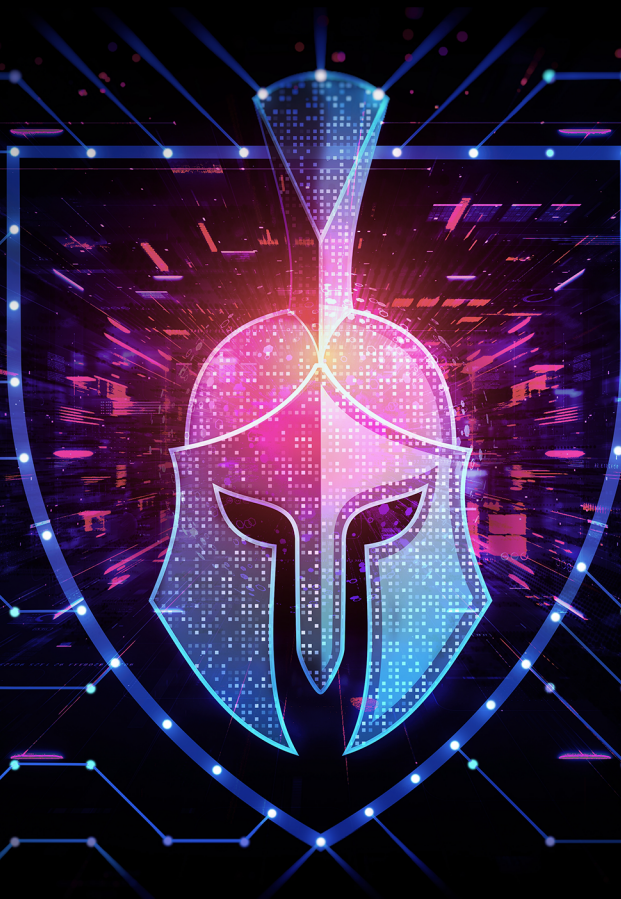




EC-Council
CERTIFIED
INCIDENT HANDLER

MASTER THE CRITICAL FIRST LINE OF DEFENSE

Gain The Ultimate Skills to Identify,
Contain and Minimize Cyber Incidents

Tiempo promedio de respuesta a incidentes: Un problema creciente

277 días

Tiempo promedio para identificar y contener una brecha de datos.

49 días

Las brechas de ransomware tardaron 49 días más que el promedio en identificarse y contenerse.

303 Días

Tiempo promedio para identificar y contener un compromiso en la cadena de suministro.

¿Por qué las organizaciones necesitan respuesta a incidentes?

1. ¿Las organizaciones invierten en comprar productos de seguridad costosos?

➤ **SI**

2. ¿Confiaron en exceso en los productos de seguridad implementados?

➤ **SI**

3. ¿Contrataron a personas o equipos para configurar esos productos de seguridad?

➤ **No muy a menudo**

4. ¿Tuvieron éxito en evitar incidentes de seguridad?

➤ **No**

5. ¿Predijeron las posibles formas del ataque y su impacto?

➤ **No**

6. ¿Tenían un plan estructurado de gestión y respuesta a incidentes para enfrentar posibles incidentes de seguridad?

➤ **NO**

¿Qué es la respuesta a incidentes?

1. Un proceso que permite a las organizaciones manejar y responder instantáneamente a diversos incidentes de seguridad
2. Un proceso que permite a las organizaciones detectar, validar, contener y erradicar diversos incidentes de seguridad
3. Un proceso que garantiza la recuperación segura y sistemática de todos los activos organizacionales del impacto de los incidentes de seguridad
4. Un proceso que asegura que las organizaciones estén bien preparadas para manejar los incidentes de seguridad más comunes

En resumen, las organizaciones necesitan
un plan/proceso de gestión y respuesta a incidentes.

Las organizaciones necesitan
un Gestor de Incidentes Certificado por EC-Council.

Descripción general del programa E|CIH

¿Qué es E|CIH?

