Cyber Advance Malware Analyst Investigator

40 Hours

Description

Wawiwa's Cyber Advance Malware Analyst Investigator is a one-of-a-kind program, specifically aimed for professionals who seek to make their next step in malware analysis.

The program uses Wawiwa's virtual labs, developed in Israel, the Startup Nation.

Expectations and Goals

In this program, students gain advanced knowledge on malware threats and malware analysis techniques.

Learning Objectives

- Detect, identify, and contain the most common cyber security incidents
- Look for suspicious activity of malwares and malicious code on endpoints
- Analyze malwares with several techniques (static and dynamic)
- Get to know the reverse engineering process

Target Audience

- Incident handlers (Tier 2 and above) and leaders of incident handling teams
- System administrators
- Security practitioners and architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks
- Students for technological bachelor's degree

Prerequisites

- Advance knowledge on Microsoft's Operating Systems
- Understanding of networks and protocols
- Basic knowledge of monitoring and security devices

What Graduates Receive

- Course presentation as PDF file
- Cheat sheet and useful documentation
- "Swiss Army Knife" - 3GB of IR tools

Virtual Lab

The course uses envario ™ virtual labs , an Israeli based Cyber virtual lab

Wawiwa provides the center with a unique cloud environment with the following Virtual Machines:

- Clean VM (Win10 64-bit) – For first Lab Installation
- Malware Analysis VM (Win10 64-bit)
- Digital Forensics VM (Win10 64-bit)
- Certificates

Students are expected to bring their own laptops, unless the center has appropriate training classes with computers. Hardware requirements: Intel: i3 or higher, Win 10, Min 8GB RAM

Internet bandwidth at home - minimum base connection speed of 100 Mbps down is required, Internet latency less than 50ms.

Classroom Facility

A fully equipped classroom, with the required multimedia infrastructure. At list 2 screens of 50” or higher connected to the instructor working station

a. Workstations with internet communication,

b. Minimal requirements for student’s workstation (per student) and 1 for Instructor:

1. Windows 10 OS, MS office
2. Intel: i5 processor or higher
3. x64-compatible 2.0 GHz CPU minimum or higher
4. 8 GB RAM minimum
5. 250 GB SSD available hard-drive space
6. Laptop or stationary computer workstation recommended monitors of 22” or larger

c. Minimum base connection speed of 100 Mbps down is required, Internet latency less than 50ms.

Practical Learning (Hands-On)

- 23 hours of hands-on activities
- Hands-on activities on local environments

Course Syllabus

Main Module	Hours + Labs
Module 1 - PE Files ● Headers ● Sections ● Import / Exports ● Resources ● CFF Explorer	**8**
Module 2- WinAPI ● Concept ● Common DLLs ● Kernel Objects ● Ansi and Unicode ● Suspicious APIs and their uses	**2**
Module 3 - Extra Static Analysis ● Packers ● Obfuscators ● VMs ● Crypters ● RDG Packer Detector ● Entropy	**3**
Module 4 - Basic and Advance Dynamic Analysis ● Sysinternals ● Apimonitor ● Wireshark ● ApateDNS ● InetSIM	**7**

● Netcat ● Sandboxes	
Module 5 - Assembly Crash ● Architecture (x86) ● Memory Management ● Registers ● Instructions ● Opcodes	**3**
Module 6 - RE Methodology ● What is RE? ● Approaching RE ● Decompilers	**5**
Module 7 - Debugging Methodology ● What is debugging? ● Approaching debugging ● Debugger overview	**3**
Module 8 - IDA ● Overview ● Cheatsheet ● Flirt signatures	**4**
Module 9 - Malicious Techniques ● Hooking ● Code Injection ● Anti VM / Debug ● Obfuscation ● Persistence ● Dynamic function resolving (using APIs and using PEB) ● Encryption	**2**
Module 10 - Course Final Project	**2**

● Sub Module 10 ● Final Hands-On Drill	

* Virtual labs are implemented using classroom facilities or can be provided 100% virtual (no need for facility only Bring Your own laptops)