*Brought to you by* **iEnabler – THE IT ENABLING COMPANY**

# EC Council Certified Incident Handler

**(Version 2)**

**What is an Incident Handler?**

Incident handler is a term used to describe the activities of an organization to identify, analyze, and correct hazards to prevent a future reoccurrence. These incidents within a structured organization are normally dealt with by either an Incident Response Team (IRT) or an Incident Management Team (IMT). These teams are often either designated beforehand or during the event and are placed in control of the organization while the incident is dealt with, in order to retain business processes.

**Course Objective :**

To enable individuals and organizations with the ability to handle and respond to different types of cybersecurity incidents in a systematic way. To ensure that organization can identify, contain, and recover from an attack. To reinstate regular operations of the organization as early as possible and mitigate the negative impact on the business operations. To be able to draft security policies with efficacy and ensure that the quality of services is maintained at the agreed levels. To minimize the loss and after-effects breach of the incident. For individuals: To enhance skills on incident handling and boost their employability.

**Prerequisite:**

- The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old
- Basic computer literacy & Basic PC operating system navigation skills
- One year of work experience in the Information Security domain will be an advantage

**Target 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.**

**Training Methodology:**

This course includes official courseware, 1 certification exam voucher and iLabs/online labs (6 months access).

**Certificate Of Attendance:**

Certificate Of Attendance will be awarded to participants completing the course achieving minimum 75% attendance.

| EC Council Certified Incident Handler v2 Certification Exam | Training Duration: | Course Fee: |
|---|---|---|
| **ECIH Exam Code : 212-89**<br>Exam Duration : 3 hrs<br>Format : Multiple Choice/100 Questions | Full-Time : 3 Weekdays<br>Time : 9.30am – 5.30pm | Normal Course Fee : S$1299<br>Regn Fee : S$30 and Exam Proctor Fee : S$50<br>* Course fee includes 1 ECIH Exam voucher<br>All fees subject to GST 7%. |

## DETAILED COURSE OUTLINE

### 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*
- *Step 1: Preparation for Incident Handling and Response*
- *Step 2: Incident Recording and Assignment*
- *Step 3: Incident Triage*
- *Step 4: Notification*
- *Step 5: Containment*
- *Step 6: Evidence Gathering and Forensics Analysis*
- *Step 7: Eradication*
- *Step 8: Recovery*
- *Step 9: 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 Threats*
- *Eradication of Insider Threats*
- *Recovery after Insider Attacks*
- *Best Practices Against Insider Threats*



IT Enabler Consultancy Pte Ltd (Co Reg No. 200211025Z)
35 Selegie Road #09-06 Parklane Shopping Mall Singapore188307 | Tel: 6333 4843 | Fax: 6333 4883 | www.ienabler.com.sg