El programa Certified Incident Handler de EC-Council equipa a los estudiantes con los conocimientos, habilidades y capacidades para prepararse eficazmente, enfrentar y erradicar amenazas y actores maliciosos durante un incidente. Este programa proporciona el proceso completo de gestión y respuesta a incidentes, junto con laboratorios prácticos que enseñan los procedimientos y técnicas tácticas necesarias para planificar, registrar, clasificar, notificar y contener de manera efectiva. Los estudiantes aprenderán a manejar diversos tipos de incidentes, metodologías de evaluación de riesgos, así como leyes y políticas relacionadas con la gestión de incidentes.

Después de asistir al curso, los estudiantes podrán crear políticas de IH&R y enfrentar diferentes tipos de incidentes de seguridad, como malware, seguridad del correo electrónico, seguridad de redes, seguridad de aplicaciones web, seguridad en la nube e incidentes relacionados con amenazas internas. El E|CIH (EC-Council Certified Incident Handler) también cubre actividades posteriores al incidente, como contención, erradicación, recopilación de evidencia y análisis forense, que pueden conducir a la persecución legal o la implementación de contramedidas para garantizar que el incidente no se repita.

El E|CIH es un curso orientado por métodos que proporciona un enfoque holístico, cubriendo conceptos amplios relacionados con la gestión y respuesta a incidentes en una organización (IH&R), desde la preparación/planificación del proceso de respuesta a incidentes hasta la recuperación de los activos organizacionales del impacto de los incidentes de seguridad. Estos conceptos son esenciales para manejar y responder a incidentes de seguridad con el fin de proteger a las organizaciones de amenazas o ataques futuros.

Con más de 95 laboratorios avanzados, 800 herramientas cubiertas y exposición a actividades de gestión de incidentes en muchos sistemas operativos diferentes, E|CIH ofrece un enfoque integral pero táctico para planificar y enfrentar incidentes cibernéticos. El programa E|CIH aborda todas las etapas involucradas en el proceso de IH&R, y esta atención hacia un enfoque realista y orientado al futuro convierte a E|CIH en una de las certificaciones más completas relacionadas con IH&R disponibles en el mercado actual.

Módulos del curso E|CIH:

MÓDULO 01: INTRODUCCIÓN A LA GESTIÓN Y RESPUESTA A INCIDENTES

- Comprender las amenazas de seguridad de la información y los vectores de ataque
- Explicar diversos marcos de ataque y defensa
- Comprender los conceptos de seguridad de la información
- Comprender los incidentes de seguridad de la información
- Comprender el proceso de gestión de incidentes
- Comprender la automatización y la orquestación de la respuesta a incidentes
- Describir diversas buenas prácticas de gestión y respuesta a incidentes
- Explicar diversos estándares relacionados con la gestión y respuesta a incidentes
- Explicar diversos marcos de ciberseguridad
- Comprender las leyes y el cumplimiento legal sobre gestión de incidentes

MÓDULO 02: PROCESO DE GESTIÓN Y RESPUESTA A INCIDENTES

- Comprender el proceso de gestión y respuesta a incidentes (IH&R)
- Explicar los pasos de preparación para la gestión y respuesta a incidentes
- Comprender el registro y la asignación de incidentes
- Comprender la clasificación (triage) de incidentes
- Explicar el proceso de notificación
- Comprender el proceso de contención
- Describir la recopilación de evidencia y el análisis forense
- Explicar el proceso de erradicación
- Comprender el proceso de recuperación
- Describir diversas actividades posteriores al incidente
- Explicar la importancia de las actividades de intercambio de información

MÓDULO 03: PRIMERA RESPUESTA

- Explicar el concepto de primera respuesta
- Comprender el proceso de asegurar y documentar la escena del delito
- Comprender el proceso de recopilación de evidencia en la escena del delito
- Explicar el proceso de preservación, embalaje y transporte de la evidencia

MÓDULO 04: GESTIÓN Y RESPUESTA A INCIDENTES DE MALWARE

- Comprender la gestión de incidentes de malware
- Explicar la preparación para gestionar incidentes de malware
- Comprender la detección de incidentes de malware
- Explicar la contención de incidentes de malware
- Describir cómo realizar análisis de malware
- Comprender la erradicación de incidentes de malware
- Explicar la recuperación después de incidentes de malware
- Comprender la gestión de incidentes de malware – estudio de caso
- Describir las mejores prácticas contra incidentes de malware

