SC-100T00: MICROSOFT CYBERSECURITY ARCHITECT

Objetivos Didácticos

- Diseñar una estrategia y arquitectura de Confianza cero.
- Evaluar estrategias técnicas de gobernanza, riesgo y cumplimiento (GRC) y estrategias de operaciones de seguridad.
- Diseñar la seguridad de una infraestructura.
- Diseñar una estrategia para datos y aplicaciones.

Audiencia

Los profesionales de TI deben tener experiencia y conocimientos avanzados en una amplia gama de áreas de ingeniería de seguridad, como la identidad y el acceso, la protección de plataformas, las operaciones de seguridad, la protección de datos y la protección de aplicaciones. También deben tener experiencia con implementaciones híbridas y en la nube.

Requisitos previos

- Experiencia avanzada y conocimientos sobre la identidad y el acceso, la protección de plataformas, las operaciones de seguridad, la protección de datos y la protección de aplicaciones.
- Experiencia en implementaciones híbridas y en la nube.

Metodología

Presencial, Aula Virtual

Duración

4 días

TEMARIO DEL CURSO

MÓDULO 1: CREACIÓN DE UNA ESTRATEGIA Y UNA ARQUITECTURA DE SEGURIDAD GENERAL

- Introducción
- Introducción a Confianza cero
- Desarrollo de puntos de integración en una arquitectura
- Desarrollar requisitos de seguridad basados en objetivos comerciales.
- Convertir los requisitos de seguridad en funciones técnicas
- Diseño de la seguridad para una estrategia de resistencia
- Diseñar una estrategia de seguridad para entornos híbridos y multiinquilino
- Diseño de estrategias técnicas y de gobernanza para el filtrado y la segmentación del tráfico
- Descripción de la seguridad de los protocolos

MÓDULO 2: DISEÑO DE UNA ESTRATEGIA DE OPERACIONES DE SEGURIDAD

- Introducción
- Descripción de los marcos de operaciones de seguridad, los procesos y los procedimientos
- Diseño de una estrategia de seguridad de registro y auditoría
- Desarrollo de operaciones de seguridad para entornos híbridos y multinube
- Diseño de una estrategia de Administración de eventos e información de seguridad (SIEM) y de orquestación, automatización y respuesta de seguridad (SOAR).
- Evaluación de flujos de trabajo de seguridad
- Revisión de las estrategias de seguridad para la administración de incidentes
- Evaluación de la estrategia de operaciones de seguridad para compartir inteligencia técnica sobre amenazas
- Supervisión de orígenes para obtener información sobre amenazas y mitigaciones

MÓDULO 3: DISEÑO DE UNA ESTRATEGIA DE SEGURIDAD DE IDENTIDAD

- Introducción
- Protección del acceso a los recursos en la nube
- Recomendación de un almacén de identidades para la seguridad
- Recomendación de estrategias de autenticación segura y autorización de seguridad
- Protección del acceso condicional
- Diseño de una estrategia para la asignación y la delegación de roles
- Definición de la gobernanza de identidades para las revisiones de acceso y la administración de derechos
- Diseño de una estrategia de seguridad para el acceso de roles con privilegios a la infraestructura
- Diseño de una estrategia de seguridad para actividades con privilegios
- Descripción de la seguridad de los protocolos

MÓDULO 4: EVALUACIÓN DE UNA ESTRATEGIA DE CUMPLIMIENTO NORMATIVO

- Introducción
- Interpretación de los requisitos de cumplimiento y su funcionalidad técnica
- Evaluar el cumplimiento de la infraestructura con Microsoft Defender for Cloud.
- Interpretar las puntuaciones de cumplimiento y recomendar acciones para resolver problemas o mejorar la seguridad.
- Diseño y validación de la implementación de Azure Policy
- Diseño conforme a los requisitos de residencia de los datos
- Conversión de los requisitos de privacidad en requisitos de las soluciones de seguridad

MÓDULO 5: EVALUACIÓN DE LA POSICIÓN DE SEGURIDAD Y RECOMENDACIÓN DE ESTRATEGIAS TÉCNICAS PARA ADMINISTRAR EL RIESGO

- Introducción
- Evaluación de las posiciones de seguridad mediante puntos de referencia
- Evaluación de las posiciones de seguridad mediante Microsoft Defender for Cloud
- Evaluación de las posiciones de seguridad mediante puntuaciones de seguridad
- Evaluación de la higiene de seguridad de las cargas de trabajo en la nube
- Diseño de la seguridad de una zona de aterrizaje de Azure
- Interpretación de la inteligencia sobre amenazas técnica y recomendación de mitigaciones de riesgos
- Recomendación de características o controles de seguridad para mitigar los riesgos identificados

MÓDULO 6: DESCRIPCIÓN DE LOS PROCEDIMIENTOS RECOMENDADOS PARA LA ARQUITECTURA Y CÓMO CAMBIAN CON LA NUBE

- Introducción
- Planeamiento e implementación de una estrategia de seguridad entre equipos
- Establecimiento de una estrategia y un proceso para la evolución proactiva y continua de una estrategia de seguridad
- Descripción de los protocolos de red y los procedimientos recomendados para la segmentación de la red y el filtrado del tráfico

MÓDULO 7: DISEÑO DE UNA ESTRATEGIA PARA PROTEGER LOS PUNTOS DE CONEXIÓN DE SERVIDOR Y DE CLIENTE

- Introducción
- Especificación de las líneas base de seguridad para los puntos de conexión de servidor y de cliente
- Especificar los requisitos de seguridad para servidores
- Especificar los requisitos de seguridad para dispositivos móviles y clientes
- Especificar los requisitos para proteger Active Directory Domain Services
- Diseño de una estrategia para administrar secretos, claves y certificados
- Diseño de una estrategia para el acceso remoto seguro
- Descripción de los marcos de operaciones de seguridad, los procesos y los procedimientos
- Procedimientos de análisis forense profundo por tipo de recurso

MÓDULO 8: DISEÑO DE UNA ESTRATEGIA PARA PROTEGER LOS SERVICIOS PAAS, IAAS Y SAAS

- Introducción
- Especificación de líneas base de seguridad para servicios PaaS
- Especificación de líneas base de seguridad para servicios IaaS
- Especificación de líneas base de seguridad para servicios SaaS
- Especificación de los requisitos de seguridad para cargas de trabajo de IoT
- Especificación de los requisitos de seguridad para cargas de trabajo de datos
- Especificación de los requisitos de seguridad para cargas de trabajo web
- Especificación de los requisitos de seguridad para cargas de trabajo de almacenamiento
- Especificación de los requisitos de seguridad para contenedores
- Especificación de los requisitos de seguridad para la orquestación de contenedores

MÓDULO 9: ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD PARA APLICACIONES

- Introducción
- Modelado de amenazas de aplicaciones
- Especificación de prioridades para mitigar las amenazas a las aplicaciones
- Especificación de un estándar de seguridad para la incorporación de una nueva aplicación
- Especificación de una estrategia de seguridad para aplicaciones y API

MÓDULO 10: DISEÑO DE UNA ESTRATEGIA PARA PROTEGER LOS DATOS

- Introducción
- Clasificación por orden de prioridad de la mitigación de amenazas a los datos
- Diseño de una estrategia para identificar y proteger datos confidenciales
- Especificación de un estándar de cifrado para los datos en reposo y en movimiento