CompTIA Security+

Duración: 5 Días Código del Curso: G013 Version: SY0-701 Método de Impartición: Curso Cerrado (In-Company)

Temario:

El curso CompTIA Security+ está diseñado para ayudarle a preparar el examen SY0-701. El examen CompTIA Security+ certifica y valida el conocimiento necesarias para instalar y configurar sistemas para asegurar aplicaciones, redes y dispositivos; realizar análisis de amenazas y responder con técnicas de mitigación apropiadas; participar en actividades de mitigación de riesgos; y operar con una conciencia de las políticas, leyes y reglamentos aplicables.

Curso Cerrado (In-Company)

Debido a que nuestra formación es modular, nuestros responsables de formación e instructores pueden trabajar con usted y su equipo para detectar las necesidades formativas y adaptar un temario de forma rápida y rentable. Durante una formación cerrada, usted recibirá una formación de expertos en un curriculum adaptado a sus necesidades.

Dirigido a:

CompTIA Security+ está dirigido a profesionales de TI con funciones laborales como: Administrador de seguridadEspecialista en

Objetivos:

- **Este curso enseña a los participantes las siguientes habilidades:**
- Evaluar el posicionamiento de la seguridad de un entorno empresarial y recomendar e implementar soluciones de seguridad adecuadas.
- Supervisar y proteger los entornos híbridos, incluida la nube, los dispositivos móviles, el Internet de las cosas (IoT) y la tecnología operativa.
- Operar con conocimiento de las normativas y políticas aplicables, incluidos los principios de gobernanza, riesgo y cumplimiento.
- Identificar, analizar y responder a incidentes y eventos de seguridad

Prerequisitos:

Conocimientos de redes y administración de redes TCP/IP basadas en Windows y familiaridad con otros sistemas operativos, como OS X, Unix o Linux.

- G005 - CompTIA Network+

Exámenes y certificación

CompTIA Security+ es la primera certificación de ciberseguridad que un candidato debe obtener al comienzo de su carrera. Dota a los profesionales de ciberseguridad con las habilidades básicas de seguridad necesarias para proteger redes, detectar amenazas y proteger datos a través de preguntas basadas en el rendimiento, ayudándoles a iniciar una carrera de ciberseguridad y convertirse en un defensor de confianza de los entornos digitales.

- **Examen requerido**: SY0-701
- **Número de preguntas:** Máximo 90
- **Tipos de preguntas:** De opción múltiple y basadas en el rendimiento
- **Duración del examen:** 90 minutos
- **Experiencia recomendada:** Un mínimo de 2 años de experiencia en administración de TI centrada en la seguridad, experiencia práctica en seguridad técnica de la información y amplios conocimientos de los conceptos de seguridad.

Idiomas: Inglés, japonés, vietnamita, tailandés, portugués (Inglés, japonés, portugués y español)

Siguientes cursos recomendados:

- GK5867 - CompTIA CySA+ Cybersecurity Analyst
- G015 - CompTIA PenTest+ Certification Prep Course
- GK2951 - CompTIA SecurityX Certification Prep Course

Contenido:

Conceptos generales de seguridad 12%

- Comparar y contrastar varios tipos de controles de seguridad.
- Resumir los conceptos fundamentales de seguridad.
- Explicar la importancia de los procesos de gestión de cambios y su impacto en la seguridad.
- Explicar la importancia de utilizar soluciones criptográficas adecuadas.

Amenazas, vulnerabilidades y mitigación 22%

- Comparar y contrastar actores y motivaciones de amenazas comunes.
- Explicar los vectores de amenaza y las superficies de ataque más comunes.
- Explicar varios tipos de vulnerabilidades.
- Dado un escenario, analizar los indicadores de actividad maliciosa.
- Explicar la finalidad de las técnicas de mitigación utilizadas para proteger la empresa.

Arquitectura de seguridad 18%

- Comparar y contrastar las implicaciones de seguridad de diferentes modelos de arquitectura.
- A partir de un escenario, aplicar los principios de seguridad para proteger la infraestructura de la empresa.
- Comparar y contrastar conceptos y estrategias para proteger los datos.
- Explicar la importancia de la resistencia y la recuperación en la arquitectura de seguridad.

Operaciones de seguridad 28%

- Dado un escenario, aplicar técnicas de seguridad comunes a los recursos informáticos.
- Explicar las implicaciones para la seguridad de una gestión adecuada de los activos de hardware, software y datos.
- Explicar varias actividades asociadas con la gestión de vulnerabilidades.
- Explicar conceptos y herramientas de alerta y supervisión de la seguridad.
- A partir de un escenario, modificar las capacidades de la empresa para mejorar la seguridad.
- Dado un escenario, implementar y mantener la gestión de identidades y accesos.
- Explicar la importancia de la automatización y la orquestación en relación con las operaciones seguras.
- Explicar las actividades adecuadas de respuesta a incidentes.
- Dado un escenario, utilizar fuentes de datos para apoyar una investigación.

Gestión y supervisión de programas de seguridad 20%.

- Resumir los elementos de una gobernanza eficaz de la seguridad.
- Explicar los elementos del proceso de gestión de riesgos.
- Explicar los procesos asociados a la evaluación y gestión de riesgos de terceros.
- Resumir los elementos de un cumplimiento eficaz de la seguridad.
- Explicar los tipos y objetivos de las auditorías y evaluaciones.
- A partir de una situación hipotética, aplicar prácticas de concienciación en materia de seguridad.

Información Adicional:

Acreditado por ANSI para demostrar el cumplimiento de la norma ISO 17024.

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid