The DevSecOps Company

Microsoft Partner

SC-100T00
Microsoft Cybersecurity Architect

Información general.

Se trata de un curso avanzado de nivel de experto. Aunque no es necesario asistir, se recomienda encarecidamente que los alumnos hayan aprobado otra certificación de nivel de técnico auxiliar en la cartera seguridad, cumplimiento e identidad (como AZ-500, SC-200 o SC-300) antes de asistir a esta clase. Este curso prepara a los alumnos con la experiencia para diseñar y evaluar estrategias de ciberseguridad en las siguientes áreas: Confianza cero; gobernanza, riesgo y cumplimiento (GRC), operaciones de seguridad (SecOps) y datos y aplicaciones. Los alumnos también aprenderán a diseñar soluciones siguiendo los principios de confianza cero y a especificar los requisitos de seguridad para la infraestructura en la nube en diferentes modelos de servicio (SaaS, PaaS, IaaS).

Duración.

4 Días.

Perfil del público.

Este curso es para ingenieros de seguridad en la nube con experiencia que han aprobado una certificación anterior en la cartera seguridad, cumplimiento e identidad. Concretamente, los alumnos 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. En su lugar, los alumnos principiantes deben realizar el curso SC-900.

Examen.

SC-100: Microsoft Cybersecurity Architect.

Temario.

Ruta de aprendizaje: Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades.

Aprenderá a usar procedimientos recomendados de seguridad críticos de Microsoft para mejorar la posición de seguridad de una organización, aplicar principios de Confianza Cero y minimizar el riesgo de ataques emergentes. Entre los marcos descritos se incluyen Cloud Adoption Framework (CAF), Well-Architected Framework (WAF) y Arquitectura de referencia de ciberseguridad de Microsoft (MCRA).

Módulo 1: Introducción a los marcos de procedimientos recomendados y la Confianza cero.

Conozca los procedimientos recomendados, cómo los arquitectos de ciberseguridad los usan y algunos marcos clave de procedimientos recomendados para las funcionalidades de ciberseguridad de Microsoft. También obtendrá información sobre el concepto de Confianza cero y cómo empezar a trabajar con la Confianza cero en una organización.

- Introducción a los procedimientos recomendados.
- Introducción a la Confianza cero.
- Iniciativas de Confianza cero.
- Pilares tecnológicos de la Confianza cero, parte 1.
- Pilares tecnológicos de la Confianza cero, parte 2.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

Módulo 2: Diseñar soluciones de seguridad que se alineen con Cloud Adoption Framework (CAF) y Well-Architected Framework (WAF).

Obtendrá información sobre Cloud Adoption Framework (CAF) y el Marco de buena arquitectura (WAF) y cómo puede usarlos para diseñar soluciones más seguras.

- Definición de una estrategia de seguridad.
- Introducción a Cloud Adoption Framework.
- Metodología de seguridad de Cloud Adoption Framework.
- Introducción a las zonas de aterrizaje de Azure.
- Diseño de la seguridad con zonas de aterrizaje de Azure.
- Introducción al Marco de buena arquitectura.
- Pilar de seguridad del Marco de buena arquitectura.

Módulo 3: Diseño de soluciones que se alineen con la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB).

Obtendrá información sobre la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB) y cómo puede utilizarlos para diseñar soluciones más seguras.

- Introducción a la Arquitectura de referencia de ciberseguridad de Microsoft y Cloud Security Benchmark.
- Diseñar soluciones con procedimientos recomendados para funcionalidades y controles.
- Diseño de soluciones con procedimientos recomendados para proteger contra ataques internos, externos y de cadena de suministro.

Módulo 4: Diseño de una estrategia de resistencia para ransomware y otros ataques en función de los procedimientos recomendados de seguridad de Microsoft.

Obtendrá información sobre ciberamenazas comunes, como el ransomware, y para qué tipos de patrones de ataque se debe preparar una organización.

