EDUCATION COURSES

TRAIN YOUR CYBER SECURITY WORKFORCE TO BUILD ADVANCED SKILLS AND EXPERTISE TO SECURE AND DEFEND THE ENTERPRISE.

OVERVIEW

At Mandiant, education and training are part of our mission. We believe we have a responsibility to share what we know with those who need it most. Our classrooms are filled with executives from companies in virtually all industry verticals, law enforcement officials and even independent security consultants. All of our courses are taught by practitioners that have first-hand experience with the latest twists and turns in the ever-changing world of cybercrime on its most aggressive and sophisticated level.

- All courses are taught by some of the most experienced cyber security professionals in the business.
- Classes and exercises are reality-based rather than classroom mock-ups
- Operational case scenarios ensure greater effectiveness.

COURSE OFFERING:

Malware Analysis

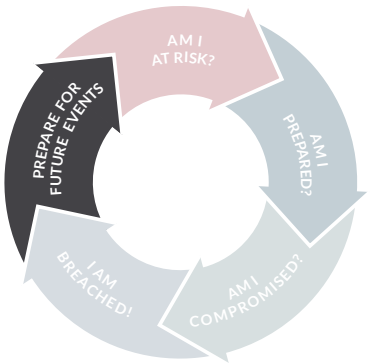
Introduction to Malware Analysis for Non-programmers (1 day)

This course provides a beginner-level introduction to the tools and methodologies used to perform malware analysis on executables found on Windows systems using a practical, hands-on approach. This class is taught by M-Labs Malware Analysts who are experienced in analyzing a diverse set of malware.

Malware Analysis Crash Course (2 days)

This course provides a rapid introduction to the tools and methodologies used to perform malware analysis on executables found on Windows systems using a practical, hands-on approach.

MANDIANT®
A FireEye® Company



In a world where threats continuously evolve, nothing is more important than continuing education.

MANDIANT DIFFERENCE

Mandiant is a trusted advisor to organizations globally with over 10 years of experience dealing with advanced threat actors from around the world. We support organizations during the most critical times after a security breach has been identified, and proactively help them improve their detection, response, and containment capabilities.

Our training courses offer practical, realistic security frameworks developed from the front lines of incident response.

FireEye®
SECURITY REIMAGINED

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, and 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.

Fundamentals of Malware Reverse Engineering (3 days)

This course provides a rapid introduction to the tools and methodologies used to perform malware analysis 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, and 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.

Special Topics in Malware Analysis (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 in order to benefit from this course.

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.

Customized Malware Analysis (19 modules available, ½ day per module)

We offer customized malware analysis training solutions in order to address the business needs of our clients that may have specific learning objectives. We can build a course that includes any of our 19 malware analysis modules. These modules range from basic concepts of analyzing disassembly to advanced concepts such as x64 and anti-reverse engineering techniques. Each module includes targeted learning and hands-on activities that were authored by the FLARE malware analysis team at FireEye.

Cyber Crime & Incident Response

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.

Introduction to Cyber Crime for Executives (1 day)

Network security breaches transform calm working environments into high-stress battle zones that require executives to rapidly make key decisions impacting the company and the investigation. Informed executives are better equipped to understand the threat and make the right decisions in minimal time.

The Mandiant Introduction to Cybercrime for Executives course was developed to educate senior staff on cybercrime and incident response. During the course, instructors will guide students through a scenario based on real-world intrusions involving sophisticated attackers. The scenario is provided from both the attacker and victim perspectives. Throughout the course, instructors present the tactics and technologies used by the victim and attackers. The scenario illustrates the most common method that attackers use to establish a foothold and remain undetected in the victim network.

The class discusses the pros and cons of the various courses of action available to the victim, providing students with critical insight into the many issues investigators and victim organizations face in defending networks and responding to security breaches.

Network Investigations

Network Traffic Analysis (3 days)

Sophisticated attackers frequently go undetected in a victim network for an extended period of time. Attackers know how to blend their traffic with legitimate traffic, and only the skilled network traffic analyst will know how to find them. Network traffic analysis is a critical skill set for any organization.

Mandiant's intense three-day Network Traffic Analysis course prepares students to face the challenge of identifying malicious network activity. The course provides an overview of network protocols, network architecture, intrusion detection systems, network traffic capture, and traffic analysis. The course consists of lecture and multiple hands-on labs to reinforce technical concepts.

Wireless Security (2 days)

Wireless computing devices are everywhere, and new products seem to appear daily. The explosive growth of wireless devices also brings an increased risk to networks permitting wireless access. As a result, network and information security personnel must understand the risk of wireless computing.

The Mandiant Wireless Security course is a two-day class specifically designed for professionals who support, design, or assess IEEE 802.11 wireless environments, commonly known as Wi-Fi. It is a hands-on course presented from the attacker's perspective and helps students to understand the wireless attacker methodology. The course includes a variety of case studies and numerous lab exercises to reinforce wireless security concepts and materials.

Operating System Investigations

Introduction to Linux for Security Professionals (3 days)

The Mandiant Introduction to Linux for Security Professionals course introduces information security professionals to the Linux operating system and helps prepare them to conduct investigations in a UNIX environment. The course follows the "learn by doing" philosophy. Students perform Linux/UNIX commands and discover how the operating system functions. Attendees will primarily operate in the command-line environment.

The course includes relevant case studies and reinforces key concepts with hands-on exercises to ensure that students gain practical experience in each critical area discussed.

UNIX Investigations (5 days)

Attacks against systems running variants of the UNIX operating system are on the rise. In order to effectively respond to the escalating threat, organizations must have skilled information security staff able to rapidly detect and remove threats.

Mandiant developed the UNIX Investigations course to provide information security personnel the fundamental skills needed to quickly identify and eliminate threats targeting UNIX or variants of the UNIX operating systems. The course is based on the real-world experience of Mandiant consultants who have years of experience combating these types of attacks. The course reinforces key concepts with hands-on exercises to ensure students gain practical experience in each critical area discussed.

For more information on Mandiant consulting services, visit:
www.FireEye.com/Mandiant.html

Mandiant, a FireEye Company
1440 McCarthy Blvd. Milpitas, CA 95035
(703) 935 1701 | 800.647.7020 | info@mandiant.com

www.FireEye.com

FireEye