

Ruta de aprendizaje: Descripción de los conceptos de seguridad, cumplimiento e identidad.

Obtén información sobre los conceptos básicos fundamentales para la seguridad, el cumplimiento y las soluciones de identidad, como la confianza cero, la residencia de datos, la responsabilidad compartida, el rol de los proveedores de identidades, etc.

Módulo 1: Descripción de conceptos de seguridad y cumplimiento.

Obtenga información sobre los conceptos comunes de seguridad y cumplimiento que son fundamentales para las soluciones de Microsoft. Entre estos temas, se incluyen los modelos de responsabilidad compartida y confianza cero, el cifrado, la residencia de datos y la soberanía de datos, etc.

- Descripción del modelo de responsabilidad compartida.
- Descripción de la defensa en profundidad.
- Descripción del modelo de Confianza cero.
- Descripción del cifrado y el código hash.
- Describir los conceptos de gobernanza, riesgo y cumplimiento (GRC).

Módulo 2: Descripción de los conceptos de identidad.

Conozca los conceptos clave de autenticación y autorización, y por qué la identidad es importante para proteger los recursos corporativos. También aprenderá sobre servicios relacionados con la identidad.

- Definición de autenticación y autorización.
- Definición de identidad como perímetro de seguridad principal.
- Descripción del rol del proveedor de identidades.

- Descripción del concepto de servicios de directorio y Active Directory.
- Descripción del concepto de federación.

Ruta de aprendizaje: Descripción de las capacidades de Microsoft Entra.

Microsoft Entra ID es la solución de administración de identidades y acceso basada en la nube de Microsoft. Obtenga más información sobre las entidades de seguridad y los servicios de Microsoft Entra, la autenticación segura y las funcionalidades para la administración del acceso, así como la gobernanza y la protección de la identidad.

Módulo 3: Describir la función y los tipos de identidad de identificador de Microsoft Entra.

Microsoft Entra ID es la solución de administración de identidades y acceso basada en la nube de Microsoft que conecta los usuarios a sus aplicaciones, dispositivos y datos. Aprenda las funciones y los tipos de identidad admitidos por Microsoft Entra ID.

- Describir Microsoft Entra ID.
- Describir tipos de identidades.
- Descripción de identidad híbrida.
- Describir identidades externas.

Módulo 4: Descripción de las funcionalidades de autenticación de Microsoft Entra ID.

Obtenga información sobre las funcionalidades de autenticación de Microsoft Entra ID, incluida la autenticación multifactor, y cómo mejoran la seguridad. También obtendrá información sobre el autoservicio de restablecimiento de contraseña (SSPR) y las funcionalidades de administración y protección de contraseñas.

- Descripción de los métodos de autenticación.
- Descripción de la autenticación multifactor.
- Descripción del autoservicio de restablecimiento de contraseña.
- Descripción de las funcionalidades de administración y protección de contraseñas.

Módulo 5: Describir las funcionalidades de administración de acceso de Microsoft Entra.

Una función clave de Microsoft Entra es administrar el acceso. Obtenga información acerca de la solución Microsoft Security Service Edge (SSE), el acceso condicional y cómo los roles de Microsoft Entra y el control de acceso basado en rol (RBAC) ayudan a las organizaciones a administrar el acceso.

- Descripción del acceso condicional.
- Descripción del Acceso global seguro en Microsoft Entra.
- Descripción de los roles y el control de acceso basado en roles (RBAC) de Microsoft Entra.

Módulo 6: Descripción de las funcionalidades de gobernanza y protección de identidades de Microsoft Entra.

Microsoft Entra proporciona funcionalidades de protección y gobernanza de identidades. Obtenga información sobre estas funcionalidades, sus casos de uso y sus ventajas.

- Descripción de la gobernanza de Microsoft Entra ID.
- Descripción de las revisiones de acceso.
- Descripción de la administración de derechos.
- Descripción de las funcionalidades de Privileged Identity Management.
- Descripción de la Protección de Microsoft Entra ID.
- Descripción de la Administración de permisos de Microsoft Entra.
- Descripción del id. verificado por Microsoft Entra.
- Descripción de la integración de Microsoft Entra con Microsoft Security Copilot.

Ruta de aprendizaje: Descripción de las funcionalidades de las soluciones de seguridad de Microsoft.

Obtenga más información sobre las funcionalidades de seguridad de Microsoft. Los temas tratados incluyen las funcionalidades de red y plataformas de Azure, la administración de seguridad de Azure y Sentinel. Obtendrá más información sobre la protección contra amenazas con Microsoft Defender XDR y la administración de la seguridad de Microsoft 365.

Módulo 7: Descripción de Seguridad de Microsoft Copilot.

Familiarícese con Microsoft Security Copilot. Conocerás la terminología básica, cómo Microsoft Security Copilot procesa las solicitudes, los elementos de una solicitud eficaz y cómo habilitar la solución.

- Familiarícese con Microsoft Security Copilot.
- Descripción de la terminología de Seguridad de Microsoft Copilot.
- Descripción de cómo Microsoft Security Copilot procesa solicitudes de avisos.
- Describir los elementos de un mensaje eficaz.
- Descripción de cómo habilitar Microsoft Security Copilot.