Módulos del curso E|CIH:

MÓDULO 05: GESTIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD DE CORREO ELECTRÓNICO

- Comprender los incidentes de seguridad de correo electrónico
- Explicar los pasos de preparación para gestionar incidentes de seguridad de correo electrónico
- Comprender la detección y contención de incidentes de seguridad de correo electrónico
- Comprender el análisis de incidentes de seguridad de correo electrónico
- Explicar la erradicación de incidentes de seguridad de correo electrónico
- Comprender el proceso de recuperación después de incidentes de seguridad de correo electrónico
- Comprender la gestión de incidentes de seguridad de correo electrónico – estudio de caso
- Explicar las mejores prácticas contra incidentes de seguridad de correo electrónico

MÓDULO 06: GESTIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD DE RED

- Comprender la gestión de incidentes de seguridad de red
- Prepararse para gestionar incidentes de seguridad de red
- Comprender la detección y validación de incidentes de seguridad de red
- Comprender la gestión de incidentes de acceso no autorizado
- Comprender la gestión de incidentes de uso inapropiado
- Comprender la gestión de incidentes de denegación de servicio (DoS)
- Comprender la gestión de incidentes de seguridad en redes inalámbricas
- Comprender la gestión de incidentes de seguridad de red – estudio de caso
- Describir las mejores prácticas contra incidentes de seguridad de red

MÓDULO 07: GESTIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD DE APLICACIONES WEB

- Comprender la gestión de incidentes de aplicaciones web
- Explicar la preparación para gestionar incidentes de seguridad de aplicaciones web
- Comprender la detección y contención de incidentes de seguridad de aplicaciones web
- Explicar el análisis de incidentes de seguridad de aplicaciones web
- Comprender la erradicación de incidentes de seguridad de aplicaciones web
- Explicar la recuperación después de incidentes de seguridad de aplicaciones web
- Comprender la gestión de incidentes de seguridad de aplicaciones web – estudio de caso
- Describir las mejores prácticas para asegurar aplicaciones web

Módulos del curso E|CIH:

MÓDULO 08: GESTIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD EN LA NUBE

- Comprender la gestión de incidentes de seguridad en la nube
- Explicar los diversos pasos involucrados en la gestión de incidentes de seguridad en la nube
- Comprender cómo manejar incidentes de seguridad en Azure
- Comprender cómo manejar incidentes de seguridad en AWS
- Comprender cómo manejar incidentes de seguridad en Google Cloud
- Comprender la gestión de incidentes de seguridad en la nube – estudio de caso
- Explicar las mejores prácticas contra incidentes de seguridad en la nube

MÓDULO 09: GESTIÓN Y RESPUESTA A AMENAZAS INTERNAS

- Comprender la gestión de amenazas internas
- Explicar los pasos de preparación para gestionar amenazas internas
- Comprender la detección y contención de amenazas internas
- Explicar el análisis de amenazas internas
- Comprender la erradicación de amenazas internas
- Comprender el proceso de recuperación después de ataques internos
- Comprender la gestión de amenazas internas – estudio de caso
- Describir las mejores prácticas contra amenazas internas

MÓDULO 10: GESTIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD EN ENDPOINTS

- Comprender la gestión de incidentes de seguridad en endpoints
- Explicar la gestión de incidentes de seguridad basados en dispositivos móviles
- Explicar la gestión de incidentes de seguridad basados en IoT
- Explicar la gestión de incidentes de seguridad basados en OT
- Comprender la gestión de incidentes de seguridad en endpoints – estudio de caso

¿Qué aprendes con E|CIH?

Principales problemas que afectan al mundo de la seguridad de la información.

Diversos tipos de amenazas de ciberseguridad, vectores de ataque, actores de amenazas y sus motivos, metas y objetivos en los ataques de ciberseguridad.

