MANDIANT
NOW PART OF Google Cloud

# Mandiant Academy Course Catalog

# Contents

## Advanced Acquisition and Testing Techniques



## Workshops



## Exercises and Preparedness

# Introduction

## Course Listings

The Mandiant Academy courses in this catalog address essential cyber security skills that use free, open-source or existing customer technologies.

## Instructor-led Training

Instructor-led training is presented by a live instructor, either in-person or via a virtual classroom. Instructor-led training includes hands-on labs designed to accelerate learner acquisition of practical skills.

All Mandiant instructors are security professionals with years of security experience working on the frontlines of major cyber incidents around the world.

The duration of a single instructor-led training course can range from a half-day to five days.

## Web-based Training

Web-based training (WBT) are self-paced, on-demand online courses that can be accessed at any time, from any location. Learners may pause and resume training as their schedule allows.

Our web-based training is designed to work in modern desktop browsers (Chrome, Firefox, Safari, and Microsoft Edge) and tablets (such as iPad) without the use of browser plugins. Technology requirements and exceptions are noted in course descriptions when applicable.

The duration of a web-based training course can range from a half-day to four days of content.

## Experiential Learning

Experiential learning uses a hands-on approach that recreates a network compromise situation and provides a holistic incident response experience. A cyber simulation range provides a consequence-free environment where participants are challenged to respond as a team to the latest advanced persistent threat (APT) attack methodologies.

The ability to expose teams to nation-state level attacks within a cyber range allows them to learn, practice, and innovate without experiencing an actual compromise. Experiential learning connects the training environment to the operating environment, which allows leadership to assess team performance and get an honest assessment of team readiness against relevant threats.

## Delivery methods by course

**Onsite ILT.** An onsite instructor-led course delivered at your organization's office.

**Offsite ILT.** An offsite instructor-led course delivered at a third-party location.

**Virtual ILT.** A virtual (online) instructor-led course delivered exclusively to your organization.

**Web-based training.** A web-based (also on-demand or self-paced) training course accessible to your organization anytime, anywhere.

**Public ILT.** A public instructor-led course delivered at a Mandiant office or third-party classroom. It may include attendees from many different organizations.

**Public VILT.** A public virtual (online) instructor-led course which may include attendees from many different organizations.

**TABLE 1.** Cyber security training from Mandiant.

| | Onsite ILT | Offsite ILT | Virtual ILT | Web-Based Training | Public ILT (Per Seat) | Public VILT (Per Seat) |
|---|---|---|---|---|---|---|
| Advanced Red Teaming Techniques: Malware Authoring and Repurposing | x | x | | | | |
| Advanced Windows Enterprise Incident Response | x | x | | | | |
| Audits and Compliance in the Cyber Domain | x | x | | | | |
| Business Email Compromise | x | x | x | | | |
| Combined Windows-Linux Enterprise Incident Response | x | x | | | | |
| Creative Red Teaming | x | x | x | | x | x |
| Cyber Intelligence Foundations | x | x | x | x | x | x |
| Cyber Intelligence Production | x | x | x | x | | |
| Cyber Security Awareness | x | x | x | | | |
| Cyber Security Policy and Implementation | x | x | | | | |
| Digital Forensics and Incident Response for PLCs | x | x | | | | |
| Essentials of Malware Analysis | | | | x | | |
| Fundamentals of Cyber Security | x | x | x | | | |
| Fundamentals of Industrial Control Systems (ICS) Security | x | x | x | | x | x |
| Incident Response for Everyone | x | x | x | | x | x |
| Inside the Mind of an APT | | | | x | | |
| Intelligence Research I—Scoping | x | x | x | x | | |
| Intelligence Research II—Open Source Intelligence (OSINT) | x | x | x | x | x | x |
| Introduction to Cyber Crime for Executives | x | x | x | | | |
| Introduction to Mandiant Security Instrumentation Platform | x | x | x | | | |
| Introduction to Threat Intelligence and Attribution | x | x | x | | x | x |

**TABLE 1.** Cyber security training from Mandiant.

| | Onsite ILT | Offsite ILT | Virtual ILT | Web-Based Training | Public ILT (Per Seat) | Public VILT (Per Seat) |
|---|---|---|---|---|---|---|
| Linux Enterprise Incident Response | x | x | x | | x | x |
| Malicious Documents Analysis | x | x | x | | x | x |
| Malware Analysis Fundamentals | x | x | x | | | |
| Malware Analysis Crash Course | x | x | x | | x | x |
| Malware Analysis Master Course | x | x | | | | |
| Network Traffic Analysis | x | x | x | | x | x |
| Practical Mobile Application Security | x | x | | | | |
| Practical Threat Hunting | x | x | x | | x | x |
| Senior Executive Mentorship Program | x | x | | | | |
| ThreatSpace: Real-World Attack Scenarios | x | x | x | | | |
| Windows Enterprise Incident Response | x | x | x | | x | x |

# Introductory Courses

## Introduction to Cyber Crime for Executives

Security breaches transform calm working environments into high-stress battle zones. Informed executives are better equipped to understand the threat and make corresponding decisions smartly and quickly.

