

Certified Incident Handling Engineer

KEY DATA

Course Name: Certified Incident Handling Engineer

Duration: 5 days

Language: English

Format:

Instructor-led
Live Virtual Training

Prerequisites:

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Basic Knowledge of Linux is essential

Student Materials:

- Student Workbook
- Student Lab Guide
- Student Exam prep guide

Certification Exam:

- CIHE- Certified Incident Handling Engineer
- Covers GCIH- GIAC Certified Incident Handler

CPEs: 40

COURSE OVERVIEW

The Certified Incident Handling Engineer vendor neutral certification is designed to help Incident Handlers, System Administrators, and any General Security Engineers understand how to plan, create and utilize their systems in order to prevent, detect and respond to attacks.

In this in-depth training, students will learn step-by-step approaches used by hackers globally, the latest attack vectors and how to safeguard against them, Incident Handling procedures (including developing the process from start to finish and establishing your Incident Handling team), strategies for each type of attack, recovering from attacks and much more.

Furthermore, students will enjoy numerous hands-on laboratory exercises that focus on topics, such as reconnaissance, vulnerability assessments using Nessus, network sniffing, web application manipulation, malware and using Netcat plus several additional scenarios for both Windows and Linux systems.

BENEFITS OF CIHE COURSE

Graduates of the mile2 Certified Incident Handling Engineer training obtain real world security knowledge that enables them to recognize vulnerabilities, exploit system weaknesses and help safeguard against threats. This course covers the same objectives as the SANS® Security 504 training and prepares students for the GCIH® and CIHE certifications

Incident Handling Career



All Combos Include:

- Online Video
- Electronic Book
(Workbook/Lab guide)
- Exam Prep Questions
- Exam
- Cyber Range



ACCREDITATIONS



NICCS™

NATIONAL INITIATIVE FOR
CYBERSECURITY CAREERS AND STUDIES



is ACCREDITED by the NSA CNSS 4011-4016
Is MAPPED to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

UPON COMPLETION

Upon completion of the Certified Incident Handling Engineer course, students will be able to confidently undertake the CIHE certification examination (recommended). Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever changing security world. This course offers up-to-date proprietary laboratories that have been researched and developed by leading security professionals from around the world.

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. The cost is \$400 USD and must be purchased from Mile2.com.



OUTLINE

- Module I - Incident Handling Explained**
- Module II - Threats, Vulnerabilities and Exploits**
- Module III - Preparation**
- Module IV - First Response**
- Module V - Containment**
- Module VI - Eradication**
- Module VII - Recovery**
- Module VIII - Follow-Up**

LAB OUTLINE



- Module One Lab - Attacks Under the Microscope**
- Module Two Lab - Ticketing System**
- Module Three Lab - SysInternals Suite**
- Module Four Lab - Examine System Active Processes Running Services**
- Final Scenario - 4 hours**

ADVANCED LABS

- Advanced Module 1 Lab - Computer Security Incident Response Team**
- Advanced Module 2 Lab - Log File Analysis: Analyzing a Shell History File**
- Advanced Module 2 Lab - Log File Analysis: Searching attacks in your Apache logs**
- Advanced Module 3 Lab - Rootkits and Botnets: How to Crash your Roommate's Windows 7 PC**
- Advanced Module 3 Lab - Rootkits and Botnets: Exploit MS Word to Embed a Listener**
- Appendix Labs**
- Advanced Module 3 Lab - Rootkits and Botnets: Stuxnet Trojan**
- Advanced Module 3 Lab - Rootkits and Botnets: Zeus Trojan**
- Advanced Module 4 Lab - Artifact Analysis: Processing and Storing Artifacts**

Introduction

Courseware Materials
Who is this class for?
What is the purpose of this course?

What information will be covered?
The Exam

Module I - Incident Handling Explained

Security Events
Logs
Alerts
What is an Incident?
Security Incident
Indication of Compromise

What is Incident Handling?
Difference between IH and IR
Common Tools
IPS vs WAF
SOC
Six Step Approach to Incident Handling

Module II - Threats, Vulnerabilities and Exploits

Overview
Vulnerabilities
Exploits

Threat
Incident Classification

Module III – Preparation

Overview
Policies & Procedures
The Team
Identify Incident Handling Team
Roles of the Incident Handling Team
IH Team Makeup
Team Organization
Incident Communication
Incident Reporting
Incident Response Training and Awareness
Underlining Technologies

Anti-virus
SEIM
User Identity
Ticketing Systems
Digital Forensics
eDiscovery
Data Backup and Recovery
Underlining Technologies
Technical Baselines
System Hardening
Summary

Module IV - First Response

Overview
Responder Toolkit
Responder's System
What to look for
Attention
Volatility
First things first
Review
Goal
Challenges
Categorize Incidents

Incident Signs
Basic Steps
Receive
Examples of Electronic Signs
Examples of Human Signs
Analyze
Analysis
Incident Documentation
Incident Prioritization
Incident Notification

Module V – Containment

Overview
 Containment
 Goals
 Delaying Containment
 Choosing a Containment Strategy
 On-site Response
 Secure the Area

Conduct Research
 Procedures for Containment
 Make Recommendations
 Establish Intervals
 Capture Digital Evidence
 Change Passwords

Module VI – Eradication

Overview
 Eradication
 Goals

Procedures for Eradication
 Determine Cause
 Procedures for Eradication

Module VII – Recovery

Overview
 Recovery

Goals
 Procedure for Recovery

Module VIII - Follow-Up

Overview
 Follow-up

Goals
 Procedures of Follow-up

DETAILED LAB OUTLINE



Introduction

Lab Resources
 Knowing your way around VMware Player.

Module One - Attacks Under the Microscope

Lab objectives
 Wireshark
 Why Wireshark?
 Running Wireshark
 Starting Wireshark
 User interface
 Filters
 Netstat
 Command
 Options

Examples
 Netcat
 Cyber Attacks
 Understanding the hacking methodology
 IP Space Scanning
 Port Scanning
 Network Based Attacks
 Web Application Based Attacks
 Host Based Attacks

Module Two - Ticketing System

Introduction
 Ticketing System Components
 Tickets:
 Queues:

System Functionality
 System login



Ticket Creation
Ticket Correspondence
Ticket Priority Escalation
Ticket Assignment
Request Tracker for Incident Response – RTIR
Normal user role:

Incident Handling
Role:
Viewing unlinked Incident Reports:
Create an Incident
Linking Incident Reports to an incident:
Starting an Investigation

Module Three Lab - SysInternals Suite

Introduction
Getting Sysinternals.
Usage Guide
Process Explorer
Process Monitor
Autoruns

PsTools
Disk Utilities
Security Utilities
Network and Communication utilities.
First Response Lab Scenario

Module Four Lab - Examine System Active Processes and Running Services

Examine Startup Folders
The Local Registry
The IOC Finder – Collect

IOC Finder – Generate Report
Malware Removal

Final Scenario - 4 hours

ADVANCED LABS

Advanced Module 1 – Computer Security Incident Response Team

Advanced Module 2 – Log File Analysis: Analyzing a Shell History File

Advanced Module 2 – Log File Analysis: Searching attacks in your Apache logs

Advanced Module 3 - Rootkits and Botnets: How to Crash your Roommate's Windows 7 PC

Advanced Module 3 – Rootkits and Botnets: Exploit MS Word to Embed a Listener

Appendix Labs

Advanced Module 3 – Rootkits and Botnets: Stuxnet Trojan

Advanced Module 3 – Rootkits and Botnets: Zeus Trojan

Advanced Module 4 – Artifact Analysis: Processing and Storing Artifacts