Diversos marcos de ataque y defensa (metodología Cyber Kill Chain, marco MITRE ATT&CK, etc.)

Fundamentos de los conceptos de seguridad de la información (evaluación de vulnerabilidades, gestión de riesgos, inteligencia de amenazas cibernéticas, modelado de amenazas y cacería de amenazas).

Fundamentos de la gestión de incidentes (incidentes de seguridad de la información, señales y costos de un incidente, gestión y respuesta a incidentes, y automatización y orquestación de la respuesta a incidentes).

Diferentes mejores prácticas de gestión y respuesta a incidentes, estándares, marcos de ciberseguridad, leyes, normas y regulaciones.

Diversos pasos involucrados en la planificación de un programa de gestión y respuesta a incidentes (planificación, registro y asignación, triage, notificación, contención, recopilación de evidencia y análisis forense, erradicación, recuperación y actividades posteriores al incidente).

Importancia de la primera respuesta y el procedimiento de primera respuesta (recopilación de evidencia, documentación, preservación, embalaje y transporte).

Cómo manejar y responder de manera sistemática a diferentes tipos de incidentes de ciberseguridad (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, incidentes relacionados con amenazas internas e incidentes de seguridad en endpoints).

Aprender las **9 etapas** del proceso de Gestión y Respuesta a Incidentes (IH&R)



Características clave y componentes críticos del programa E|CIH



- Basado en un análisis exhaustivo de tareas laborales (JTA) a nivel de la industria
- Enfoque estructurado para ejecutar el proceso de gestión y respuesta a incidentes
- Enfoque en desarrollar habilidades para manejar diferentes tipos de incidentes de ciberseguridad

Cubre lo más reciente &

Recopilación de

Plantillas de gestión de incidentes	Guías operativas y manuales de ejecución para la gestión de incidentes	Listas de verificación y kits de herramientas para la gestión de incidentes
Hojas de referencia rápida para la gestión de incidentes	Herramientas y plataformas de gestión y respuesta a incidentes	Marcos de gestión y respuesta a incidentes
Estándares, leyes y cumplimiento legal en la gestión de incidentes		Estudios de caso en tiempo real sobre la gestión y respuesta a incidentes de ciberseguridad

Beneficios únicos de los laboratorios avanzados de EICIH

01



La configuración del laboratorio

simula un entorno en tiempo real con redes y plataformas reales

02



Cada objetivo de aprendizaje se demuestra utilizando laboratorios complejos y avanzados

03



Programa intensivo en laboratorios

(Demostración de diversos incidentes de ciberseguridad mediante laboratorios basados en escenarios)

04



Práctico

(Dedicación del 50 % del tiempo de capacitación a laboratorios)

05



Parcheado más reciente

Sistemas operativos de Windows

06



Ubuntu,

Parrot Security, firewall Pfsense, servidor OSSIM y Android para realizar los laboratorios.

07



Software

Forense avanzado

08



Plataformas de inteligencia de amenazas más recientes

09



Soluciones más recientes de monitoreo de red
Laboratorios basados en escenarios

10



Aprende

a manejar y responder a diversos tipos de incidentes de seguridad en una red organizacional en tiempo real.

11



Comprender, detectar y analizar técnicas, tácticas y procedimientos (TTPs) de ataques modernos utilizando diversas herramientas de gestión de incidentes.



E|CIH está diseñado para remediar las amenazas cibernéticas modernas

Beneficios clave / Componentes críticos del curso E|CIH explicados:

1) Cumplimiento al 100 % con la Publicación Especial 800-181 de NICE Marco de Fuerza Laboral en Ciberseguridad

E|CIH se mapea completamente con la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) en la categoría Protect and Defend (PR) y en el área de especialidad Incident Response (CIR), que se ocupa de investigar, analizar y responder a incidentes cibernéticos dentro de un entorno o enclave de red.