This course is designed to educate senior leaders about cyber crime and incident response. Learners will review a scenario based on real-world intrusions by a sophisticated attacker, examining tactics and technologies from both the attacker's and victim's perspectives. This scenario illustrates the most common method that attackers use to establish a foothold and remain undetected in the victim's network.

The course also covers the pros and cons of follow-up actions available to the victim and provide critical insight into the many issues investigators and victim organizations face when defending networks and responding to security breaches.

### Learning objectives

After completing this course, learners should be able to:

- Understand how attackers defeat defenses and compromise networks
- Explore the most common network defense posture assumed by victims
- Collect electronic evidence
- Understand how investigators analyze data and use findings to resolve incidents
- Grasp the challenges an organization faces after its computer security defenses are breached

### Who should attend

Executives, security staff, corporate investigators or other staff who need a general understanding of network security and network operations.

### Delivery method

In-person or virtual instructor-led training

### Duration

1 day (in-person delivery)
1 day (virtual delivery)

## Cyber Security Awareness

This three-day course provides an overview of cyber security threats along with the fundamentals of a strong cyber security program. It is designed for both non-technical and technical learners who want to understand how threat actors see their targets, and it shares methods to help mitigate risks.

Learners will be introduced to foundational elements of cyber security programs, including security governance to establish a security framework, and ways to align the security program with business objectives. Security risk management, measurement and communications will also be covered. Security architecture topics will address common security practices and tools used to monitor and protect mature organizations. Cyber defense topics such as building an incident response plan will also be discussed, alongside examples of incident response methodologies.

### Learning objectives

After completing this course, learners should be able to:

- Have enhanced awareness of today's threat landscape
- Understand common attacker methodologies
- Understand how an attacker enters, persists, and exfiltrates data from an organization via the attack lifecycle
- Establish governance that will provide guidance and oversight to the cyber security program
- Write an effective cyber security mission statement, vision statement, and strategic plan
- Understand how a cyber security risk program enables the business to make informed, risked-based decisions
- Define the basic security architecture necessary to protect any organization
- Understand the most common technologies used by modern cyber security programs
- Understand the foundational components of a strong cyber security program

### Who should attend

Managers, technical staff, and non-technical staff in cyber security roles, or other roles supporting cyber security functions.

### Prerequisites

A working understanding of basic information security principles is a plus, but not required.

### Delivery method

In-person or virtual instructor-led training

### Duration

2 days (in-person delivery)
3 days (virtual delivery)

## Fundamentals of Industrial Control Systems (ICS) Security

This two-day course provides IT security professionals and ICS/OT engineers interested in ICS/OT security with the fundamental knowledge and skills required to build and expand an ICS/OT security team.

Learners will become familiar with ICS/OT security concepts, secure architecture, threat models and ICS/OT security standards and best practices. The course will also discuss today's security trends and the current threat landscape. Throughout the course, exercises and demonstrations inspired by actual cases and incidents in the ICS world will enable learners to advance their knowledge in their day jobs.

### Learning objectives

After completing this course, learners should be able to:

- Understand ICS/OT security history, today's trends and threat landscape
- Discuss ICS/OT standards and best practices: NIST SP800-82, IEC62443, MITRE ATT&CK for ICS framework
- Describe the Purdue model of architecture, defense in depth, and secure ICS/OT network zoning and segmentation.
- Understand the elements of effective ICS/OT security monitoring and incident response programs
- See how a set of selected of useful ICS/OT security tools could be used.

### Who should attend

IT security professionals and ICS/OT engineers developing a ICS/OT security foundation.

### Prerequisites

Knowledge of ICS, DCS, SCADA, Modbus, OPC, IP address and IP packet.

### Delivery method

In-person and virtual instructor-led training

### Duration

2 days (in-person delivery)
3 days (virtual delivery)

### What to bring

Recommended Windows 7 or higher to install Wireshark and NetworkMiner (free version). Students may use macOS if they can successfully install both Wireshark and NetworkMiner (free version). If not, we recommend installing Windows on a VM.

## Fundamentals of Cyber Security

This five-day course provides a managerial perspective of contemporary computer and network security issues. The course gives learners the knowledge to design, implement, and maintain a network security plan that successfully defends a network from malicious or accidental intrusion.

