APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

EC-Council Certified Incident Handler (ECIH) Training

EC-Council Authorized Training · Applied Technology Academy

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.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**3 Days**	**1 year: Security**	**$70,000**	**Yes**

Course Overview

Following a rigorous development which included a careful Job Task Analysis (JTA) related to incident handling and incident first responder jobs, EC-Council developed a highly interactive, comprehensive, standards-based, intensive 3-day training program and certification that provides a structured approach to learning real-world incident handling and response requirements.

- Understand the key issues plaguing the information security world
- Learn to combat different types of cybersecurity threats, attack vectors, threat actors and their motives
- Learn the fundamentals of incident management including the signs and costs of an incident

Understand the fundamentals of vulnerability management, threat assessment, risk management, and incident response automation and orchestration

- Master all incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Decode the various steps involved in planning an incident handling and response program
- Gain an understanding of the fundamentals of computer forensics and forensic readiness

Comprehend the importance of the first response procedure including evidence collection, packaging, transportation, storing, data acquisition, volatile and static evidence collection, and evidence analysis

Understand anti-forensics techniques used by attackers to find cybersecurity incident cover-ups

Course Outline

- **Module 01: Introduction to Incident Handling and Response**
- **Module 02: Incident Handling and Response Process**
- **Module 03: Forensic Readiness and First Response**
- **Module 04: Handling and Responding to Malware Incidents**

- **Module 05: Handling and Responding to Email Security Incidents**
- **Module 06: Handling and Responding to Network Security Incidents**
- **Module 07: Handling and Responding to Web Application Security Incidents**
- **Module 08: Handling and Responding to Cloud Security Incidents**
- **Module 09: Handling and Responding to Insider Threats**

Intended Audience

This course will significantly benefit incident handlers, risk assessment administrators, penetration testers, cyber forensic investigators, venerability assessment auditors, system administrators, system engineers, firewall administrators, network managers, IT managers, IT professionals and anyone who is interested in incident handling and response.

Prerequisites

E|CIH is a specialist-level program that caters to mid-level to high-level cybersecurity professionals. In order to increase your chances of success, it is recommended that you have at least 1 year of experience in the cybersecurity domain. E|CIH members are ambitious security professionals who work in Fortune 500 organizations globally.

Follow-On Courses

- EC-Council Certified Ethical Hacker (CEH)
- Disaster Recovery Professional (EDRP)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.