Certified Malware Investigator (CMI) Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This is a core-level technical course for people looking to extend their digital forensic knowledge beyond conventional device analysis.

COURSE OVERVIEW

On this five-day practical course you will investigate forensic case studies, applying the principles, knowledge and techniques learnt during the course. It will help you protect your IT environment by showing you how to conduct malware analysis, from first principles all the way to investigating network activity stemming from malicious software infection that your AV software has failed to detect.

.

Prerequisites

Completion of the CFIP course is highly recommended. Otherwise you will need:

- Knowledge of the principles surrounding forensic investigation and an understanding of the preliminary forensic investigation case considerations
- Sound experience with the Microsoft Windows operating systems
- An understanding of how a web page is requested and delivered
- Ideally an understanding of Command Line Interface (CLI) and TCP/IP networking concepts

WHO SHOULD ATTEND

For those looking to develop their skills in malware identification and analysis, including:

- Digital forensic analysts
- Cyber incident investigators
- Law Enforcement Officers
- System administrators

Certified Malware Investigator (CMI) Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

THE SKILLS YOU WILL LEARN

Practical application of course content will be through the use of case scenarios in order to gain a practical understanding of modern malware beyond the often quoted traditional principles; mount forensic images for analysis; build virtual machines for analysis, and build a network environment to carry out network forensic analysis.

KEY BENEFITS

The course will give you:

- You will learn how to identify, analyse and interpret malicious software and associated forensic artefacts, including Trojan horses, viruses, worms, backdoors and rootkits
- How Trojan payloads can be used to bypass anti-virus software, personal and corporate firewalls
- You will practice malware investigations from mounted, booted and network perspectives, and undertake real-world exercises, including the conversion of E01 forensic images to bootable virtual machine disks
- The function, structure and operation of the Windows registry, and investigation of malicious software locations in the registry and file system
- The skills to analyse and interpret malicious software, and investigate network activity initiated by malicious software infection
- An understanding of how to simplify complex evidence, and collate and report results
- An industry-recognised qualification in malware investigation

Outline

Analysis Environments

- Identify and define the five analysis environments
- Identify situations in which each of the investigation environments could be used effectively
- Identify their respective levels of risk both to the original data as well as other systems

Malicious Software

- Define the term 'malicious software'
- Identify and define different types of malicious software
- Identify similarities and differences between different types of malicious software

Malware Investigation

- Identify the stages of malware investigation
- Critically assess the capabilities and limitations of anti-malware tools
- Identify the different means of running software at system start-up

Methods of Deception

- Identify mechanisms of malware delivery

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Identify mechanisms of disguise
- Identify client security circumvention

Mounted Analysis

- Mounting forensic images as logical drives
- Using malware scanners against the mounted image
- Documenting the results of malware scans
- Using online scanners for further clarification

Booted Analysis

- Identify approaches to creating a booted analysis environment
- Experiment with making a Virtual Machine
- Identifying password implications
- Identifying and explaining the potential differences between mounted and booted analysis results

Network Analysis

- Identify key reasons for network analysis
- Methods of building a network for analysis
- Explaining network communication protocols
- Using traffic analysis tools for network analysis
- External Port Analysis
- Identifying and explaining the potential differences between network and other analysis results

Virtualisation Malware

- Explain how hardware Hypervisor support allows for virtualisation malware
- Define Type I, Type II and Type III malware

Simplifying Complex Evidence

- Aiming the report at a subject knowledge level fitting the target audience
- Discuss a sample report outline