Certified Cybercrime Threat Investigator Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Over this five-day National Cyber Security Center (NCSC) assured course, learners will develop the skills to monitor networks, detect and respond to an attack, and handle incidents and threats effectively. The course covers how to correlate threats, perform threat hunting, acquire evidence, and conduct forensic investigation to reconstruct attacks. Learners will also be introduced to the key tools and techniques used in attack analysis, equipping them with practical skills to investigate malicious programs and adversary activity. Through a blend of theory, practical exercises, and hands-on labs, the course provides the skills required to build strong defensive and attack ready capabilities.

Prerequisites

We recommend that learners have essential security knowledge prior to attending. The OffSec SEC-100 Security Essentials course is advised as a prerequisite.

Target audience

This course is designed for:

- Cybersecurity professionals and incident responders
- Security operations centre (SOC) analysts
- IT and network administrators responsible for threat monitoring
- Forensic investigators and security engineers
- Risk and compliance managers requiring hands-on understanding of threat detection and response

What You Will Learn

By the end of this course, learners will be able to:

- Detect threats both before and after an attack occurs
- Apply advanced techniques to handle cyber-attacks in real time
- Use threat modelling to strengthen organisational resilience
- Hunt, trace, detect, and acquire evidence during and after incidents
- Conduct forensic investigation, analysis, and attack reconstruction
- Apply tools and techniques to examine network traffic, to discover anomalies
- Gain familiarity with malware behaviours, anti-forensics detection

Outline

Module 1 – Incident management and threat assessment

- Engagement lifecycle management

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Incident chronology
- Record keeping, interim reporting, and final results
- Threat assessment

Module 2 – Network threat monitoring and discovery

- IP protocols and network architectures
- Common classes of tools
- OS and application fingerprinting
- Network access control analysis
- Cryptography and applications of cryptography
- File system permissions and host analysis techniques
- Understanding common data formats
- Exercises:
  - Reviewing HTTP and HTTPS traffic using a network analyser
  - Identifying network connections with netstat
  - Password cracking using NMAP
  - Analysing file permissions in Linux

Module 3 – Background information gathering and open source intelligence

- Registration records and DNS analysis
- Open source investigation and web enumeration
- Extraction of document metadata
- Community knowledge sources
- Exercises:
  - Using DNSrecon to enumerate a website
  - Performing Google Dorking to gather target information
  - Gathering intelligence on domains using OSINT-spy
  - Using tools to monitor crypto transactions and abuse
  - Investigating IP addresses with OSINT tools

Module 4 – Threat detection and treatment

- Network traffic capture, logs, and configuration security
- Identifying unusual protocol behaviour, beaconing, and encryption misuse
- Command and control channels, data exfiltration, reconnaissance
- Internal spread, privilege escalation, and managing false positives
- Exercises:
  - Examining PCAP data
  - Analysing torrent traffic
  - Reviewing Apache logs using Excel
  - Investigating a large firewall dataset
  - Performing social engineering attacks

Module 5 – Analysing threat intrusions

- Host-based data acquisition and live analysis setup
- Windows file systems, file structures, and registry essentials
- Identifying suspect files and storage media analysis
- Memory analysis and infection vectors
- Malware behaviours, anti-forensics, and rootkit identification
- Exercises:

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Capturing and examining memory artefacts
- Examining external media, browser, account usage, and emails
- Analysing Windows artefacts in an espionage scenario
- Detecting exploit kits within a network
- Creating malware samples for testing
- Identifying rootkits using chkrootkit

Module 6 – Threat detection engineering and malware discovery

- Anti-reverse engineering techniques
- Functionality identification and Windows architecture
- API development and binary code structures
- Cryptographic techniques and processor architectures
- Windows executable formats, obfuscation, and hiding techniques
- Malware behavioural analysis and reporting

Exams and assessments

This course includes the National Cyber Security Center (NCSC) assured training exam:

- Online proctored exam taken after the course
- Duration: 90 minutes
- Format: 60 multiple-choice questions
- Passing score: 60%
- Successful learners receive a digital badge

Hands-on learning

This course provides extensive practical application, including:

- Scenario-driven exercises across all modules
- Network traffic analysis and log investigation
- Use of OSINT and threat intelligence tools
- Memory forensics and malware analysis techniques
- Realistic intrusion case studies to develop investigative skills