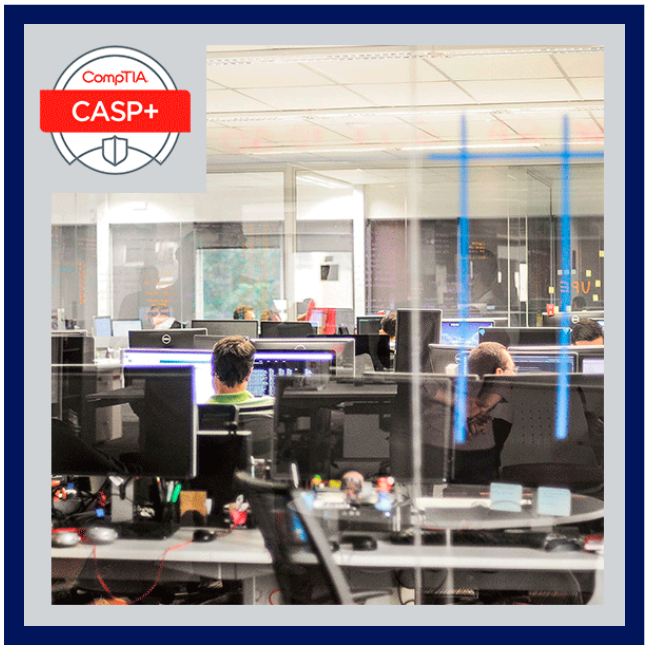
CompTIA Advanced Security Practitioner (CASP+)

Código: COM-120

Propuesta de Valor: COMPTIA

Duración: 40 Horas



El panorama actual de seguridad cibernética requiere habilidades especializadas para solucionar problemas y crear soluciones sólidas. Debe ser combatido con experiencia y habilidades de seguridad a nivel de maestro. Como profesional de TI certificado por CASP, demostrará que puede proporcionar las mejores soluciones y protección de ciberseguridad para organizaciones de todo el mundo.

AUDIENCIA

- CompTIA CASP+ Advanced Security Practitioner está dirigida a profesionales de la seguridad con un mínimo de diez años de experiencia en administración de TI, que incluyen al menos cinco años de experiencia práctica en seguridad técnica.

PRE REQUISITOS

- Aunque no hay prerrequisitos, la certificación CASP ha sido diseñada para seguir a CompTIA Security+ o su equivalente en experiencia.

OBJETIVOS

- CompTIA Security+ certificará que el candidato seleccionado posee los conocimientos y habilidades necesarias para instalar y configurar sistemas para proteger 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 conocimiento de las políticas, leyes y regulaciones aplicables. El candidato seleccionado realizará estas tareas para respaldar los principios de confidencialidad, integridad y disponibilidad.

CERTIFICACIÓN DISPONIBLE

- El curso lo prepara para la certificación: **CASP+ CAS-004**.

CONTENIDO

1. APOYO AL GOBIERNO DE TI Y LA GESTIÓN DE RIESGOS

1.1. IDENTIFICAR LA IMPORTANCIA DEL GOBIERNO DE TI Y LA GESTIÓN DE RIESGOS
1.2. EVALUAR EL RIESGO
1.3. MITIGAR EL RIESGO
1.4. INTEGRAR LA DOCUMENTACIÓN EN LA GESTIÓN DE RIESGOS

2. APROVECHAR LA COLABORACIÓN PARA RESPALDAR LA SEGURIDAD

2.1. FACILITAR LA COLABORACIÓN ENTRE LAS UNIDADES DE NEGOCIO
2.2. COMUNICACIONES SEGURAS Y SOLUCIONES DE COLABORACIÓN

3. USO DE LA INVESTIGACIÓN Y EL ANÁLISIS PARA PROTEGER LA EMPRESA

3.1. DETERMINAR LAS TENDENCIAS DE LA INDUSTRIA Y SUS EFECTOS EN LA EMPRESA
3.2. ANALIZAR ESCENARIOS PARA PROTEGER LA EMPRESA