Módulo 8: Descripción de los servicios principales de seguridad de infraestructuras en Azure.

Obtenga información sobre las funcionalidades que admite Azure para proteger la red, las VM y los datos.

- Descripción de la protección contra DDoS de Azure.
- Descripción de Azure Firewall.
- Descripción de Web Application Firewall.
- Descripción de la segmentación de red en Azure.
- Descripción de los grupos de seguridad de red de Azure.
- Descripción de Azure Bastion y Azure Key Vault.

Módulo 9: Describir las funcionalidades de administración de seguridad de Azure.

Obtenga información sobre Microsoft Defender for Cloud y las capacidades que reúne para proteger la nube mediante la puntuación segura, las recomendaciones y las características mejoradas que proporcionan protección de cargas de trabajo en la nube.

- Descripción de Microsoft Defender for Cloud.
- Descripción de cómo las directivas de seguridad y las iniciativas mejoran la posición de seguridad en la nube.
- Descripción de la administración de la posición de seguridad en la nube.
- Descripción de la seguridad mejorada de Microsoft Defender for Cloud.
- Descripción de la administración de seguridad de DevOps.

Módulo 10: Descripción de las funcionalidades de seguridad de Microsoft Sentinel.

Obtenga información sobre Microsoft Azure Sentinel, una solución de administración de eventos de información de seguridad (SIEM) y respuesta automatizada de orquestación de seguridad (SOAR) que es escalable y nativa de la nube. En este módulo, también obtendrá información sobre Seguridad de Microsoft Copilot.

- Definición de los conceptos de SIEM y SOAR.
- Descripción de las funcionalidades de detección y mitigación de amenazas en Microsoft Sentinel.
- Descripción de la integración de Microsoft Sentinel con Microsoft Security Copilot.

Módulo 11: Descripción de la protección contra amenazas con Microsoft Defender XDR.

Protección contra amenazas cibernéticas con Microsoft Defender XDR en puntos de conexión, identidades, correo electrónico y aplicaciones.

- Descripción de los servicios de Microsoft Defender XDR.
- Describir Microsoft Defender for Office 365.
- Describir Microsoft Defender para punto de conexión.
- Descripción de Microsoft Defender for Cloud Apps.
- Describir Microsoft Defender for Identity.
- Descripción de Administración de vulnerabilidades de Microsoft Defender.
- Descripción de la inteligencia sobre amenazas de Microsoft Defender.
- Describir el portal de Microsoft Defender.
- Descripción de la integración de Copilot con Microsoft Defender XDR.

Ruta de aprendizaje: Describir las funcionalidades de Microsoft Priva y Microsoft Purview.

Obtenga información sobre las soluciones de cumplimiento de Microsoft. Entre los temas tratados se incluirán el portal de cumplimiento de Microsoft Purview, la protección de la información y gobernanza en Microsoft 365, así como soluciones de eDiscovery, auditoría y riesgo interno. También se incluyen las funcionalidades de gobernanza de recursos de Azure.

Módulo 12: Descripción del Portal de confianza de servicios y las funcionalidades de privacidad de Microsoft.

¡Microsoft se basa en la confianza! Aquí explorará el Portal de confianza de servicios para ver contenido sobre cómo brinda Microsoft nuestro compromiso de confianza. También obtendrá información sobre Microsoft Priva, una solución para ayudar a cumplir los objetivos de privacidad.

- Descripción de las ofertas del Portal de confianza de servicios.
- Describir los principios de privacidad de Microsoft.
- Descripción de Microsoft Priva.

Módulo 13: Descripción de las soluciones de seguridad de datos de Microsoft Purview.

Descripción de las soluciones de seguridad de datos de Microsoft Purview.

- Descripción de las funcionalidades de clasificación de datos de Microsoft Purview Information Protection.
- Descripción de las etiquetas y directivas de confidencialidad en Microsoft Purview Information Protection.
- Describir la prevención de pérdida de datos en Microsoft Purview.
- Descripción de la administración de riesgos internos en Microsoft Purview.
- Descripción de la protección adaptable en Microsoft Purview.

Módulo 14: Descripción de las soluciones de cumplimiento de datos de Microsoft Purview.

Obtenga información sobre cómo las soluciones de cumplimiento de datos de Microsoft Purview ayudan a las organizaciones a administrar los requisitos normativos y de riesgo.

- Descripción de la auditoría en Microsoft Purview.
- Descripción de eDiscovery.
- Descripción del Administrador de cumplimiento.
- Descripción del cumplimiento de comunicaciones.
- Descripción de la administración del ciclo de vida de los datos.
- Descripción de la administración de registros.

Módulo 15: Descripción de las soluciones de gobierno de datos de Microsoft Purview.

Obtenga información sobre las soluciones de gobierno de datos de Microsoft Purview que aprovechan la IA y las tecnologías modernas para garantizar la calidad, la seguridad y el cumplimiento de los datos, al tiempo que aceleran la creación de valor.

- Descripción de los conceptos y ventajas del gobierno de datos.
- Descripción del Catálogo de datos de Microsoft Purview.