Certified Incident Handling Engineer

The Certified Incident Handling Engineer certification course is designed to help Incident Handlers, System Administrators, and Information Security professionals understand how to plan, create, and utilize their Incident Detection and Response systems to quickly and efficiently respond to potential threats. In the realm of information security incidents, it's not a matter of "if," but "when." Preparation and preemptive training can make the difference between experiencing a security incident and being subjected to a disastrous event. Students will receive in-depth training to learn methodologies and exploits utilized by malicious actors, the latest attack vectors, and industry best practices for developing procedures and teams to safeguard against them. This course also provides numerous hands-on laboratory exercises that focus on topics such as reconnaissance, vulnerability assessments using Nessus, network sniffing, web application manipulation, and malware identification.

Duration: 5 Days CPE Credits: 40 Course Fee: $3,500

Learning Objectives

01) Overview: Incident Handling and Incident Response
02) Overview: The Attack Life Cycle
03) Threats, Vulnerabilities, and Exploits
04) Overview: Technology and Cyber Crime Topology
05) Preparation and Development Phase
06) Computer Security Incident Response Teams
07) Initial Response and Investigative Phase
08) Overview: Network Infrastructure Services
09) Investigating Windows Systems
10) Data Analysis Methodologies
11) NTFS and File System Analysis
12) Log Analysis and SIEM Architecture
13) Artifact Identification and Analysis
14) Overview: Data Collection and Forensic Duplication
15) Investigating Application Data
16) Incident and Compromise Containment
17) Malware Triage and Analysis (Static and Dynamic)
18) Incident Eradication Methodologies
19) System and Operational Recovery Strategies
20) Incident Documentation and Remediation Strategies

Hardcopy Training Materials	Digital Training Materials
Course Text / Workbook	Course Text / Workbook
Course Lab Manual	Course Lab Manual
Supplemental Handout	Course Video Series
Text: Key Security Concepts	Exam Prep Study Guide
Exam Prep Study Guide	Exam Simulator
USB Drives	CPE Credit Certificate

Certification examination is included in the course fee.

The Certified Incident Handling Engineer course is a component of the career progression track that supports the following Categories, Specialty Areas, and Work Roles as defined by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework:

Exploitation Analyst
(AN-EXP-001)

Law Enforcement Forensics Analyst
(IN-FOR-001)

Cyber Intel Planner
(CL-OPL-001)

Cyber Crime Investigator
(IN-INV-001)

All Source – Collection Manager
(CO-CLO-001)

Cyber Defense Forensics Analyst
(IN-FOR-002)

Average Yearly Salary:
$74,507

Phase2 Advantage | **Phone**: (912) 244-0394 | **Email**: info@phase2advantage.com