2) Cumplimiento al 100 % con los marcos de trabajo CREST Certified Incident Manager (CCIM)

E|CIH se mapea completamente con CREST Certified Incident Manager (CCIM), que es un esquema de alcance amplio enfocado en mantener un estándar apropiado para la respuesta a incidentes, administrado por un organismo profesional de la industria, entregado por la industria y respaldado por CESG y CPNI. El esquema CCIM, actualmente administrado por CREST, también se conoce como CREST Certified Incident Response Scheme (CSIR).

3) Basado en un análisis exhaustivo de tareas laborales en toda la industria

El programa E|CIH fue desarrollado después de un análisis intensivo de todas las posibles combinaciones de tareas, conocimientos, habilidades y capacidades (TKSA) de ofertas laborales relevantes de diversas empresas multinacionales.

4) Enfoque en un método estructurado para IH&R

Este proceso incluye diversas etapas como la preparación de IH&R, el registro y asignación de incidentes, la clasificación y notificación de incidentes, la contención de incidentes, la recopilación de evidencia y análisis forense, la erradicación de incidentes, la recuperación de sistemas y las actividades posteriores al incidente.

5) Amplia colección de plantillas, listas de verificación y kits de herramientas para la gestión de incidentes

Esta amplia colección de material documental permite a los gestores de incidentes realizar de manera eficaz la documentación relacionada con incidentes en su organización dentro de un plazo razonable. Las plantillas de gestión de incidentes ayudan a los gestores a redactar informes completos basados en la audiencia objetivo y los incidentes, proporcionando así más opciones a los estudiantes y gestores de incidentes que cualquier otro programa del mercado.

6) Amplia colección de playbooks y runbooks para la gestión de incidentes

Cuando se usan conjuntamente, los playbooks y los runbooks pueden guiar a los gestores de incidentes en la orquestación de diversos procesos de seguridad según el tipo de incidente. Los playbooks y runbooks listos para usar ayudan al equipo de IH&R a automatizar ciberataques comunes como phishing, malware y denegación de servicio.

7) Enfoque en desarrollar habilidades para manejar diversos incidentes de ciberseguridad

Este programa demuestra de manera sistemática el proceso completo de IH&R para diversos tipos de incidentes de ciberseguridad, incluidos malware, seguridad de correo electrónico, seguridad de red, seguridad de aplicaciones web, seguridad en la nube, amenazas internas, seguridad basada en dispositivos móviles, seguridad basada en IoT y seguridad basada en OT. Cubrir el proceso completo de IH&R de extremo a extremo convierte a E|CIH en un programa único en el mercado.

8) Énfasis en la preparación forense y los procedimientos de primera respuesta

La falta de preparación forense o de procesos de primera respuesta ante incidentes puede causar daños drásticos y desastrosos en las organizaciones. El programa E|CIH se centra en cómo una organización debe estar preparada y equipada para enfrentar cualquier tipo de incidente cibernético, junto con los pasos que debe seguir el primer respondedor para registrar o gestionar incidentes.

9) Programa intensivo en laboratorios (demostración de diversos incidentes de ciberseguridad mediante laboratorios basados en escenarios)

El programa E|CIH demuestra incidentes de seguridad en tiempo real mediante laboratorios basados en escenarios y con respecto a diversas fases de la gestión de incidentes. Esto ayuda a los estudiantes y gestores de incidentes a adquirir conocimientos y habilidades profundos en preparación IH&R, registro y asignación, clasificación y notificación, contención, recopilación de evidencia y análisis forense, erradicación, recuperación de sistemas y actividades posteriores al incidente.

10) Programa práctico (50% del tiempo de capacitación dedicado a laboratorios)

La proporción teoría-práctica en el programa E|CIH es 50:50, proporcionando a los estudiantes experiencia en tiempo real en escenarios IH&R y práctica con las herramientas, técnicas, metodologías y marcos más recientes.

11) El entorno de laboratorio simula un entorno posterior a la brecha

El entorno de laboratorio simula una situación en tiempo real para los gestores de incidentes, y esta experiencia puede ayudar a enfrentar efectivamente incidentes en las organizaciones.

