SeeSecurity

SEE SECURITY
CYBER SECURITY COLLEGE

Advanced Malware Analysis

A unique hands-on advanced training programme in Malware Analysis for experienced professionals who wish to master the field.

CYBER SECURITY MALWARE ANALYSIS
CSMA
See
© see security international college

This course is aimed at those having the fundamental knowledge and skills in malware analysis. It is a continuation of See Security’s Cyber Security Malware Analysis Level 1 training programne, and covers advanced, more sophisticated topics and techniques in the field.

In this course you will get a deep understanding of the inner workings, the building blocks and the understanding of malware infection kill chain, the ability to defeat anti-analysis malware protection mechanisms, the ability to fight packed malware to the death to eventually unpack them to fully reverse engineer them. Finally, you will learn many tips and tricks that are based on many years of experience in order to reverse engineer malware in the right way with the right mindset.

At the end of the course, you will master the creed of malware reverse engineering.

Advanced Malware Analysis Training Programme

A unique hands-on advanced training programme in Malware Analysis for experienced professionals who wish to master the field.

About See Security College

See Security College is a highly specialised and international cybersecurity college. One of seven colleges of its kind, our college offers training programmes aimed for absolute beginners to more advanced professionals. The college delivers its study programs worldwide, through the See Security International brand as well as well-known governmental and special cybersecurity agencies.

See-Security CEO, Mr. Avi Weissman is one of the leaders of the Israeli Cyber industry and serves as an advisor and commentator to the Israeli government for the regulation of cyber professions. Further, Mr. Weissman was the co-founder of the Israeli Forum for Information Security (IFIS) together with Maj. Gen. (Res.) and former head of National Security Council, Yaakov Amidror. In addition to his role in leading the college, Avi is also a co-CEO of a cyber human resources company, See-HR and a cybersecurity consulting company, See Events – Managed SIEM/SOC.

About The Programme

In this course you will get a deep understanding of the inner workings, the building blocks and the understanding of malware infection kill chain, the ability to defeat anti-analysis malware protection mechanisms, the ability to fight packed malware to the death to eventually unpack them to fully reverse engineer them. Finally, you will learn many tips and tricks that are based on many years of experience in order to reverse engineer malware in the right way with the right mindset.

At the end of the course, you will master the creed of malware reverse engineering.

Key Features	
Cost	TBD
Aaudience	Advanced, experienced cybersecurity professionals
Orientation	Theoretical and applicative knowledge
Objectives	To get a deep understanding of the inner workings, the building blocks and the understanding of advanced malware analysis topics.
Entry requirements	Practical knowledge in OS, networking code, Basic understanding of x86 Assembly, C and Python, PC/MAC with Intel i5/i7/i9 CPU, 16GB of RAM and an SSD storage, Local administrator account, VMware Workstation/Fusion installed.
Certifications	Advanced Malware Analyst Specialist
Academic hours	Total of 40 online training sessions
Homework	Total of 100 homework assignments
Course format	Online lectures accompanied with 1-on-1 session with the lecturer

Target Audience

This course is primarily aimed for Malware Analysts who wish to get a better understanding of the inner mechanisms of malware. It is also suitable for IT security professionals, Digital Forensics experts as well as others with the passion and eagerness to discover and learn new topics.

The Lecturer – Uriel Kosayev

Uriel is a cybersecurity researcher, founder of TRIOX and former researcher at the IDF. Founder of communities such as Caliber-Training and MalwareAnalysis.co., Uriel has a broad experience in Digital Forensics, Malware Analysis, Penetration

Testing and Reverse Engineering. Uriel Joined our team in 2019 and serves as a lecturer in a variety of programmes.

Entry Requirements

You will not be tested on these requirements for enrolment. However, we emphasize that without the required background knowledge it will be difficult ti keep up with the materials covered theought the course and even more challenging to pass the exams and assignments. The following are required:

- Basic understanding of networking: TCP/IP, Routing, Forwarding.
- Reading and understanding code.
- Basic understanding of Windows Server and Linux Shell commands.
- Basic understanding of x86 Assembly, C and Python.
- Basic understanding of well-known protocols such as HTTP/HTTPS, DNS, SMTP, FTP, SSH.
- PC/MAC with Intel i5/i7/i9 CPU, 16GB of RAM and an SSD storage.
- Local administrator account is must.
- VMware Workstation/Fusion installed.

Important Remarks

- The amount of hours required for this advanced and extensive course includes class-based practical labs.
- Students are required to invest twice as much in practical homework labs.
- It is mandatory for the student to pass the final project based on its malware research and report of findings to be qualified as a professional malware analyst.

Curriculum

Introduction & Lab Setup (5 hours)

1.1. What is Malware and common types of Malware.
1.2. What is Malware Analysis and its purposes?
1.3. Types and levels of Malware Analysis (static, dynamic and code reverse engineering).
1.4. Setting up the Lab (lab architecture overview, setting up Windows Malware analysis lab).
1.5. Optimizing the lab for better and efficient Malware Analysis.
1.6. Tools of the trade (deployment and overview).

Malware Reverse Engineering (35 hours)

2. Windows Internals (Optional if this is apart from the basic course requirements).
2.1. OS Protection Rings.
2.2. Hardware Abstraction Layer.
2.3. MMU-TLB, VAD and memory virtualization.
2.4. Virtual vs. Physical memory.
2.5. Process vs. Thread.
2.6. Registry.
2.7. COM and OLE objects.
2.8. Stack vs. Heap.

3. Code Reverse Engineering.
3.1. Dissecting Maldoc and malicious PDF.
3.2. Disassembler vs. Debugger.
3.3. Disassemble, debug and patch of PE executables using IDA Pro.
3.4. Debugging PE executables using X64dbg.
3.5. Reverse Engineering and unpacking of packed/obfuscated malware samples.
3.6. Inspecting Windows API calls using API Monitor.
3.7. Decompile and debug .NET code using dnSpy.

4. Deep dive into malware functionalities and persistence methods.
4.1. Dissecting keylogging techniques.
4.2. Deep dive into malware persistence techniques.
4.3. Deep dive into hooking and Process-Injection techniques.
4.4. Analyzing PowerShell stagers.