COURSE OVERVIEW

Course Name:
(CH-ECIH)
EC-Council Certified Incident Handler

COURSE DURATION: 3 Days

Gauteng:
3rd Floor, 34 Whitely Road
Melrose Arch
Johannesburg
2196

Gauteng:
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

Cape Town:
3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

Durban:
9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

087 941 5764
sales@impactful.co.za
impactful.co.za

INTRODUCTION

This latest iteration of EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

- Learn real world incident handling skills.
- Not only detect but manage security incidents.
- Maps to industry frameworks
- Method driven program.
- Learn all stages in incident handling.
- Think global employability.

DELIVERY METHOD

Our courses have flexible delivery options:

- In-person classroom training at the Impactful training facilities
  - Johannesburg, Durban, Cape Town
- Virtual instructor-led training
- Nationally: on-site at the client

IMPACTFUL
Powered by LRMG

TARGET AUDIENCE

- Penetration Testers
- Application Security Engineers
- Vulnerability Assessment Auditors
- Cyber Forensic Investigators/ Analyst and SOC Analyst
- Risk Assessment Administrators
- System Administrators/ Engineers Network Administrators
- Firewall Administrators and Network Managers/IT

PREREQUISITES

Mid-Level to High-Level Cyber Security Professionals with a minimum of 3 years of experience.
Information security professionals who want to enrich their skills and knowledge in the field of incident

COURSE OBJECTIVES

The ECIH program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats.
The comprehensive training program will make students proficient in handling as well as responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

- Principals, processes, and techniques for detecting and responding to security threats/
- breaches.
- Liaison with legal and regulatory bodies
- Learn to handle incidents and conduct assessments.
- Cover various incidents like malicious code, network attacks, and insider attacks.

COURSE CONTENT

Module 01: Introduction to Incident Handling and Response

- Overview of Information Security Concepts
- Understanding Information Security Threats and Attack Vectors
- Understanding Information Security Incident
- Overview of Incident Management
- Overview of Vulnerability Management
- Overview of Threat Assessment
- Understanding Risk Management
- Understanding Incident Response Automation and Orchestration
- Incident Handling and Response Best Practices
- Overview of Standards
- Overview of Cybersecurity Frameworks
- Importance of Laws in Incident Handling
- Incident Handling and Legal Compliance

Module 02: Incident Handling and Response Process

- Overview of Incident Handling and Response (IH&R) Process
- Preparation for Incident Handling and Response
- Incident Recording and Assignment
- Incident Triage
- Notification
- Containment
- Evidence Gathering and Forensics Analysis
- Eradication
- Recovery
- Post-Incident Activities

Module 03: Forensic Readiness and First Response

- Introduction to Computer Forensics
- Overview of Forensic Readiness
- Overview of First Response
- Overview of Digital Evidence
- Understanding the Principles of Digital Evidence Collection
  Collecting the Evidence
- Securing the Evidence
- Overview of Data Acquisition
- Understanding the Volatile Evidence Collection
- Understanding the Static Evidence Collection
- Performing Evidence Analysis
- Overview of Anti-Forensics

Module 04: Handling and Responding to Malware Incidents

- Overview of Malware Incident Response
- Preparation for Handling Malware Incidents
- Detecting Malware Incidents
- Containment of Malware
- Incidents Eradication of Malware Incidents
- Recovery after Malware Incidents
- Guidelines for Preventing Malware Incidents

Module 05: Handling and Responding to Email Security Incidents

- Overview of Email Security Incidents.
- Preparation for Handling Email Security Incidents
- Detection and Containment of Email Security Incidents
- Eradication of Email Security Incidents
- Recovery after Email Security Incidents

Module 06: Handling and Responding to Network Security Incidents

- Overview of Network Security Incidents
- Preparation for Handling Network Security Incidents
- Detection and Validation of Network Security Incidents
- Handling Unauthorized Access Incidents
- Handling Inappropriate Usage Incidents
- Handling Denial-of-Service Incidents
- Handling Wireless Network Security Incidents

Module 07: Handling and Responding to Web Application Security Incidents

- Overview of Web Application Incident Handling
- Web Application Security Threats and Attacks
- Preparation to Handle Web Application Security Incidents
- Detecting and Analyzing Web Application Security Incidents
- Containment of Web Application Security Incidents
- Eradication of Web Application Security Incidents
- Recovery from Web Application Security Incidents
- Best Practices for Securing Web Applications

Module 08: Handling and Responding to Cloud Security Incidents

- Cloud Computing Concepts
- Overview of Handling Cloud Security Incidents
- Cloud Security Threats and Attacks
- Preparation for Handling Cloud Security Incidents
- Detecting and Analyzing Cloud Security Incidents
- Containment of Cloud Security Incidents
- Eradication of Cloud Security Incidents
- Recovering from Cloud Security Incidents Best Practices Against Cloud-based Incidents

Module 09: Handling and Responding to Insider Threats

- Introduction to Insider Threats
- Preparation for Handling Insider Threats
- Detecting and Analyzing Insider Threats
- Containment of Insider ThreatsEradication of Insider Threats
- Recovery after Insider Attacks
- Best Practices Against Insider Threats

Associated Certification & Exam

Exam title: EC-Council Certified Incident Handler
Exam code: 212-89
Number of questions: 100
Duration: 4 Hours
Availability: EC-Council Exam Portal
Test Format: Multiple Choice
Passing Score: 70%