12) Cubre las herramientas, plataformas y marcos IH&R más recientes

El curso E|CIH incluye una biblioteca de herramientas, plataformas y marcos en diferentes plataformas operativas que los gestores y respondedores de incidentes requieren para manejar y responder de forma efectiva a diversas amenazas e incidentes organizacionales.

13) Cubre los estudios de caso más recientes en tiempo real sobre la gestión y respuesta a incidentes de ciberseguridad

Estos estudios de caso son específicos de incidentes reportados por organizaciones o usuarios, incluyendo procedimientos de gestión de incidentes, desde la fase de detección hasta la recuperación, así como las lecciones aprendidas.



Detalles del Examen:

Título del Examen:

Gestor de Incidentes Certificado por EC-Council

Código de Examen:

212-89

Número de Preguntas:

100

Duración:

3 horas

Disponibilidad del examen:

ECC Exam Portal

Formato de la prueba:

Selección Múltiple

Passing Score: Refer <https://cert.eccouncil.org/faq.html>

Detalles de la capacitación

Entrenamiento: 3 Días

Opciones de Capacitación:

iLearn (Autoestudio)

Esta solución es un entorno asincrónico de autoestudio en formato de transmisión de video.

iWeek (En vivo online)

Esta solución es un curso de capacitación en línea, en vivo y dirigido por un instructor.

Partner de Capacitación (Presencial)

Esta solución ofrece capacitación presencial para que puedas beneficiarte de la colaboración con tus compañeros.



Roles laborales mapeados a E|CIH:

- 1 Gestor de incidentes
- 2 Respondedor de incidentes
- 3 Consultor/Asociado/Analista/Ingeniero/Especialista
Experto/Gerente de Respuesta a Incidentes
- 4 Analista/Ingeniero/Gerente de CSIRT
- 5 Asociado/Analista/Ingeniero/Especialista/
Gerente de Seguridad de la Información
- 6 Asociado/Analista/Ingeniero/Especialista/
Gerente de Seguridad de la Información
- 7 Analista de Centro de Operaciones de Seguridad de TI
(Analista/Ingeniero SOC)
- 8 Investigador/Consultor/Analista/Gerente de Ciberforense
- 9 Analista de forense digital
- 10 Analista/Gerente de vulnerabilidades y riesgos cibernéticos
- 11 Analista de inteligencia cibernética y analista/
Especialista de amenazas de ciberseguridad
- 12 Líder del equipo de respuesta a incidentes de ciberseguridad
- 13 Evaluador de penetración (Pentester)

Quiénes pueden postular a E|CIH:

- Cualquier profesional de ciberseguridad de nivel intermedio a alto con un mínimo de 3 años de experiencia
- Personas de la profesión de seguridad de la información que deseen enriquecer sus habilidades y conocimientos en el campo de la gestión y respuesta a incidentes
- Personas interesadas en prevenir amenazas cibernéticas



Principales herramientas, playbooks y más en el curso E|CIH

10 herramientas populares o más recientes:

- Cyber Triage
- KeepNote
- IDA and OllyDbg
- Wireshark
- MxToolbox
- Rmail
- AlienVault OSSIM
- RdpGuard
- Nessus
- dotDefender
- MalwareBytes
- ManageEngine Endpoint Central

Los 5 principales playbooks y runbooks:

- Playbook de respuesta a incidentes DDoS
- Playbook de respuesta a incidentes de phishing
- Playbook de respuesta a incidentes de amenazas internas
- Playbook de respuesta a incidentes de ransomware
- Runbook de respuesta a incidentes DDoS

Principales metodologías y marcos más recientes:

- Playbook de respuesta a incidentes DDoS
- Playbook de respuesta a incidentes de phishing
- Playbook de respuesta a incidentes de amenazas internas
- Playbook de respuesta a incidentes de ransomware
- Runbook de respuesta a incidentes DDoS

Principales: plantillas, listas de verificación y kits de herramientas más recientes:

- Plantilla de documento de política de preparación de informática forense
- Plantilla de plan de gestión y respuesta a incidentes
- Plantilla de documento de políticas y procedimientos de gestión y respuesta a incidentes
- Lista de verificación del gestor de incidentes
- Requisitos del kit de herramientas del respondedor de incidentes
- Reconocimiento / Endoso / Mapeamiento del informe de análisis forense

Reconocimiento / Endoso / Mapeamiento



ElCIHv3 es el programa más deseado según los principales profesionales de gestión de incidentes a nivel global



El E|CIH es el programa más completo y proporciona herramientas y metodologías aplicables a cualquier industria. Me ayudó mucho a desarrollar mi trabajo, para que pueda ofrecer a mi organización las mejores prácticas y las mejores formas de identificar...

