UTI ACADEMY

UTI Academy provides specialized courses for IT professionals and organizations willing to take benefit from the competitive advantages provided by international certifications.

In a world where threats continuously evolve, there's nothing more important than constant training that enables specialists to fight the latest turns in the ever-changing world of cybercrime on its most aggressive and sophisticated level.

Join the Mandiant courses delivered by UTI Academy to get in touch with valuable know-how.

MANDIANT

Mandiant believes in intense, hands-on training that develops performable skills. We use operational case scenarios to ensure greater effectiveness. Our classes and exercises are reality-based rather than classroom mock-ups, and every class is led by some of the most experienced cyber security professionals in the business.

We follow a proven training methodology that is enhanced by our significant experience responding to real-world attacks. Mandiant helps our clients respond to sophisticated security breaches on a daily basis - we are able to leverage our understanding of attackers’ methodologies, tools, and tactics to emulate real-world attacks and identify security vulnerabilities. Mandiant consultants have extensive experience providing information security advice to Fortune 500 organizations and government agencies.

Our consultants include former law enforcement officers, intelligence officers, Department of Defense computer security specialists, computer programmers, forensic examiners, and published experts who have significant experience shaping the information security programs at global organizations.
COURSES

ENTERPRISE INCIDENT RESPONSE (3 DAYS)

Attacks against computer systems continue to increase in frequency and sophistication. In order to effectively defend data and intellectual property, organizations must have the ability to rapidly detect and respond to threats. This intensive three-day course is designed to teach the fundamental investigative techniques needed to respond to today’s landscape of threat actors and intrusion scenarios. This class is built upon a series of hands-on labs that highlight the phases of a targeted attack, key sources of evidence, and the forensic analysis know-how required to analyze them. Students will learn how to conduct rapid triage on a system to determine if it is compromised, uncover evidence of initial attack vectors, recognize persistence mechanisms, develop indicators of compromise to further scope an incident, and much more.

MODULES INCLUDED

• The Incident Response Process: An introduction to the targeted attack life-cycle, initial attack vectors used by different threat actors, the stages of an effective incident response process, and remediation.
• Acquiring Forensic Evidence: An overview of volatile and non-volatile evidence, live response acquisition versus forensic imaging, and related methods and tools.
• Introduction to Windows Evidence: Analysis of the key sources of evidence that can be used to investigate a compromised Windows system, including NTFS artifacts, prefetch, web browser history, event logs, the registry, and more.
• Memory Acquisition and Analysis: How memory is structured on a Windows system, the artifacts and evidence available in physical memory and the page file, and how memory analysis can identify advanced techniques used by malware.
• Investigating Lateral Movement: An in-depth analysis of how attackers move from system-to-system in a compromised Windows environment, the distinctions between network logons and interactive access, and the resulting sources of evidence on disk, in logs, and in the registry.
• Persistence: Analysis of advanced persistence mechanisms, such as DLL search order hijacking; introduction to user-land and kernel root kits; alternative remote-access mechanisms exploited by attackers.

WHO SHOULD ATTEND

The content and pace is intended for professionals with some background in conducting forensic analysis, network traffic analysis, log analysis, security assessments & penetration testing, or even security architecture and system administration duties. It is also well suited for those managing CIRT / incident response teams, or in roles that require other investigative tasks.

COURSE PRE-REQUISITES

• Executing command line utilities as an Administrator.
• Navigating the Windows file system using the command line.
• Common file system structures.
• Microsoft Windows registry.
• Active Directory and basic Windows security controls.
• Networking fundamentals, including common Windows protocols.
This course provides a rapid introduction to the tools and methodologies used to perform on executables found on Windows systems using a practical, hands-on approach. Students will learn how to find the functionality of a program by analyzing disassembly and by watching how it modifies a system and its resources as it runs in a debugger. They will learn how to extract host and network-based indicators from a malicious program. They will be taught about dynamic analysis and the Windows APIs most often used by malware authors. Each section is filled with in-class demonstrations and hands-on labs with real malware where the students practice what they have learned.

MODULES INCLUDED

Module 1: Basic Static Analysis
Learn to quickly perform a malware autopsy.

Module 2: Safe Environment
Learn how to protect yourself by analyzing malware in a safe environment, such as using virtual machines.

Module 3: Basic Dynamic Analysis
Learn to analyze running malware.

