MALWARE ANALYSIS FUNDAMENTALS

Check Point SOFTWARE TECHNOLOGIES LTD

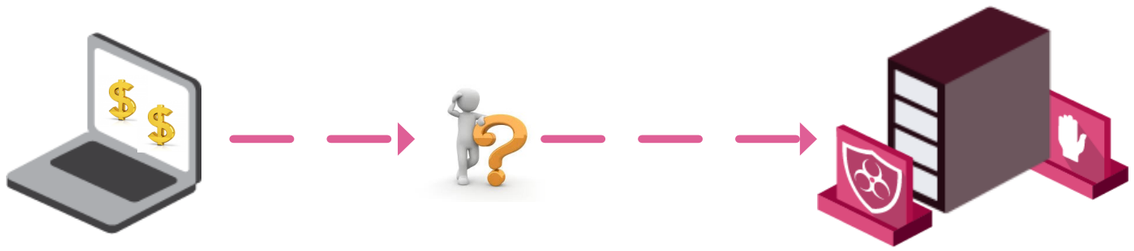
4 DAY CLASS

PART OF HACKINGPOINT

Get Certified Today!

This curriculum covers the fundamentals of Malware Analysis

Malware is one the major challenges facing the security industry today. It plays a critical role in high profile targeted attacks, such as the breach at Sony entertainment, as well as large, indiscriminate outbreaks, such as WannaCry.



WHO SHOULD TAKE THIS CLASS?

- Analysts working in forensics, incident response, and other malware-protection fields.
- Security professionals wishing to expand their knowledge.
- Anyone interested in malware threats and analyzing them.

Identifying and analyzing malware is an essential skill for any security professional - whether investigating a security incident, tracking a large-scale campaign, or discovering yet unknown threats.

This technical 4-day course covers all the fundamentals of malware analysis, providing the student with a solid understanding of the malware world, as well as the tools and hands-on skills required to effectively analyze malicious files.

Course curriculum

Introduction to Malware

- Who perpetrates these attacks?
- What is their goal?
- Types of malware
- Malware history and evolution

Malware Behavior and Techniques

- Malware lifecycle
- Infection, persistence, privilege escalation
- Stealth, network communication

Malware Analysis Overview

- Analysis types
- Tools and techniques

Triage Analysis

- Identifying malware
- Analyzing the PE header
- Examining static features
- Utilizing OSINT tools

Dynamic Analysis — OS Behavior

- Monitoring OS activity — process, file, registry
- Mapping execution flow
- Detecting malicious behaviors such as, persistence, injection, hooking

Dynamic Analysis — Network Behavior

- Malware communication techniques
- Analyzing malware traffic
- Controlling responses

Analyzing Malicious Office Documents

- Droppers and downloaders
- Debugging macro scripts

Automated Analysis

- Working with sandboxes
- Evasion techniques and how to bypass them