### Learning objectives

After completing this course, learners should be able to:

- Explain the concepts of information systems security as applied to an IT infrastructure
- Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure
- Explain the importance of critical contributors to the effective implementation of security policy, such as access controls, operations, administration, security audits, testing, and monitoring
- Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems
- Explain how businesses use cryptography to maintain information security
- Analyze why network principles and architecture are important to security operations
- Explain how attackers compromise systems, and what networks and defenses are used by organizations
- Apply international and domestic information security standards and compliance laws to real-world implementation in both the private and public sector

### Who should attend

Governance, risk, compliance, and IT professionals, as well as anyone else who wants to understand how cyber security relates to their profession.

### Prerequisites

A working understanding of basic information security principles is a plus, but not required.

### Delivery method

In-person instructor-led training

### Duration

5 days

## Cyber Security Policy and Implementation

This five-day course teaches learners how to manage information security policies and frameworks, how to establish their needs, and how to identify potential challenges around those policies in an organizational environment. Learners will explore policy implementation issues and ways to overcome barriers to implementation.

Effective policy design and maintenance will be discussed along with frameworks that organizations can use to help with risk management and compliance. Finally, a review of U.S. compliance laws and associated Information Security requirements will be conducted.

### Learning objectives

After completing this course, learners should be able to:

- Identify the role of an information systems security (ISS) policy framework in overcoming business challenges
- Analyze how security policies help mitigate risks and support business processes in various domains in the information technology (IT) infrastructure
- Describe the components and basic requirements for creating a security policy framework
- Describe the different methods, roles, responsibilities and accountabilities of personnel, along with the governance and compliance of security policy framework
- Describe the different ISS policies associated with the user domain, IT infrastructure, and risk management
- Describe different issues related to implementing and enforcing ISS policies
- Describe the different issues related to defining, tracking, monitoring, reporting, automating, and configuring compliance systems and emerging technologies

### Who should attend

Security managers, project managers, system administrators, and auditors. Personnel responsible for the protection of corporate resources or those involved in the creation and maintenance of security policy.

### Delivery method

In-person instructor-led training

### Duration

5 days

## Audits and Compliance in the Cyber Domain

This five-day course trains learners on concepts associated with cyber security compliance and scope of audits. This course will also detail the various tools, techniques, and frameworks that can aid in the auditing process. Learners will be able to describe auditable domains in an organization, as well as the end-to-end process of an audit, including how to prepare, conduct, and complete an audit report.

### Learning objectives

After completing this course, learners should be able to:

- Describe the role of ISS compliance in relation to U.S. compliance laws
- Explain the use of standards and frameworks in a compliance audit of an IT infrastructure
- Describe the components and basic requirements for creating an audit plan to support business and system considerations
- Describe the different parameters required to conduct and report on IT infrastructure audit for organizational compliance
- Describe information security systems compliance requirements within the User, Workstation, LAN, Remote Access, and System/Application domains
- Describe the frameworks used to implement ISS compliance within the LAN-to-WAN and WAN domains
- List the qualifications, ethics, and certification organizations for IT auditors

### Who should attend

Security and audit professionals, managers of audit or security teams, system and network administrators.

### Delivery method

In-person instructor-led training

### Duration

5 days

## Introduction to the Mandiant Security Instrumentation Platform

This two-day introduction to the Mandiant Security Instrumentation Platform provides hands-on experience with the platform to introduce core concepts and important modules. It provides a solid understanding of the platform and reinforces knowledge gained from the self-paced training series. The goal is to have participants be able to start using the platform effectively in their environment to improve their organization's security posture.

### Learning objectives

After completing this course, learners should be able to:

- Explain the purpose of the Security Instrumentation Platform
- Install network and endpoint Actors
- Use the platform to test network and security controls, identify areas of improvement and monitor progress
- Run security content, including Actions, Sequences and Evaluations
- Evaluate test results and analyze essential takeaways
- Setup, configure and maintain AEDA monitors
- Analyze platform analytics and develop custom reports
- Explain Protected Theater
- Create custom security content
- Examine system administration, maintenance and troubleshooting features of the platform

### Who should attend

Security professionals who will be using the Security Instrumentation Platform to manage and report their organization's systemic cyber security risk.

### Delivery method

In-person or virtual instructor-led training

### Prerequisites

Varies based on audience

### Duration

2 days

### Registration instructions

Contact training@mandiant.com for more information, including prerequisites and upcoming class dates.

# Intelligence and Attribution Courses

## Introduction to Threat Intelligence and Attribution

This course is a fast-paced introduction to threat intelligence and attribution. It is designed to provide insight into attribution methodology and demonstrate the proper handling of threat intelligence information.