Module 4: Disassembly
Learn the basics and build a foundation of the x86 assembly language and also learn how to use IDA Pro THE tool for disassembly analysis.

Module 5: Windows Internals
Learn a wide range of Windows-specific concepts that are relevant to analyzing Windows malware.

Module 6: Debugging
Learn how to monitor and change malware behavior, as it runs, at a low level.

WHO SHOULD ATTEND

- Software developers
- Information security professionals
- Incident responders
- Computer security researchers
- Corporate investigators
- Others requiring an understanding of how malware works and the steps and processes involved in performing.

COURSE PRE-REQUISITES

Students should have an excellent knowledge of computer and operating system fundamentals. Computer programming fundamentals and Windows Internals experience is highly recommended.
SPECIAL TOPICS IN MALWARE ANALYSIS– ADVANCED (5 DAYS)

Malware authors sometimes take deliberate steps to thwart the reverse engineering of their malware. This course is focused on advanced topics related to combating malware defense mechanisms. Designed for the experienced malware analyst, a robust skill set in x86 architecture and the Windows APIs is essential. Students will learn how to specifically combat against anti-disassembly, anti-debugging and anti-virtual machine techniques.

Students will also learn how to defeat packed and armored executables and will be challenged to demonstrate these skills several times throughout the course. Additional topics covered will include malware stealth techniques, such as process injection and rootkit technology; analyses of samples written in alternate programming languages, such as Delphi and C++; and a review of available tools and techniques.

All concepts and materials presented are reinforced with demonstrations, real-world case studies, follow-along exercises, and student labs to allow students to practice what they have learned. This class is taught by senior FLARE Malware Analysts who are experienced in fighting through the state-of-the-art malware armor.

MODULES INCLUDED

Module 7: Stealth
Learn how malware hides its execution, including process injection and user-space rootkits.

Module 8: Shellcode
Learn how shellcode works from beginning to end, including position independence and symbol resolution.

Module 9: Anti-Disassembly
Learn how to circumvent the anti-disassembly mechanisms that malware authors use to thwart your analysis in tools like IDA Pro.

Module 10: Scripting IDA PRO
Learn how to automate IDA Pro to help you analyze malware more efficiently.

Module 11: Anti-Debugging
Learn how to combat anti-debugging, including how to bypass timing checks, Windows debugger detection, and debugger vulnerabilities.

Module 12: Anti-VM
Malware can detect it is running in your safe environment; learn how to fool it to think otherwise.

Module 13: Reversing C++
Learn how C++ concepts like inheritance, polymorphism, and objects influence analysis.

Module 14: Packers and Unpacking
Learn how to unpack manually - an important skill for analyzing malware.

Module 15: 64-bit Malware
Learn about how x64 changes the game for , including how WOW64 works and the architecture changes from x86.

Module 16: Encryption and Encoding
Learn to deal with string obfuscation techniques commonly used by malware and take malware communications and analyze network packet captures based on your analysis.

Module 17: .NET Reversing
Learn how to reverse engineer .NET bytecode and deal with obfuscation techniques employed by attackers.

WHO SHOULD ATTEND

· Information security staff
· Forensic investigators
· Others requiring an understanding of how to overcome difficult challenges in .

COURSE PRE-REQUISITES

Training or experience in and extensive knowledge of computer and operating system fundamentals is required. Completion of MANDIANT’s “Crash Course”, while not required, is extremely beneficial. Exposure to software development is also highly recommended.
# LOCATION AND PRICES

<table>
<thead>
<tr>
<th>Course</th>
<th>Date</th>
<th>Location</th>
<th>Instructors</th>
<th>Price (VAT Excluded)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Incident Response (3 days)</td>
<td>May 29 - 31</td>
<td>Budapest, Hungary</td>
<td>Andy Rector, Julian Pileggi</td>
<td>2990 EUR</td>
</tr>
<tr>
<td>Malware Analysis Crash Course (2 days)</td>
<td>June 1 - 2</td>
<td>Budapest, Hungary</td>
<td>Nick Harbour, Omar Sardar</td>
<td>1790 EUR</td>
</tr>
<tr>
<td>Special Topics in Malware Analysis (5 days)</td>
<td>June 26 - 30</td>
<td>Bucharest, Romania</td>
<td>Willi Ballenthin, Moritz Raabe</td>
<td>3990 EUR</td>
</tr>
</tbody>
</table>

*Please send a request to training@utiacademy.ro*