- Patrones comunes de ciberamenazas y ataques.
- Compatibilidad con la resistencia empresarial.
- Diseñar soluciones para mitigar ataques de ransomware, incluida la priorización de BCDR y el acceso con privilegios.
- Diseño de soluciones para continuidad empresarial y recuperación ante desastres (BCDR), incluida la copia de seguridad y restauración seguras.
- Evaluación de soluciones para actualizaciones de seguridad.

Módulo 5: Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades (Caso práctico).

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de operaciones de seguridad, identidad y cumplimiento. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas de casos prácticos.
- Tutorial conceptual.
- Tutorial técnico.

Ruta de aprendizaje: Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento.

Aprenderá a diseñar soluciones para operaciones de seguridad (SecOps), administración de identidades y acceso, acceso con privilegios y cumplimiento normativo.

Módulo 6: Diseño de soluciones para el cumplimiento normativo.

Aprenderá a interpretar y traducir los requisitos normativos en soluciones técnicas. También aprenderá a usar las funcionalidades que se encuentran en Microsoft Purview, Microsoft Priva y Defender for Cloud para el cumplimiento.

- Introducción al cumplimiento normativo.
- Requisitos de cumplimiento en controles de seguridad.
- Diseño de una solución para abordar los requisitos de cumplimiento mediante Microsoft Purview.
- Abordar los requisitos de cumplimiento con Microsoft Priva.
- Abordar los requisitos de seguridad y cumplimiento con Azure Policy.
- Evaluación y validación de la alineación con estándares normativos y pruebas comparativas mediante Microsoft Defender for Cloud.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

Módulo 7: Diseño de soluciones para la administración de identidades y acceso.

Obtendrá información sobre varias estrategias para administrar identidades y el acceso a los recursos, incluidos escenarios híbridos y multinube, identidades externas y acceso condicional.

- Introducción a la administración de identidades y acceso.
- Diseño de estrategias de acceso en entornos de nube, híbridos y multinube (incluido Microsoft Entra ID).
- Diseño de una solución para identidades externas.
- Diseño de estrategias modernas de autenticación y autorización.
- Alineación del acceso condicional y la Confianza cero.
- Especificación de los requisitos para proteger Active Directory Domain Services (AD DS).
- Diseño de una solución para administrar secretos, claves y certificados.

Módulo 8: Diseño de soluciones para proteger el acceso con privilegios.

Aprenderá técnicas avanzadas para diseñar soluciones que administren el acceso con privilegios de forma eficaz.

- Introducción al acceso con privilegios.
- Modelo de acceso empresarial.
- Evalúe la seguridad y la gobernanza de las soluciones de Microsoft Entra ID.
- Diseño de una solución para proteger la administración de inquilinos.
- Diseño de una solución para estaciones de trabajo de acceso con privilegios y servicios bastión.
- Evaluación de una solución de administración de revisiones de acceso.
- Evaluación de la seguridad y gobernanza de Active Directory Domain Services (AD DS) local, incluida la resistencia a ataques comunes.

Módulo 9: Diseño de soluciones para operaciones de seguridad.

Aprenderá técnicas para diseñar funcionalidades de operaciones de seguridad, como el registro, la auditoría, la Administración de eventos e información de seguridad (SIEM), la Orquestación de la seguridad y la respuesta automatizada (SOAR) y los flujos de trabajo de seguridad.

- Introducción a las operaciones de seguridad (SecOps).
- Supervisión de diseño para admitir entornos híbridos y multinube.
- Diseño de registro y auditoría centralizados, incluida la auditoría de Microsoft Purview.
- Diseño de una solución de detección y respuesta que incluye la detección y respuesta extendidas (XDR) y la Administración de eventos e información de seguridad (SIEM).
- Diseñar una solución para la detección y respuesta que incluye la detección y respuesta extendidas (XDR) y la administración de eventos e información de seguridad (SIEM).
- Diseño de una solución para la Orquestación de seguridad, automatización y respuesta (SOAR).
- Diseñar y evaluar flujos de trabajo de seguridad, incluida la respuesta a incidentes, la búsqueda de amenazas y la administración de incidentes.
- Diseñar y evaluar la cobertura de detección de amenazas mediante matrices de MITRE ATT&CK, como Cloud, Enterprise, Mobile e ICS.

