New Horizons
Centro de Capacitación

EC-Council
Building A Culture Of Security

D|FE
Digital Forensics Essentials

Digital Forensics Essentials

Inicia tu trayectoria en ciberseguridad con habilidades técnicas y prácticas fundamentales en el campo de la informática forense digital.

No se requiere experiencia previa en TI o ciberseguridad.
Incluye: Lecciones en video - Laboratorios prácticos - Desafíos tipo Capture the Flag (CTF) - Examen supervisado

EC-COUNCIL ESSENTIALS SERIES

La ciberseguridad es un campo muy amplio y complejo, con múltiples áreas de especialización. En muchas ocasiones, determinar el área adecuada de especialización y desarrollar las competencias fundamentales correctas representa un desafío significativo.
La Serie Essentials es un programa práctico e inmersivo diseñado para ayudar a los participantes a adquirir habilidades técnicas sólidas en diversas áreas de la ciberseguridad, asegurando al mismo tiempo que el programa sea altamente accesible y asequible.
Está diseñado y creado para formar una nueva generación de profesionales con capacidades técnicas desde el inicio de sus carreras en ciberseguridad. La metodología de los cursos de la Serie Essentials está pensada para estudiantes escolares, recién graduados, profesionales en transición, principiantes y equipos de TI o tecnología con poca o ninguna experiencia previa en TI o ciberseguridad.
Esta certificación en fundamentos de ciberseguridad permite a los estudiantes y equipos de TI aprender los diferentes principios que conforman la ciberseguridad, ayudándoles a identificar por sí mismos su área de interés o especialización, mientras desarrollan un conjunto de habilidades diversas en distintos dominios esenciales.
Adquiere las competencias necesarias para tu primera competencia Capture the Flag (CTF) con este curso de la Serie Essentials. El módulo final, correspondiente al proyecto integrador de laboratorio (Capstone Project), incluye un CTF simulado para poner a prueba tus habilidades en un entorno controlado.
Utiliza máquinas virtuales en vivo, software real y redes reales para resolver desafíos del mundo real, tanto desde la perspectiva del atacante como del defensor.
La Serie Essentials de EC-Council cubre ocho habilidades esenciales:
Hacking Ético, Defensa de Redes, Informática Forense Digital, Seguridad en la Nube, Seguridad del Internet de las Cosas (IoT), Operaciones de Centro de Operaciones de Seguridad (SOC), Inteligencia de Amenazas y DevSecOps.

¿Qué es EC-Council Digital Forensics Essentials?

El programa Digital Forensics Essentials (DFE) ayuda a los participantes a fortalecer su competencia y especialización en informática forense y seguridad de la información, incrementando así su valor profesional dentro de su entorno laboral y para su empleador.
Este curso introduce a los participantes en los fundamentos de la informática forense y en el proceso de investigación forense computacional. También abarca temas como la Dark Web, los sistemas operativos Windows y Linux, la forensia de malware y mucho más.
El componente de laboratorios interactivos garantiza que los estudiantes adquieran la experiencia práctica y aplicada necesaria para desempeñarse en el futuro en el ámbito de la informática forense digital.
Pon a prueba tus habilidades recién adquiridas con un emocionante ejercicio Capture the Flag (CTF), perfectamente integrado en nuestro proyecto final (Capstone Project).
Este CTF combina el uso de máquinas virtuales en tiempo real, software auténtico y redes reales, todo dentro de un entorno seguro y controlado tipo sandbox.
A través de estos desafíos exclusivos y prácticos —de tipo humano contra máquina— desarrollarás las competencias técnicas esenciales para destacar y alcanzar el éxito en tu carrera profesional dentro del campo de la ciberseguridad.

Los participantes certificados en DFE (Digital Forensics Essentials) cuentan con un medio formal de reconocimiento que pueden añadir a su currículum para demostrar su experiencia y competencias técnicas ante posibles empleadores.
Esto mejora sus oportunidades de crecimiento profesional, la posibilidad de acceder a mejores salarios y una mayor satisfacción laboral.
Si deseas continuar tu aprendizaje y avanzar en el campo de la informática forense digital, haz clic aquí: Certificación en Informática Forense Digital (Computer Hacking Forensics Investigator – C|HFI).

