EC-Council

EC-Council

Certified Incident Handler v2

Prepárate para Manejar y Responder a los Incidentes de Seguridad

Descripción del curso

Esta última iteración del programa de Gestión de Incidentes Certificado (ECIH) del EC-Council ha sido diseñada y desarrollada en colaboración con profesionales de ciberseguridad y manejo de incidentes y respuesta en todo el mundo.

Es un programa integral de nivel especializado que imparte los conocimientos y habilidades que las organizaciones necesitan para manejar las consecuencias posteriores a la infracción al reducir el impacto del incidente, tanto desde la perspectiva financiera como reputacional.

ECIH es un programa basado en métodos que utiliza un enfoque holístico para abarcar vastos conceptos relacionados con el manejo y respuesta organizacionales de incidentes que van desde la preparación y planificación del proceso de respuesta de manejo de incidentes hasta la recuperación de los activos organizacionales después de un incidente de seguridad.

Estos conceptos son esenciales para manejar y responder a los incidentes de seguridad para proteger a las organizaciones de futuras amenazas o ataques.

¿Quién debería asistir?

- Penetrarion Testers
- Auditores de Valoración de Vulnerabilidad
- Administradores de Valoración de Riesgos
- Administradores de Red
- Ingenieros de Seguridad de Aplicaciones
- Administradores / Ingenieros de Sistemas
- Administradores de Firewall / Gerentes de Red / Gerente de TI
- Investigadores de Forensia / Analistas y Analistas de SOC

Agenda del curso

Duración: 24 horas

Día 1

- Introducción al Manejo y Respuesta de Incidentes
- Manejo de Incidentes y Proceso de Respuesta
- Preparación Forense y Enumeración de Primera Respuesta

Día 2

- Manejo y respuesta a incidentes de malware
- Manejo y Respuesta a Incidentes de Seguridad de Correo Electrónico
- Manejo y Respuesta a Incidentes de Seguridad de Red

Día 3

- Manejo y Respuesta a Incidentes de Seguridad de Aplicaciones Web
- Manejo y Respuesta a Incidentes de Seguridad en la Nube
- Manejo y Respuesta a las Amenazas Internas

Necesidad de la Gestión de Incidentes

TIEMPO PARA IDENTIFICAR UN ATAQUE MALICIOSO	TIEMPO PARA CONTENER Y RECUPERARSE DE UN ATAQUE	ORGANIZACIONES QUE NO TIENE UN PLAN DE RESPUESTA A INCIDENTES
214 días	77 días	76%

74% de los empleadores calificaron la dificultad de contratar personal calificado con experiencia como muy alta	
Dos de las 10 medidas principales para reducir costos en caso de una brecha de información	
Costo promedio de ahorro por registro con personal entrenado en Seguridad de información	Costo promedio de ahorro con un equipo de Respuesta a Incidentes
9.3 USD	14 USD

SAVANT CONSULTORES

EC-Council

809-363-1162 | cursos@savant.com.do | www.savant.com.do

Objetivos de aprendizaje

- Comprender los problemas clave que afectan al mundo de la seguridad de la información.
- Aprenda a combatir diferentes tipos de amenazas de ciberseguridad, vectores de ataque, actores de amenazas y sus motivos.
- Conozca los fundamentos de la gestión de incidentes, incluidos los signos y los costos de un incidente.
- Comprender los fundamentos de la gestión de vulnerabilidades, evaluación de amenazas, gestión de riesgos y automatización y orquestación de respuesta a incidentes.
- Domine todas las mejores prácticas de manejo y respuesta de incidentes, estándares, marcos de seguridad cibernética, leyes, actos y regulaciones
- Decodifique los diversos pasos involucrados en la planificación de un programa de manejo y respuesta de incidentes
- Obtenga una comprensión de los fundamentos de la informática forense y la preparación forense
- Comprender la importancia del primer procedimiento de respuesta, incluida la recopilación de pruebas, el embalaje, el transporte, el almacenamiento, la adquisición de datos, la recopilación de pruebas estáticas y volátiles, y el análisis de pruebas
- Comprender las técnicas anti-forenses utilizadas por los atacantes para encontrar encubrimientos de incidentes de seguridad cibernética
- Aplique las técnicas correctas a diferentes tipos de incidentes de ciberseguridad de manera sistemática, incluidos incidentes de malware, incidentes de seguridad de correo electrónico, incidentes de seguridad de red, incidentes de seguridad de aplicaciones web, incidentes de seguridad en la nube e incidentes relacionados con amenazas internas

Aprenda todas las fases en el Manejo de Incidentes

SAVANT CONSULTORES

EC-Council

Examen

Duración: 3 horas

Nombre del examen: EC-Council Certified Incident Handler
Código del examen: 212-89
Cantidad de preguntas: 100
Formato: Selección múltiple
Disponibilidad: EC-Council Exam Portal
Puntuación para pasar: 70%

Certificación

El examen **ECIH** puede ser tomado después de finalizar la asistencia al curso oficial completo de **ECIH**.
Los candidatos que pasan con éxito el examen recibirá su certificado **ECIH** y los privilegios de membresía.
Se espera que los miembros se adhieran a los requisitos de recertificación a través de los requisitos de Educación Continua.

Información general

- El costo del curso oficial incluye el voucher para tomar el examen
- Courseware digital con más de 1,000 páginas repletas de contenido organizado metodológicamente
- Acceso al portal Aspen.eccouncil.org donde puede acceder miles de herramientas
- Subscripción por seis meses a los laboratorios virtuales para mayor comodidad con más de 50 laboratorios

EC-Council Accredited Training Center

ECIH™ EC-Council Certified Incident Handler

CEI Certified EC-Council Instructor

SAVANT CONSULTORES

EC-Council

809-363-1162 | cursos@savant.com.do | www.savant.com.do