Módulo 10: Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento (Caso práctico).

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de operaciones de seguridad, identidad y cumplimiento. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas de casos prácticos.
- Tutorial conceptual.
- Tutorial técnico.

Ruta de aprendizaje: Diseño de soluciones de seguridad para aplicaciones y datos.

Obtenga información sobre cómo diseñar soluciones para proteger datos y aplicaciones, que incluyen: Microsoft 365, desarrollo de aplicaciones, carteras de aplicaciones existentes, detección y clasificación de datos con Microsoft Purview y seguridad de datos para cargas de trabajo de Azure.

KeD® es una marca registrada ante el Instituto Mexicano de la Propiedad Intelectual

Módulo 11: Diseñar soluciones para proteger Microsoft 365.

Aprenderá a diseñar soluciones de seguridad para Exchange, Sharepoint, OneDrive y Teams.

- Introducción a la seguridad para Exchange, Sharepoint, OneDrive y Teams.
- Evaluación de la posición de seguridad de las cargas de trabajo de productividad y colaboración mediante métricas.
- Diseño de una solución de Microsoft Defender XDR.
- Diseño de configuraciones y prácticas operativas para Microsoft 365.
- Evaluación de los controles de cumplimiento y seguridad de datos en los servicios de Microsoft Copilot para Microsoft 365.
- Evaluación de soluciones para proteger los datos en Microsoft 365 mediante Microsoft Purview.

Módulo 12: Diseño de soluciones para proteger aplicaciones.

Aprenderá a proteger las aplicaciones, las API y el proceso de desarrollo mediante técnicas como la administración de posiciones, el modelado de amenazas y el acceso seguro para las identidades de carga de trabajo.

- Introducción a la seguridad de las aplicaciones.
- Diseñar e implementar estándares para proteger el desarrollo de aplicaciones.
- Evaluación de la posición de seguridad de las carteras de aplicaciones existentes.
- Evaluación de amenazas de aplicaciones con modelado de amenazas.
- Diseño de la estrategia de ciclo de vida de seguridad para aplicaciones.
- Acceso seguro para identidades de carga de trabajo.
- Diseño de una solución para la administración y seguridad de API.
- Diseño de una solución para el acceso seguro a las aplicaciones.

Módulo 13: Diseño de soluciones para proteger los datos de una organización.

Obtenga información sobre cómo diseñar soluciones que protejan los datos de una organización mediante funcionalidades como Microsoft Purview, Defender para SQL y Defender para Storage.

- Introducción a la seguridad de los datos.
- Evaluación de soluciones para la detección y clasificación de datos.
- Evaluación de soluciones para el cifrado de datos en reposo y en tránsito, incluido Azure KeyVault y el cifrado de infraestructura.
- Diseño de la seguridad de datos para cargas de trabajo de Azure.
- Diseño de la seguridad para Azure Storage.
- Diseño de una solución de seguridad con Microsoft Defender para SQL y Microsoft Defender para Storage.

Módulo 14: Diseño de soluciones de seguridad para aplicaciones y datos (Caso práctico).

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de protección de aplicaciones y datos. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas del caso práctico.
- Tutorial conceptual.
- Tutorial técnico.

Ruta de aprendizaje: Diseño de soluciones de seguridad para infraestructura.

Aprenderá a diseñar soluciones para la seguridad de la infraestructura. Estas soluciones de infraestructura incluyen la especificación de requisitos para diferentes modelos en la nube, el diseño de soluciones para la administración de posturas en entornos híbridos y multinube y la protección de puntos de conexión.

