

CERTIFIED INCIDENT HANDLING ENGINEER

KEY DATA

Course Title: C)IHE

Duration: 5 days

CPE Credits: 40

Class Format Options:

Instructor-led classroom
Live Virtual 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

CGIH: GIAC Certified Incident Handler

Certification Track:

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 using Nessus, 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
- Be ready to sit for the C)IHE Exam

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 \$300 USD and must be purchased from the store on Mile2.com.

The GIAC Certified Incident Handler exam is another certification for incident handling professionals that this course has more than prepared you to pass. We

Also available as:

**LIVE VIRTUAL
TRAINING**

**Attend live classes from
anywhere in the world!**

**Visit Mile2.com
for more information**

strongly recommend the more advanced C)IHE exam by Mile2, please consult your instructor if you have any further questions. The exam is available for purchase through giac.org

COURSE CONTENT

Module 1: Introduction
Module 2: Threats, Vulnerabilities, and Exploits
Module 3: Identification and Initial Response
Module 4: RTIR
Module 5: Preliminary Response
Module 6: Identification and Initial Response
Module 7: Sysinternals
Module 8: Containment
Module 9: Eradication
Module 10: Follow-Up
Module 11: Recovery
Module 12: Virtual Machine Security
Module 13: Malware Incident Response

Lab 1: Netcat (Basics of Backdoor Tools)
Lab 2: Exploiting and Pivoting our Attack
Lab 3: Creating a Trojan
Lab 4: Capture FTP Traffic
Lab 5: ARP Cache Poisoning Basics
Lab 6: ARP Cache Poisoning - RDP
Lab 7: Input Manipulation
Lab 8: Shoveling a Shell
Lab 9: Virus Total
Lab 10: Create Malware using SET
Lab 11: The Trojans
Lab 12: Examine System Active Processes and Running Services
Lab 13: Examine Startup Folders
Lab 14: The Local Registry
Lab 15: The IOC Finder – Collect
Lab 16: IOC Finder – Generate Report
Lab 17: Malware Removal

DETAILED MODULE DESCRIPTION

Module 1 - Introduction

Introduction
Courseware Materials
Who is this class for?
What is the purpose of this course?
What information will be covered?
The Exam
What is Incident Handling?
What is a security event?
Common Security Events of Interest
What is a security incident?
Why Incident Response?
Common Goals of Incident Response Management
What is an incident response plan?
When does the plan get initiated?
Six Step Approach to Incident Handling
Course Details

Module 2: Threats, Vulnerabilities and Exploits

Overview
Malware
Botnets:
Attacks: IP Spoofing
CM: Ingress Filtering
ARP Cache Poisoning
ARP Normal Operation
ARP Cache Poisoning
ARP Cache Poisoning (Linux)
Countermeasures
What is DNS spoofing?
Tools: DNS Spoofing
Session Hijacking
Session Hijacking
4 Methods continued
Methods to Prevent Session Hijacking
Buffer Overflows
Buffer Overflow Definition
Evading The Firewall and IDS
Evasive Techniques
Firewall – Normal Operation
Evasive Technique -Example
Attack: Phishing
Social Engineering
SET
SET
Attack: Denial of Service
Attack: Insider Threat
Wireless Attacks

Software Attacks
Vulnerability Assessment
Penetration Testing
Exploitation
Review

Module 3: Preparation

Overview
Senior Management Support
Policies and Procedures
The Team
Identify Incident Response Team
Roles of the Incident Response Team
IRT Team Makeup
Team Organization
Incident Communication
Incident Reporting
Incident Response Training and Awareness
Underlining Technologies
Anti-virus
Virus Total
Demo
SEIM
User Identity
Ticketing System
Instructor Demo
RTIR Features and Demo
Digital Forensics
eDiscovery
Data Backup and Recovery
Underlining Technologies
Technical Baselines

Module 4: RTIR

Overview
What is Request Tracker?
RT Cake
Why Use Request Tracker?
Who Uses Request Tracker?
RT Components
Tickets
Queues
What is RTIR?
RTIR Components
RTIR Workflow
File an Incident Report
Create an Incident
Launch an Investigation
Initiating a Block
RTFM

Module 5: Preliminary Response

Overview
Responder Toolkit
Responder's System
What to look for
Attention
Volatility
First things first
Windows Log Events
Windows Log Events
Windows Services
Windows Network Usage
Windows Network Usage
Windows Scheduled Tasks
Windows Accounts
Windows Tools
Linux Log Events
Linux Log Events
Linux Processes
Linux Network Usage
Linux Scheduled Tasks
Linux Accounts
Linux Files
Linux Files
Linux Tools
Review

Module 6: Identification and Initial Response

Goal
Challenges
Categorize Incidents
Incident Signs
Three Basic Steps
Receive
Examples of Electronic Signs
Examples of Human Signs
Analyze
Analysis
Incident Documentation
Incident Prioritization
Incident Notification

Module 7: Sysinternals

Overview
Introduction
Where to get them
Process Explorer
Procexp Features
Process Monitor
Promon Filtering engine
Autoruns

PsTools
Psexec
Disk Utilities
Disk Monitor
Diskview
Security Utilities
Sigcheck
TCPView

Module 8: 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 9: Eradication

Overview
Eradication
Goals
Procedures for Eradication

Module 10: Follow-up

Overview
Follow-up
Goals
Procedures of Follow-up

Module 11: Incident-handling recovery

Overview
Recovery
Goals
Procedure for Recovery

Module 12: Virtual Machine Security

Virtualization Components
Virtualization Attacks
Identifying VMs

Module 13: Malware Incident Response

Agenda
History of Malware
Computer Viruses

Compiled Viruses
Interpreted Viruses
Computer Worms
Trojans
Backdoors
Instructor Demo
Executable Wrappers
Instructor Demo
Rootkits
Instructor Demo
Mobile Code
Blended Attacks
Cookies
Browser Plug-ins
E-mail Generators
Key Loggers
Instructor Demo
Review
Agenda
The Policy
Policy Considerations
User Awareness
Instructor Demo
Vulnerability Vs. Threat Mitigation
Patch Management
Account Security
Host Hardening
Host Hardening - Examples
Anti-virus Software
Instructor Demo
Spyware Detection and Removal
Intrusion Prevention Systems
Firewall and Routers
Application Security Settings
Instructor Demo
Review
Agenda
The Decision Flow
Confirm the Infection
Determine Course of Action Decision Flow
Clean the System Decision Flow
Attempt to Clean the System
Clean the System
Attempt to Restore System State
Rebuild the System Decision Flow
Rebuild the System
Conduct a Post-Attack Review
Review