BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Certified Incident Handler (CIH)

Course Introduction

The **Certified Incident Handler (CIH)** program is designed to equip professionals with the core competencies to detect, respond to, and mitigate cyber incidents across a range of environments. In a world of escalating cyber threats, incident handling is no longer a luxury, it’s a necessity. This intensive, hands-on course empowers participants with the latest methodologies in handling network intrusions, data breaches, ransomware, and advanced persistent threats (APTs). Through real-world case studies, frameworks, and simulation exercises, learners gain the confidence to manage incident lifecycles and reduce business risks with professionalism and speed.

Target Audience

- Incident Response Team Members and Managers
- Security Operations Center (SOC) Analysts
- Cybersecurity Engineers and Consultants
- Network Administrators and Security Architects
- Risk Management and IT Compliance Professionals
- Forensics and Threat Intelligence Analysts

Learning Objectives

- Understand the principles, phases, and frameworks of incident handling
- Recognize types and categories of cybersecurity incidents
- Prepare and implement an Incident Response Plan (IRP)
- Investigate and contain malware, insider threats, and DoS/DDoS attacks
- Apply forensic techniques in evidence collection and analysis
- Coordinate post-incident recovery, documentation, and lessons learned
- Communicate with internal/external stakeholders effectively during incidents

Course Outline

- **DAY 01**

  Introduction to Incident Handling & Response Frameworks

  - Understanding incident types and classification
  - Cyber threat landscape: threats, actors, vectors
  - Legal and ethical considerations
  - Incident response frameworks: NIST, ISO, SANS PICERL
  - Building a Computer Security Incident Response Team (CSIRT)

- **Day 02**

  Preparation & Detection

  - Crafting an Incident Response Plan (IRP)
  - Asset identification and risk prioritization
  - SIEM and log correlation basics
  - Indicators of Compromise (IoCs) and Indicators of Attack (IoAs)
  - Threat detection and early warning systems

- **Day 03**

Containment, Eradication, and Recovery

- Incident containment strategies (short-term & long-term)
- Malware containment and remediation workflows
- Root cause analysis and attack vector tracing
- Restoring systems and ensuring clean recovery
- Managing cloud and hybrid environment incidents

- **Day 04**

Digital Forensics & Investigation

- Introduction to digital evidence and forensic procedures
- Live system and memory acquisition
- Disk and file system forensics
- Evidence chain of custody and preservation
- Hands-on case analysis and artifact interpretation

- **Day 05**

Post-Incident Handling and Capstone Exercise

- Reporting, documentation, and audit readiness
- Conducting post-mortem and lessons-learned workshops
- Communication strategy during and after incidents
- Hands-on simulated cyber incident (end-to-end response)
- Final assessment and feedback

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
Dec. 7, 2025	Dec. 11, 2025	5 days	4250.00 $	KSA - Riyadh
July 14, 2025	July 18, 2025	5 days	4250.00 $	UAE - Dubai