CIHE
Certified Incident Handling Engineer

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.

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.

Course Length

5 days

Format

- Instructor-led classroom
- Live Virtual Training.

Prerequisites

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

Student Materials

- Student Workbook
- Student Lab Guide
- Exam Prep guide

Certification Exam

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

Course Contents

- Module 1 - Incident Handling Explained
- Module 2 - Threats, Vulnerabilities, and Exploits
- Module 3 – Preparation
- Module 4- First Response
- Module 5 – Containment
- Module 6 – Eradication
- Module 7 – Recovery
- Module 8 - Follow-Up
- Module 9 - Advanced Computer Security Incident Response Team
- Module 10 - Advanced - Log File Analysis
- Module 11 - Advanced - Malware, Rootkits, and Botnets
- Module 12 - Advanced - Artifact Analysis

Lab Outline

- Lab 1 - Tools Introduction
- Lab 2 - Cyber Attacks - Networking
- Lab 3 - Cyber Attacks - Web Application
- Lab 4 - Cyber Attacks - Viruses
- Lab 5 - Lab 5 Ticketing System
- Lab 6 - SysInternals Suite

- Lab 7 - Creating and Managing a CSIRT Action Plan
- Lab 8 - Log Analysis
- Lab 9 - Exploits and DoS
- Lab 10 - Stuxnet Trojan: Memory Analysis with Volatitlity
- Lab 11 - Find the hack(s) lab