Módulo 15: Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS.

Obtenga información sobre cómo analizar los requisitos de seguridad para diferentes ofertas en la nube (SaaS, PaaS e IaaS), cargas de trabajo de IoT, cargas de trabajo web y contenedores.

- Introducción a la seguridad de SaaS, PaaS e IaaS.
- Especificación de las líneas de base de seguridad para los servicios SaaS, PaaS e IaaS.

KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.

- Especificación de requisitos de seguridad para cargas de trabajo de IoT.
- Especificación de requisitos de seguridad para cargas de trabajo web.
- Especificar los requisitos de seguridad para contenedores y la orquestación de contenedores..
- Evaluación de la seguridad de los Servicios de IA.

Módulo 16: Diseño de soluciones para la administración de la posición de seguridad en entornos híbridos y multinube.

Aprenderá a diseñar soluciones de administración de la posición de seguridad que se integran en escenarios híbridos y multinube mediante las funcionalidades de Microsoft Defender for Cloud, Azure Arc y Microsoft Cloud Security Benchmark (MCSB).

- Introducción a la administración de la posición en entornos híbridos y multinube.
- Evaluación de la posición de seguridad mediante Microsoft Cloud Security Benchmark.
- Diseño de la administración de la posición integrada y la protección de la carga de trabajo.
- Evaluación de la posición de seguridad mediante Microsoft Defender for Cloud.
- Evaluación de la posición con la puntuación de seguridad de Microsoft Defender for Cloud.
- Diseño de las protecciones de las cargas de trabajo en la nube con Microsoft Defender for Cloud.
- Integración de entornos híbridos y multinube con Azure Arc.
- Diseño de una solución para administrar la superficie expuesta a ataques externos.
- Administración de posturas mediante rutas de ataque de administración de la exposición.

Módulo 17: Diseño de soluciones para proteger los puntos de conexión de cliente y servidor.

Aprenderá a analizar los requisitos de seguridad para distintos tipos de puntos de conexión, incluidos servidores, clientes, IoT, OT, dispositivos móviles y dispositivos insertados. Estos requisitos tienen en cuenta diferentes plataformas y sistemas operativos y establecerán estándares para la protección de puntos de conexión, el refuerzo de la seguridad y la configuración.

- Introducción a la seguridad de los puntos de conexión.
- Especificación de los requisitos de seguridad del servidor.
- Especificación de los requisitos para dispositivos móviles y clientes.
- Especificación de los requisitos de seguridad de Internet de las cosas (IoT) y los dispositivos insertados.
- Tecnología operativa segura (OT) y sistemas de control industrial (ICS) con Microsoft Defender para IoT.
- Especificación de líneas de base de seguridad para puntos de conexión de servidor y de cliente.
- Diseño de una solución para el acceso remoto seguro.
- Evaluación de las soluciones de Solución de contraseñas de administrador local (LAPS) de Windows.

Módulo 18: Diseño de soluciones para la seguridad de red.

Aprenderá a diseñar soluciones de red seguras mediante técnicas como la segmentación de la red, el filtrado del tráfico, la supervisión de la red y la administración de posiciones.

- Diseñar soluciones para la segmentación de la red.
- Diseño de soluciones para el filtrado del tráfico con grupos de seguridad de red.
- Soluciones de diseño para la administración de la posición de red.
- Diseño de soluciones para la supervisión de la red.
- Evaluación de soluciones que usan el acceso a Internet de Microsoft Entra.
- Evaluar soluciones que usan Acceso privado de Microsoft Entra.

Módulo 19: Diseño de soluciones de seguridad para la infraestructura (Caso práctico).

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de seguridad de la infraestructura. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Descripción del caso práctico.
- Respuestas de caso práctico.
- Tutorial conceptual.
- Tutorial técnico.