Sobre el docente

Profesional con más de 15 años en seguridad informática y respuesta a incidentes. Instructor oficial de EC-Council y CISO de RedCUDI (México), con experiencia en pentesting, Blue/Red Team y gobierno de la ciberseguridad.

Senior Cyberecurity Researcher - **Kalan T'aan**

Maestría en Ciencias - Secc. de Computación, Depto. de Ing. Eléctrica **CINVESTAV.**

Doctorado en Ciencias - Depto. Control Automático **CINVESTAV.**

Los participantes certificados en DFE (Digital Forensics Essentials) cuentan con un medio formal de reconocimiento que pueden añadir a su currículum para demostrar su experiencia y competencias técnicas ante posibles empleadores.
Esto mejora sus oportunidades de crecimiento profesional, la posibilidad de acceder a mejores salarios y una mayor satisfacción laboral.
Si deseas continuar tu aprendizaje y avanzar en el campo de la informática forense digital, haz clic aquí: Certificación en Informática Forense Digital (Computer Hacking Forensics Investigator – C|HFI).

Información del Programa Digital Forensics Essentials

Estructura del Curso

Duración: 32 horas académicas

Module 01: Fundamentos de la Informática Forense

- Fundamentos de la informática forense
- Evidencia digital
- Preparación forense (Forensic Readiness)
- Roles y responsabilidades del investigador forense
- Cumplimiento legal en informática forense

Module 02: Proceso de Investigación en Informática Forense

- Proceso de investigación forense y su importancia
- Proceso de investigación forense – Fase previa a la investigación
- Proceso de investigación forense – Fase de investigación
- Proceso de investigación forense – Fase posterior a la investigación

Laboratorios

- Realización de cálculos de Hash o HMAC
- Comparación de valores Hash de archivos para verificar su integridad
- Visualización de archivos en diversos formatos
- Creación de una imagen de disco de una partición de disco duro

Module 03: Comprensión de los Discos Duros y los Sistemas de Archivos

- Tipos de unidades de disco y sus características
- Estructura lógica de un disco
- Proceso de arranque de los sistemas operativos Windows, Linux y Mac
- Sistemas de archivos de Windows, Linux y Mac
- Examinación y análisis del sistema de archivos

Laboratorio

- Análisis del sistema de archivos de una imagen de Linux
- Recuperación de archivos eliminados de discos duros

Module 04: Adquisición y Duplicación de Datos

- Fundamentos de la adquisición de datos
- Tipos de adquisición de datos
- Formatos de adquisición de datos
- Metodología de adquisición de datos

Ejercicio de Laboratorio

- Creación de una imagen dd de una unidad del sistema
- Conversión del archivo de imagen adquirido en una máquina virtual arrancable
- Adquisición de la memoria RAM desde estaciones de trabajo Windows
- Visualización del contenido de un archivo de imagen forense

Module 05: Contrarrestando las Técnicas Anti-Forenses

- Concepto de anti-forense y sus principales técnicas
- Contramedidas frente a las técnicas anti-forenses

Laboratorios

- Extracción (file carving) en unidades SSD dentro de un sistema de archivos Windows
- Recuperación de datos desde particiones de disco perdidas o eliminadas
- Descifrado de contraseñas de aplicaciones
- Detección de esteganografía

Module 06: Informática Forense en Windows

- Información volátil y no volátil
- Análisis de la memoria y del registro de Windows
- Examen de la caché, cookies e historial registrados en los navegadores web
- Archivos y metadatos del sistema Windows

Laboratorios

- Adquisición de información volátil desde un sistema Windows en ejecución
- Análisis forense de una imagen de memoria RAM de Windows
- Examinación de artefactos de navegadores web
- Extracción de información sobre los procesos cargados en un equipo

Module 07: Informática Forense en Linux y Mac

- Datos volátiles y no volátiles en sistemas Linux
- Análisis de imágenes de sistemas de archivos utilizando The Sleuth Kit
- Forensia de memoria
- Forensia en sistemas Mac

Laboratorios

- Investigación forense sobre un volcado de memoria (memory dump) de Linux
- Recuperación de datos a partir de un volcado de memoria de Linux

Module 08: Informática Forense en Redes

- Fundamentos de la forensia de redes
- Conceptos y tipos de correlación de eventos
- Identificación de Indicadores de Compromiso (IoCs) a partir de registros de red
- Investigación del tráfico de red

