

ECIHv2: EC-Council Certified Incident Handler

El programa EC-Council Certified Incident Handler está diseñado para proporcionar las habilidades fundamentales para manejar y responder a los incidentes de seguridad informática en un sistema de información. El curso aborda varios principios y técnicas subyacentes para detectar y responder a las amenazas de seguridad informática actuales y emergentes. Los estudiantes aprenderán cómo manejar varios tipos de incidentes, metodologías de evaluación de riesgos y varias leyes y políticas relacionadas con el manejo de incidentes. Después de asistir al curso, podrán crear políticas de manejo y respuesta a incidentes y lidiar con varios tipos de incidentes de seguridad informática.

1.1 Resultados Clave

- Principios, procesos y técnicas para detectar y responder a amenazas de seguridad/ infracciones
- Enlace con órganos jurídicos y reglamentarios
- Aprender a manejar incidentes y realizar evaluaciones
- Cubrir diversos incidentes como código malicioso, ataques a la red, y los ataques internos

1.2 Temario

Módulo 1: Introducción al manejo y Respuesta a Incidentes

Módulo 2: Proceso de Respuesta y Manejo de Incidentes

Módulo 3: Lectura Forense y Primeras Respuestas

Módulo 4: Manejo y respuesta de incidentes de código malicioso

Módulo 5: Manejo y respuesta de Incidentes de seguridad de correo electrónico

Módulo 6: Manejo y respuesta de Incidentes de seguridad de red

Módulo 7: Manejo y respuesta de Incidentes de seguridad de las aplicaciones Web

Módulo 8: Manejo y respuesta de Incidentes en la seguridad de la nube

Módulo 9: Manejo y respuesta de amenazas de intrusos

1.3 Información del Examen

- Título del examen: EC-Council Certified Incident Handler
- Código de examen: 212-89
- Número de preguntas: 100
- Duración: 3 horas
- Disponibilidad: Portal Examen ECC
- Formato de Prueba: Opción múltiple
- Puntuación: 70%