Digital Forensics and Incident Response (DFIR)

Duration: 3 Days

COURSE DESCRIPTION

This course covers the standard of forensic investigation and analysis, and covers phases of incident handling and responding. In the first part, it introduces techniques and tools for digital evidence acquisition, investigation and analysis. In the second part, it covers phases of incident handling and responding; Preparation, Identification, Containment, Eradication, and Recovery.

The course targets teams who work in SOC, incident handlers, cybersecurity officers, system administrators, security analysts, and forensic investigators. The material requires some background of IT knowledge, computer network and tools, and some of cybersecurity background

COURSE OBJECTIVE

- To explain the process of incident handling and response
- To introduce steps of an effective recovery and remediation process
- To explain and demonstrate computer evidence handling techniques and tools for Windows and Linux

COURSE OUTLINE

- To introduce standard of forensic investigation and analysis
- To explain digital evidence acquisition techniques and tools for gathering evidences from computer and network system
- Digital forensic recovery and analysis techniques
- The Incident Handling and Response Process – Introduction to the cyber attack, the steps of an effective incident response process, and the recovery and remediation process.
- Demonstration and Hand-on Exercises for DFIR

PREREQUISITES

- General knowledge of computers and operating system.
- Some experience in computer programming languages.
- Background in Computer Network and Tools such as Wireshark.
- Some basic of Linux command.

WHO SHOULD ATTEND

A system administrator, a security analyst, and a forensic investigator with some background in conducting forensic analysis, network traffic analysis, log analysis, and security assessments. It is also well suited for those managing CIRT / incident response teams, or those in roles that require oversight of forensic analysis and other investigative tasks.

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th