Laboratorio

- Identificación e investigación de diversos ataques de red utilizando Wireshark

Module 09: Investigación de Ataques Web

- Forensia de aplicaciones web
- Análisis de registros de servidores web IIS y Apache
- Investigación de ataques web en servidores basados en Windows
- Detección e investigación de ataques en aplicaciones web

Laboratorio

- Identificación e investigación de ataques a aplicaciones web utilizando Splunk

Module 10: Forensia en la Dark Web

- Dark Web
- Forensia en la Dark Web
- Forensia del navegador TOR

Laboratorios

- Detección del navegador TOR en un equipo
- Análisis de volcados de memoria (RAM dumps) para recuperar artefactos del navegador TOR

Module 11: Investigación de Delitos por Correo Electrónico

- Fundamentos del correo electrónico
- Investigación de delitos relacionados con el correo electrónico y sus etapas

Ejercicio de Laboratorio

- Investigación de un correo electrónico sospechoso

Module 12: Informática Forense de Malware

- El malware, sus componentes y métodos de distribución
- Fundamentos de la forensia de malware y reconocimiento de los tipos de análisis de malware
- Análisis estático de malware
- Análisis de documentos de Word sospechosos
- Análisis dinámico de malware
- Análisis del comportamiento del sistema
- Análisis del comportamiento de red

Ejercicio de Laboratorio

- Realización de un análisis estático sobre un archivo sospechoso
- Examen forense de un documento de Microsoft Office sospechoso
- Ejecución de un análisis del comportamiento del sistema

Habilidades que Adquirirás

- Principales problemas que afectan a la informática forense
- Diferentes tipos de evidencia digital
- Proceso de investigación forense informática y sus fases
- Tipos de unidades de disco y sistemas de archivos
- Métodos y metodología de adquisición de datos
- Técnicas anti-forenses y sus contramedidas
- Recolección de información volátil y no volátil en sistemas Windows, Linux y Mac
- Fundamentos de la forensia de redes, correlación de eventos e investigación del tráfico de red
- Análisis forense de registros de servidores web y aplicaciones web
- Forensia en la Dark Web
- Investigación de delitos de correo electrónico
- Fundamentos de la forensia de malware y tipos de análisis de malware

¿A quién está dirigido?

- Estudiantes escolares, egresados, profesionales, personas que inician o desean cambiar de carrera, y equipos de TI / Tecnología / Ciberseguridad con poca o ninguna experiencia laboral previa.
- Estudiantes de secundaria que deseen iniciar tempranamente su trayectoria en ciberseguridad y dominar los fundamentos de la seguridad en línea.
- Estudiantes universitarios o de institutos interesados en prepararse para una carrera en ciberseguridad y complementar su formación en tecnologías de la información.
- Profesionales en actividad que deseen incursionar en el campo de la ciberseguridad y no sepan por dónde comenzar su proceso de formación.

Capacitación y Examen

Detalles de la capacitación:
Curso autoguiado, con videos bajo demanda dirigidos por instructores de nivel mundial y laboratorios prácticos.
Requisito previo:
No se requiere conocimiento previo en ciberseguridad ni experiencia laboral en TI.

Detalles del examen:

- Código del examen: 112-53
- Número de preguntas: 75
- Duración: 2 horas
- Formato de evaluación: Preguntas de opción múltiple

Características Principales

- Más de 11 horas de capacitación en video autoguiada de nivel premium
- 11 actividades de laboratorio en un entorno de simulación práctica
- Más de 750 páginas de material didáctico digital (ecourseware)
- Proyectos integradores (Capstone Projects) con desafíos reales tipo CTF
- Acceso al material del curso por un año y acceso a los laboratorios por seis meses
- Vale de examen supervisado (Proctored Exam Voucher) con validez de un año
- Incrementa tu valor profesional en el mercado laboral y potencia tu carrera
- Certificación del EC-Council reconocida a nivel mundial

Por qué la Serie Essentials de EC-Council es el programa de capacitación para principiantes más popular y de más rápido crecimiento para quienes inician o cambian de carrera

Más de **213 mil** estudiantes confían en la Serie Essentials de EC-Council.

