INTERNATIONAL CYBERSECURITY INSTITUTE

Course Outline: Digital Forensics, Incident Response, and Threat Hunting

Certification: ICSI | CDFE Certified Digital Forensics Examiner

Required Courses and Exam:

Course	Exam
Digital Forensics, Incident Response, and Threat Hunting	CDFE

Accreditation: University of Central Lancashire (MSc Cybersecurity Credits: 20)

Duration: 5 Days

Candidate Prerequisites:

Familiarity with Windows and Linux Operating System and basic knowledge digital forensics principles.

Overview:

This course provides a holistic view of how Incident Response is implemented in the real world, including Incident Response preparation, acquiring and analyzing digital forensic images and analyzing host and network data. Malware analysis, Threat intelligence and report creation are also included.

Who Should Attend:

Security Professionals seeking to acquire basic to intermediate knowledge in Digital Forensics and Incident Response.

What is Included:

- eBook
- Lab Guide
- 6 months 24x7 remote access to a virtual lab
- 1 exam voucher - Online Exam Proctoring
- Certificate of Attendance (Digital)

INTERNATIONAL CYBERSECURITY INSTITUTE

Module 1: Incident Response

- Introduction to Incident Response
- Incident Response Framework and response plan
- Incident Response Playbook

Module 2: Introduction to Digital Forensics

- Laws and Regulations
- Digital Forensics Process

Module 3: Collecting Network Evidence

- Log Configuration Management
- Network Device Evidence (SIEM)
- Packet Capture (Wireshark, WinPcap & RawCap)

Module 4: Capturing Evidence from Hosts Systems

- Capturing Volatile Data (FTK Imager)
- Remote Acquisition
- Capturing Virtual Machine Memory
- Non Volatile Data

Module 5: Forensic Imaging

- Preparation
- Imaging Types

Module 6: Analyzing Network Evidence

- Analyzing network packets with Wireshark
- Network log analysis

Module 7: Memory Analysis

- Memory Investigation Approach
- Analyzing Network Connections

Module 8: Storage Analysis

- Commercial Platforms
- Storage analysis using Autopsy

Module 9: Incident & Forensic Reporting

- Documentation
- Creating Reports

Module 10: Malware Analysis

- Malware Analysis Overview
- Static vs Dynamic Analysis

Module 11: Threat Intelligence

- Threat Intelligence Overview
- Threat Intelligence Methodology
- Sources and Platforms

Exam:

The CDFE practical certification exam covers material from all 11 modules. The exam duration is 2.5 hours. Passing Grade = 70%.