4. INTEGRACIÓN DE LA AUTENTICACIÓN AVANZADA Y TÉCNICAS DE AUTORIZACIÓN

4.1. IMPLEMENTAR TECNOLOGÍAS DE AUTENTICACIÓN Y AUTORIZACIÓN
4.2. IMPLEMENTAR LA GESTIÓN AVANZADA DE IDENTIDADES Y ACCESOS

5. IMPLEMENTACIÓN DE TÉCNICAS CRIPTOGRÁFICAS

5.1. SELECCIONAR TÉCNICAS CRIPTOGRÁFICAS
5.2. IMPLEMENTAR LA CRIPTOGRAFÍA

6. IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD PARA HOSTS

6.1. SELECCIONAR HARDWARE Y SOFTWARE DE HOST
6.2. HOSTS REFORZADOS

6.3. VIRTUALIZAR SERVIDORES Y ESCRITORIOS
6.4. PROTEGER LOS CARGADORES DE BOTAS

7. IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD PARA DISPOSITIVOS MÓVILES

7.1. IMPLEMENTAR LA ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES
7.2. ABORDAR LAS INQUIETUDES DE SEGURIDAD Y PRIVACIDAD DE LOS DISPOSITIVOS MÓVILES

8. IMPLEMENTACIÓN DE LA SEGURIDAD DE LA RED

8.1. PLANIFICACIÓN DE LA IMPLEMENTACIÓN DE DISPOSITIVOS Y COMPONENTES DE SEGURIDAD DE RED
8.2. PLANIFICACIÓN DE LA IMPLEMENTACIÓN DE DISPOSITIVOS HABILITADOS PARA RED
8.3. IMPLEMENTAR UN DISEÑO DE RED AVANZADO
8.4. IMPLEMENTAR CONTROLES DE SEGURIDAD DE RED

9. IMPLEMENTACIÓN DE LA SEGURIDAD EN EL CICLO DE VIDA DEL DESARROLLO DE SOFTWARE Y SISTEMAS

9.1. IMPLEMENTAR LA SEGURIDAD A LO LARGO DEL CICLO DE VIDA DE LA TECNOLOGÍA
9.2. IDENTIFICAR LAS VULNERABILIDADES GENERALES DE LAS APLICACIONES
9.3. IDENTIFICAR LAS VULNERABILIDADES DE LAS APLICACIONES WEB
9.4. IMPLEMENTAR CONTROLES DE SEGURIDAD DE APLICACIONES

10. INTEGRACIÓN DE ACTIVOS EN UNA ARQUITECTURA EMPRESARIAL SEGURA

10.1. INTEGRAR LOS ESTÁNDARES Y LAS MEJORES PRÁCTICAS EN LA SEGURIDAD EMPRESARIAL
10.2. SELECCIONAR MODELOS DE IMPLEMENTACIÓN TÉCNICA
10.3. INTEGRAR LOS SERVICIOS DE SEGURIDAD AUMENTADOS EN LA NUBE
10.4. ASEGURAR EL DISEÑO DE LA INFRAESTRUCTURA EMPRESARIAL
10.5. INTEGRAR LA SEGURIDAD DE LOS DATOS EN LA ARQUITECTURA EMPRESARIAL
10.6. INTEGRAR APLICACIONES EMPRESARIALES EN UN ARQUITECTURA

11. REALIZACIÓN DE EVALUACIONES DE SEGURIDAD

11.1. SELECCIONAR MÉTODOS DE EVALUACIÓN DE SEGURIDAD
11.2. REALIZAR EVALUACIONES DE SEGURIDAD CON HERRAMIENTAS ADECUADAS

12. RESPUESTA Y RECUPERACIÓN DE INCIDENTES

12.1. PREPÁRESE PARA LA RESPUESTA A INCIDENTES Y LAS INVESTIGACIONES FORENSES
12.2. REALIZACIÓN DE ANÁLISIS FORENSE Y RESPUESTA A INCIDENTES

BENEFICIOS

- La certificación CASP+ valida la competencia de nivel avanzado en gestión de riesgos, operaciones y arquitectura de seguridad empresarial, investigación y colaboración e integración de seguridad empresarial.