Certified Incident Handler (ECIH)

Why ECIH Certifications ?

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.

Training Solutions:

√ Offline Classroom Instructor-Led Training in our labs or onsite Locations.

√ Virtual Instructor-Led Training Via Virtual Video Conferencing Tools.

Why Learners Prefer CLS as their Training Services provider ?

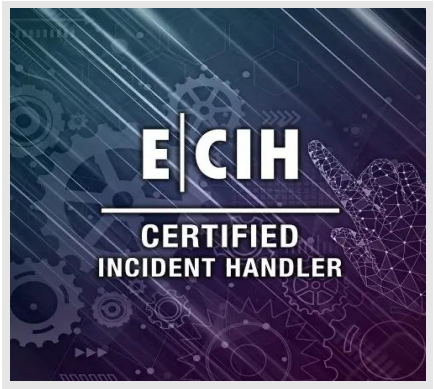
■ Premuim Training Services Accredited from Global Technology Vendors.

■ Best Rated Experts & Certified Trainers in Egypt.

■ Official Training Hours, Practice Labs, Hands-on Learning.

■ CLS Training Classrooms are designed with High Edge PCs and Training Facilities.

■ Return on Training Investment is Guaranteed to boost performance.



- Overview:

Certified Incident Handler (ECIH) Training and certification course will address the needs of the professionals who want to get equipped with the principles and knowledge for detecting and responding to the current security incidents and threats emerging in an information system. The course has been structured to equip professionals in creating incident handling codes, learning about laws and policies for incident handling and differentiating between various types of incidents such as network security incidents, malicious code incidents, and insider attack incidents.

- ECIH 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

Course Objectives:

- 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.

- Audience Profile :

Who Needs ECIH Certification?

- Incident handlers
- Risk assessment administrators
- Penetration testers
- Cyber forensic investigators
- Venerability assessment auditors
- System administrators and engineers
- Firewall administrators
- Network managers
- IT managers

Prerequisities:

- One year of experience managing Windows/Unix/Linux systems or have equivalent knowledge and skills
- Good understanding of common network and security services is required