Pedro Pachon

Cybersecurity Chief
Falabela Bank (Columbia)

El curso E|CIH nos ayuda a analizar el riesgo y, antes de eso, también a responder a cualquier incidente. Qué precauciones se deben tomar y cómo proteger a una organización de brechas, y también más sobre protección de datos.



Elysha Esaivani

Problem Manager



El E|CIH ayuda a responder a cualquier incidente cibernético o incidente de espionaje que pueda ocurrir en una organización, y realmente nos ayuda a contenerlo lo antes posible. El curso E|CIH me permite entender desde dónde se inicia el ataque y hasta dónde podemos contenerlo o controlarlo y restaurar todo nuevamente en línea.

Mathimohan Daniel Raja

Associate Analyst



Este curso es muy útil para las empresas porque aprendes cómo crear una ruta de respuesta a incidentes exitosa. Además, este programa te da el enfoque correcto al enfrentar un incidente, brindándote las soluciones correctas y adecuadas. Esto también incluye aspectos legales. Más que darte el enfoque correcto, el programa también te enseña las técnicas básicas de gestión de incidentes para que podamos trabajar con ellas.



Giovanni Miglionico

IT Security Manager



Como miembro de un equipo de ciberseguridad, mi propósito es saber cómo debería reaccionar el equipo cuando atacantes maliciosos realizan alguna actividad maliciosa en su red o en la seguridad física. Entonces, con este curso, mi conocimiento sobre cómo el equipo de respuesta inicial puede reaccionar y realizar algunas acciones es muy útil para mejorar mis habilidades y mi mentalidad cuando realizo alguna operación.

Edoardo Rosa

Cybersecurity Specialist



El programa E|CIH proporciona una visión técnica con muchos laboratorios y herramientas que pueden utilizarse en el campo de la ciberseguridad. Además, entrega los estándares y protocolos que son esenciales en el manejo de incidentes. E|CIH es muy útil y me dio una base sobre la cual puedo avanzar en mi carrera en ciberseguridad.



Lorenzo Pomanti

System Engineer

EC-Council

Building A Culture Of Security

Sobre EC-Council

EC-Council creó la certificación Certified Ethical Hacker. Fundada en 2001 como respuesta al 11/09, la misión de EC-Council es proporcionar la formación y certificaciones que tanto profesionales principiantes como experimentados en ciberseguridad necesitan para mantener a salvo de ataques a corporaciones, organismos gubernamentales y otras entidades que los emplean.

Conocida mundialmente por su programa Certified Ethical Hacker, hoy EC-Council ofrece más de 200 programas de formación, certificaciones y grados académicos en áreas como Investigación Forense Informática, Análisis de Seguridad, Inteligencia de Amenazas y Seguridad de la Información. Como organización acreditada ISO/IEC 17024, reconocida bajo la Directiva 8140/8570 del Departamento de Defensa de los Estados Unidos y por muchas otras entidades autorizadas de ciberseguridad en todo el mundo, la compañía ha certificado a más de 350.000 profesionales a nivel global. Confiada por siete de las diez empresas del Fortune 10, la mitad de las empresas del Fortune 100, y múltiples organismos públicos y privados en más de 140 países, EC-Council es el estándar de oro en educación y certificación en ciberseguridad.

Como una organización verdaderamente global, con una firme convicción en promover la diversidad, equidad e inclusión en la fuerza laboral moderna de ciberseguridad, EC-Council mantiene oficinas en Estados Unidos, Reino Unido, India, Malasia, Singapur y Indonesia.

www.eccouncil.org