SecureIOT Academy Sdn. Bhd.

A subsidiary of SysArmy

Certified Incident Handling Engineer

This 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. By the end of the course, students will obtain real world security knowledge that enables them to recognize vulnerabilities, exploit system weaknesses and help safeguard against threats.

Venue : Suite 12-12, Level 12th, Wisma Zelan No1, Jalan Tasik Permaisuri 2, Bandar Tun Razak, 56000, Kuala Lumpur.

Key Information

Duration: 5 days

Class Format Options:

- Instructor-led classroom

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 Material:

- Student Workbook
- Student Lab Guide
- Prep Guide

CPEs: 40

Who Should Attend:

- Incident Handlers
- System Administrators
- General Security Engineers

Certification:

1. CIHE – Certified Incident Handling Engineer
2. Covers GCIH –GIAC Certified Incident Handler

Please contact
commercial@sysarmy.net
for more information

What You Will Learn?

Course Content

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

Lab Content

Lab 1: Attack Under the Microscope
Lab 2: Ticketing System
Lab 3: SysInternals Suite
Lab 4: Examine System Active Processes Running Services
Lab 5: Final Scenario: 4 Hours

Advanced Labs

Lab 1: Computer Security Incident Response Team
Lab 2: Log File Analysis: Analyzing a Shell History File
Lab 3: Log File Analysis: Searching Attacks in your Apache Logs
Lab 4: Rootkits and Botnets: How to Crash your Roommate's Windows 7 PC
Lab 5: Rootkits and Botnets: Exploit MS Word to Embed a Listener
Lab 6: Rootkits and Botnets: Stuxnet Trojan
Lab 7: Rootkits and Botnets: Zeus Trojan
Lab 8: Artifact Analysis: Processing and Storing Artifacts

ACCREDITATIONS

CNSS

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

mile2

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)**