CompTIA Security+

Código: COM-103

Propuesta de Valor: COMPTIA

Duración: 40 Horas

CompTIA Security+ es la certificación confiable a nivel mundial para validar los conocimientos y habilidades de seguridad de TI fundamentales y neutrales de los proveedores.
Como un punto de referencia para las mejores prácticas en seguridad de TI, esta certificación cubre los principios esenciales para la seguridad de la red y la gestión de riesgos, lo que la convierte en un trampolín importante de una carrera en seguridad de TI.

AUDIENCIA

Candidatos para CompTIA Security+:

- Especialista / Administrador de seguridad.
- Consultor de seguridad.
- Administrador de seguridad o sistemas.
- Administrador de red.

PRE REQUISITOS

- Se recomienda que el participante haya cursado CompTIA Network+ y dos años de experiencia en administración de TI con un enfoque de seguridad.

OBJETIVOS

- Amenazas, ataques y vulnerabilidades.
- Tecnologías y herramientas.
- Arquitectura y diseño.
- Gestión de identidad y acceso.
- Gestión de riesgos.
- Criptografía y PKI.

CERTIFICACIÓN DISPONIBLE

- El curso lo prepara para la certificación : **CompTIA Security+ SY0-701**

CONTENIDO

1. RESUMIR LOS CONCEPTOS FUNDAMENTALES DE SEGURIDAD

1.1. CONCEPTOS DE SEGURIDAD
1.2. CONTROLES DE SEGURIDAD

2. COMPARAR TIPOS DE AMENAZAS

2.1. ACTORES DE AMENAZAS
2.2. SUPERFICIES DE ATAQUE
2.3. INGENIERÍA SOCIAL

3. EXPLICAR LAS SOLUCIONES CRIPTOGRÁFICAS

3.1. ALGORITMOS CRIPTOGRÁFICOS
3.2. INFRAESTRUCTURA DE CLAVE PÚBLICA
3.3. SOLUCIONES CRIPTOGRÁFICAS

4. IMPLEMENTAR LA GESTIÓN DE IDENTIDADES Y ACCESOS

4.1. AUTENTICACIÓN
4.2. AUTORIZACIÓN
4.3. GESTIÓN DE IDENTIDAD

5. ARQUITECTURA DE RED EMPRESARIAL SEGURA

5.1. ARQUITECTURA DE RED EMPRESARIAL
5.2. DISPOSITIVOS DE SEGURIDAD DE RED
5.3. COMUNICACIONES SEGURAS

6. ARQUITECTURA DE RED SEGURA EN LA NUBE

6.1. INFRAESTRUCTURA DE LA NUBE
6.2. SISTEMAS INTEGRADOS Y ARQUITECTURA DE CONFIANZA CERO

7. EXPLICAR LOS CONCEPTOS DE RESILIENCIA Y SEGURIDAD DEL SITIO

7.1. GESTIÓN DE ACTIVOS
7.2. ESTRATEGIAS DE REDUNDANCIA
7.3. SEGURIDAD FÍSICA

8. EXPLICAR LA GESTIÓN DE VULNERABILIDADES

8.1. VULNERABILIDADES DEL DISPOSITIVO Y DEL SISTEMA OPERATIVO
8.2. VULNERABILIDADES DE APLICACIONES Y NUBE
8.3. MÉTODOS DE IDENTIFICACIÓN DE VULNERABILIDADES
8.4. ANÁLISIS Y CORRECCIÓN DE VULNERABILIDADES
8.5. EVALUAR LAS CAPACIDADES DE SEGURIDAD DE LA RED

9. EVALUAR LAS CAPACIDADES DE SEGURIDAD DE LA RED

9.1. LÍNEAS BASE DE SEGURIDAD DE LA RED
9.2. MEJORA DE LA CAPACIDAD DE SEGURIDAD DE LA RED

10. EVALUAR LAS CAPACIDADES DE SEGURIDAD DE LOS ENDPOINTS

10.1. IMPLEMENTAR SEGURIDAD DE TERMINALES
10.2. ENDURECIMIENTO DE DISPOSITIVOS MÓVILES

11. MEJORAR LAS CAPACIDADES DE SEGURIDAD DE LAS APLICACIONES

11.1. LÍNEAS BASE DE SEGURIDAD DEL PROTOCOLO DE APLICACIONES
11.2. CONCEPTOS DE SEGURIDAD DE APLICACIONES WEB Y EN LA NUBE

12. EXPLICAR LOS CONCEPTOS DE MONITOREO Y RESPUESTA A INCIDENTES

12.1. RESPUESTA A INCIDENTES
12.2. ANÁLISIS FORENSE DIGITAL
12.3. FUENTES DE DATOS
12.4. HERRAMIENTAS DE ALERTA Y MONITOREO

13. ANALIZAR INDICADORES DE ACTIVIDAD MALICIOSA

13.1. INDICADORES DE ATAQUES DE MALWARE
13.2. INDICADORES DE ATAQUES FÍSICOS Y DE RED
13.3. INDICADORES DE ATAQUES A APLICACIONES

14. RESUMIR LOS CONCEPTOS DE GOBERNANZA DE LA SEGURIDAD

14.1. POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS
14.2. GESTIÓN DEL CAMBIO
14.3. AUTOMATIZACIÓN Y ORQUESTACIÓN

15. EXPLICAR LOS PROCESOS DE GESTIÓN DE RIESGOS

15.1. PROCESOS Y CONCEPTOS DE GESTIÓN DE RIESGOS

15.2. CONCEPTOS DE GESTIÓN DE PROVEEDORES

15.3. AUDITORÍAS Y EVALUACIONES

16. RESUMIR LOS CONCEPTOS DE CUMPLIMIENTO Y PROTECCIÓN DE DATOS

16.1. CLASIFICACIÓN Y CUMPLIMIENTO DE DATOS

16.2. POLÍTICAS DE PERSONAL

BENEFICIOS

- Al concluir el curso el estudiante será capaz de detectar amenazas, ataques, vulnerabilidades y lograr combatirlas con eficiencia.