

---

## Certified Incident Handling Engineer

---

**Course Title:** C)IHE

**Duration:** 5 days, 40 Hrs

**Class Format Options:**

Instructor-led  
classroom Training

**Who Should Attend:**

- Incident Handlers
- System Administrators
- Security Consultants
- IT Departments

**Prerequisites:**

A general knowledge of  
information systems  
and security

**Provided Materials:**

Student Workbook  
Security Reference Manual

**Certification Exam:**

C)IHE: Certified Incident  
Handling Engineer

### Course Overview

The Certified Incident Handling Engineer course is designed to help incident handlers, system administrators, and general security engineers understand how to plan, create, and utilize their systems in order to prevent, detect, and respond to security breaches. Every business connected to the internet is getting probed by hackers trying to gain access. The ideal situation is to prevent this from happening, but realistically every business needs to know how to detect and resolve security breaches. Certified Incident Handlers are prepared to do handle these situations effectively.

Students will learn common attack techniques, vectors, and tools used by hackers, so that they can effectively prevent, detect, and respond against them. This course is ideal for those who lead incident handling teams or are part of an incident handling team.

Furthermore, students will enjoy numerous hands-on laboratory exercises that focus on topics, such as reconnaissance, vulnerability assessments, network sniffing, web application manipulation, malware and using Netcat plus several additional scenarios for both Windows and Linux systems. The 20 hours of experience in our labs is what will put you ahead of the competition and set you apart as a leader in incident handling.

---

### Upon Completion

Students will have knowledge to:

- Detect security threats, risk, and weaknesses
  - Plan for prevention, detection, and response to security breaches
  - Accurately report on their findings from examinations
-

---

## Exam Information

The Certified Incident Handling Engineer exam is taken online through Mile2's Assessment and Certification System (MACS), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions.

---

## Course Content

**Module 1:** Introduction

**Lab 01:** Wireshark

**Module 2:** Threats, Vulnerabilities, and Exploits

**Lab 02:** Netstat

**Module 3:** Preparation

**Lab 03:** Netcat

**Module 4:** Identification and Initial Response

**Lab 04:** Cyber Attacks

**Lab 05:** Ticketing System

**Module 5:** Containment

**Lab 06:** SysInternals Suite

**Module 6:** Eradication

**Lab 07:** First Response Lab Scenario

**Module 7:** Recovery

**Lab 08:** System Examination and Handling

Malware

**Module 8:** Follow-Up

**Lab 09:** Malware Removal

**Lab 10:** Final Scenario

---