Certified Cybercrime Threat Investigator Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Over the five day delivery of this National Cyber Security Center (NCSC) assured course, you will learn how to detect an attack, how to handle it, how to trace and acquire the evidence, investigate, analyse and re-construct the incident.

We then lay the groundwork for malware analysis by presenting the key tools and techniques malware analysts use to examine malicious programs.

The Certified Cybercrime In cybercrime course will show them you how to use investigative skills and apply them in the cyber space. This course has its own NCSC assured Cybercrime Investigator exam taken online post course via APMG.

Prerequisites

This course is suitable for those that have successfully completed the Cybercrime Computing and Networking Foundation Course or Foundation Certificate in Cyber Security.

What You Will Learn

This National Cyber Security Center (NCSC) assured five-day course will help delegates learn;

- Understand how to detect an attack
- Understand how to handle an attack
- Understand how to trace and acquire the evidence during and post attack
- Understand how to investigate, analyse and re-construct a cyber security incident
- Become familar with the key tools and techniques used to examine and investigate malicious programs

Outline

Module 1 – Soft Skills and Incident Handling

- Engagement Lifecycle Management
- Incident Chronology
- Record Keeping, Interim Reporting & Final Results
- Threat Assessment

Module 2 – Core Technical Skills

- IP Protocols
- Network Architectures
- Common Classes of Tools

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- OS Fingerprinting
- Application Fingerprinting
- Network Access Control Analysis
- Cryptography
- Applications of Cryptography
- File System Permissions
- Host Analysis Techniques
- Understanding Common Data Format

Exercise - Reviewing HTTP and HTTPS traffic using a network analyser

Exercise - Identifying Network Connections with netstat

Exercise - Password cracking using NMAP

Exercise - Analysing file permissions in Linux

Module 3 – Background Information Gathering & Open Source

- Registration Records
- Domain Name Server (DNS)
- Open Source Investigation and Web Enumeration
- Extraction of Document Meta Data
- Community Knowledge

Exercise - Using DNSrecon to enumerate a website

Exercise - Performing Google dorking to gain information about a target

Exercise - Gathering intelligence on domains using OSINT-spy

Exercise - Using intelligence tools to monitor transactions and crypto abuse

Exercise - Using OSINT tools to investigate IP addresses

Module 4 – Network Intrusion Analysis

- Network Traffic Capture
- Data Sources and Network Log Sources
- Network Configuration Security Issues
- Unusual Protocol Behaviour
- Beaconing
- Encryption
- Command and Control Channels
- Exfiltration of Data
- Incoming Attacks
- Reconnaissance
- Internal Spread and Privilege Escalation
- False Positive Acknowledgement

Exercise – Examining PCAP data

Exercise – Examining torrent traffic

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Exercise – Examining Apache Logs using Excel

Exercise – Examining a large firewall log dataset

Exercise – Performing social engineering attacks

Module 5 – Analysing Host Intrusions

- Host-Based Data Acquisition
- Live Analysis Laboratory Set-up
- Windows File System Essentials
- Windows File Structures
- Application File Structures
- Windows Registry Essentials
- Identifying Suspect Files
- Storage Media
- Memory Analysis
- Infection Vectors
- Malware Behaviours and Anti-Forensics
- Rootkit Identification
- Malware Analysis

Exercise - Capturing and examining memory artefacts

Exercise - Examining memory artefacts on a live machine emails

Exercise - Examining external media, browser, account usage and emails

Exercise - Examining Windows artefacts in a corporate espionage case

Exercise - Detecting exploit kits within a network

Exercise - Creating malware to deploy to victims

Exercise - Identifying rootkits using chkrootkit

Module 6 – Reverse Engineering Malware

- Windows Anti-Reverse Engineering
- Functionality Identification
- Windows NT Architecture
- Windows API Development
- Binary code structure
- Cryptographic Techniques
- Processor Architectures
- Windows Executable File Formats
- Hiding Techniques
- Malware Reporting
- Binary Obfuscation
- Behavioural Analysis

End of Course Exam

National Cyber Security Center (NCSC) Assured Training Exam:

Certified Cybercrime Threat Investigator Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Online proctored exam is taken post course
- Duration - 90 minutes
- Questions 60, multiple choice
- Passing score of 60%
- Digital badge