The course explores the main components of a threat group and shows how Mandiant analysts use raw tactical intelligence and weigh connections and relationships to build a set of related activities that corresponds to a group of threat actors. Learners will become familiar with several factors they should consider when attributing related activity, and view real-world examples of research and pivoting. The course also examines operational and strategic intelligence, which helps determine the "who" and the "why" behind an attack.

The course also clarifies critical security terminology so learners can separate valuable information from hype.

### Learning objectives

After completing this course, learners should be able to:

- Understand various definitions of threat intelligence and attribution
- Distinguish between tactical, operational and strategic threat intelligence
- Use tactical intelligence in the early stages of a cyber attack to evaluate data and correctly identify indicators that can be grouped into a set of related activity and attributed to a threat group
- Gain insight into common errors that can occur when analyzing common forensic artifacts and interpreting information presented from various sources
- Examine operational and strategic intelligence to determine the attribution and sponsorship of an attack operation
- Understand how attribution analysis can provide crucial context to threat activity that enables more informed decisions and improved resource allocation
- Understand why attributing cyber operations to a threat group can have significant implications — and even affect geopolitical dynamics
- Consider attribution from a threat group's point of view

### Who should attend

Cyber intelligence analysts, cyber threat analysts, security analysts and penetration testers.

### Prerequisites

A working understanding of basic information security principles. A general understanding of threat intelligence and indicators of compromise (IoCs). Experience conducting forensic analysis, network traffic analysis, log analysis, security assessments and penetration testing, security architecture and system administration duties are a plus, but not required.

### Delivery method

In-person or virtual instructor-led training

### Duration

1 day (in-person delivery)
2 days (virtual delivery)

## Inside the Mind of an APT

The Inside the Mind of an APT on-demand course is designed to explore how countries use cyber operations as a tool of statecraft to advance national-level priorities and in response to geopolitical drivers. Primarily focused on the "Big 4" cyber countries—China, Iran, North Korea, and Russia—the course will examine how, why, and against whom nation-states attack. These capabilities include:

- Conducting cyber espionage
- Destructive or disruptive cyber attacks
- Cyber-enabled information operations

Insights gleaned from this course will allow students to improve their critical and lateral thinking ability to more swiftly respond to requests for information from leadership, hone forecasting skills, and fill knowledge gaps on nation-state cyber threat actors. It will also prepare organizations to proactively anticipate shifts in cyber threats and adjust their risk management and enterprise cyber security strategies accordingly.

### Learning objectives

After completing this course, learners should be able to:

- Understand how governments use cyber operations as a tool of statecraft to support national-level priorities.
- Explain why governments use cyber espionage, attacks, and cyber-enabled influence operations independently or in concert with one another.
- Recognize key intelligence services and military organizations, down to the unit level, conducting cyber operations, and their mapping to known APT groups.
- Identify catalysts that could drive potential future cyber efforts against specific industries through country-specific doctrine, policies, initiatives, or geopolitical shifts.
- Evaluate how cyber threat intelligence vendor collection and reporting can augment existing threat coverage gaps within your organization.
- Realize the complexity of work required to answer the attribution question of which nation-state is responsible for conducting a cyber operation.
- Apply structured analytic techniques (SATs) to provide rigor and the ability to convey the underpinning reasoning behind an analytic assessment.

### Who should attend

The primary audience for this course is any individual within an organization who is tasked with providing, making, supporting, researching, or communicating assessment about cyber threats or cyber risk. This course is designed as an intermediate-level, multidisciplinary survey course, but does not require students to have experience in cyber security, cyber risk management, or cyber threat analysis. Students are introduced to key concepts in cyber security, information technology (IT), cyber threat intelligence, and international relationship concepts throughout the course.

### Prerequisites

None

### Delivery method

On-demand training

### Duration

14 hours

Content is available for 3 months from date of first login. It can be accessed 24/7 from a standard web browser.

### What to bring

A computer with internet connection and a modern browser (such as Google Chrome).

## Cyber Intelligence Foundations

This three-day course explains how to apply the discipline of intelligence analysis to the cyber domain. The course covers strategic subjects such as the organizational role of cyber threat intelligence (CTI) and stakeholder analysis, as well as analytic practitioner skills development topics, such as understanding the intelligence lifecycle, developing raw data into minimally viable intelligence, and an introduction to cyber intelligence attribution.

### Learning objectives

After completing this course, learners should be able to:

- Clearly define cyber intelligence and the difference between intelligence and information, and articulate the role and importance of the cyber threat intelligence (CTI) capability
- Describe how the Intelligence Cycle functions as the working model to operationalize intelligence
- