Certified Hacking Forensic Investigator

Código: CHFI-001

Propuesta de Valor: EC-COUNCIL

Duración: 40 Horas Académicas

Las tecnologías digitales están cambiando el negocio. A medida que las organizaciones utilizan tecnologías digitales como cloud, mobile, datos y IOT, el contexto de la forense digital es más relevante que antes. El crecimiento del número de ciberdelitos ha cambiado el papel de Forense desde el ADN hasta el digital.

Según el informe de investigación de mercado publicado por IndustryARC, para el año 2020, el mercado forense alcanzará los 4.800 millones de dólares. IndustryARC también predice que el máximo uso de la técnica forense digital es del sector federal y esto crecerá de $ 1,097.2 millones en 2015 a 2.060,5 millones de dólares en 2020. Los principales conductores para esto son las amenazas, ciberdelincuencia y ataques terroristas. Foote Partners, que rastrea la tecnología de la información (TI) emplea a través de todos los niveles de habilidad, demanda de talento de la seguridad cibernética y prevee elevarse a seis millones en 2019, con un déficit esperado de 1,5 millones de profesionales.

AUDIENCIA

- CHFI v9 cubre los detalles metodológicos, enfoque forense informático y evidencia análisis. Proporciona las habilidades necesarias para identificar las huellas de los intrusos y reunir las pruebas necesarias para su procesamiento. Todas las principales herramientas y teorías utilizadas por el cibernético en la industria forense están cubiertos en el plan de estudios.

  La certificación puede fortalecer el nivel de conocimientos de la siguiente audiencia:
  - Personal encargado de hacer cumplir la ley.
  - Administradores de sistemas.
  - Agentes de seguridad.
  - Personal militar.
  - Profesionales del derecho.
  - Banqueros.
  - Encargados de la seguridad informática y de red.
  - Profesionales y cualquier persona interesada acerca de la integridad de la red y de las investigaciones.

PRE REQUISITOS

- Profesionales de TI / forenses con conocimientos básicos sobre seguridad informática / cibernética, Informática forense y respuesta a incidentes.

- La finalización previa de la formación CEH sería una ventaja.

OBJETIVOS

- Comprender la forma de ejecutar una investigación digital.
- Aplicar la metodología con la cual se llevan acabo las investigaciones forenses digitales apegadas a la legislación, códigos y normas existentes, tanto nacionales como internacionales.
- Realizar investigaciones para obtener evidencias digitales que sustenten un caso.

CERTIFICACIÓN DISPONIBLE

Computer Hacking Forensic Investigator Certification

- Número de preguntas: 150.
- Duración de la prueba: 4 Hours.
- Formato de prueba: Multiple Choice.
- Entrega de prueba: ECC EXAM.
- Prefijo de examen: 312-49 (ECC EXAM).

CONTENIDO

1. INFORMÁTICA FORENSE EN EL MUNDO DE HOY

2. PROCESO DE INVESTIGACIÓN FORENSE DE COMPUTADORAS

3. COMPRENSIÓN DE LOS DISCOS DUROS Y LOS SISTEMAS DE ARCHIVOS

4. ADQUISICIÓN Y DUPLICACIÓN DE DATOS

5. DERROTAR LAS TÉCNICAS ANTI-FORENSES

6. SISTEMA OPERATIVO FORENSE

7. ANÁLISIS FORENSE DE LA RED

8. INVESTIGACIÓN DE ATAQUES WEB

9. BASE DE DATOS FORENSE

10. CLOUD FORENSIC

11. MALWARE FORENSE

12. INVESTIGACIÓN DE DELITOS POR CORREO ELECTRÓNICO

13. FORENSE MÓVIL

14. REPORTE Y PRESENTACIÓN DE INFORMES FORENSES

BENEFICIOS

- Al finalizar el curso el estudiante podrá aplicar la metodología con la cual se llevan acabo las investigaciones forenses digitales apegadas a la legislación, códigos y normas existentes, tanto nacionales como internacionales.