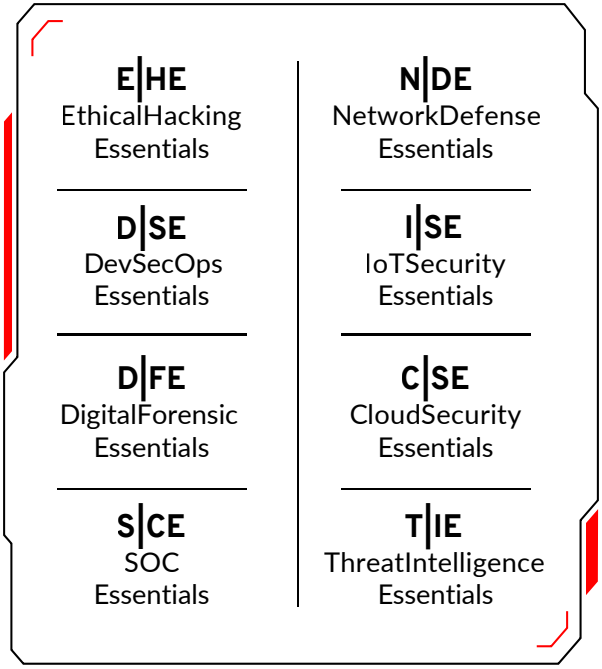
Más de **150** países

Más de **85** millones de minutos visualizados

Calificación promedio de **4.95** sobre 5.0

El **96 %** de los estudiantes dio 5 estrellas.

Aprende las habilidades fundamentales de ciberseguridad con la Serie de 8 Cursos Esenciales de EC-Council.



About EC-Council

El único propósito de EC-Council es desarrollar y fortalecer la profesión de ciberseguridad a nivel global.

Apoyamos a personas, organizaciones, instituciones educativas y gobiernos en la solución de los desafíos relacionados con la fuerza laboral mundial mediante el desarrollo y la gestión de programas educativos de ciberseguridad de clase mundial, junto con sus certificaciones correspondientes.

Asimismo, proporcionamos servicios de ciberseguridad a algunas de las empresas más grandes del mundo. Somos una entidad confiada por 7 de las 10 empresas del ranking Fortune 10, 47 de las 100 del Fortune 100, así como por el Departamento de Defensa de los Estados Unidos, la Comunidad de Inteligencia, la OTAN y más de 2,000 universidades, colegios y empresas de formación de prestigio internacional.

Nuestros programas se imparten en más de 140 países y han establecido el estándar global en educación en ciberseguridad.

Reconocidos principalmente por nuestro programa Certified Ethical Hacker (CEH), en EC-Council estamos comprometidos con la formación de más de 230,000 profesionales de la era digital, dotándolos de los conocimientos, habilidades y competencias necesarias para enfrentar y vencer a los adversarios del ciberespacio.

EC-Council fortalece las capacidades cibernéticas individuales y organizacionales mediante el programa Certified Ethical Hacker, seguido de una amplia gama de programas especializados, entre los que se incluyen:

- Certified Secure Computer User (CSCU)
- Computer Hacking Forensic Investigator (CHFI)
- Certified Security Analyst (ECSA)
- Certified Network Defender (CND)
- Certified SOC Analyst (CSA)
- Certified Threat Intelligence Analyst (CTIA)
- Certified Incident Handler (ECIH)
- Certified Chief Information Security Officer (CCISO)

Somos una organización acreditada por ANAB bajo la norma ISO/IEC 17024 y hemos recibido reconocimiento por parte del Departamento de Defensa de los Estados Unidos (DoD) bajo la Directiva 8140/8570, así como por organismos del Reino Unido como el GCHQ, CREST y otras entidades de autoridad global que influyen en toda la profesión.

Fundada en 2001, EC-Council cuenta con más de 400 colaboradores en todo el mundo y con diez oficinas internacionales ubicadas en Estados Unidos, Reino Unido, Malasia, Singapur, India e Indonesia.

Nuestras oficinas principales en Estados Unidos se encuentran en Albuquerque (Nuevo México) y Tampa (Florida).

Para más información, visita: www.eccouncil.org

New Horizons®
Centro de Capacitación

Digital Forensics Essentials

www.eccouncil.org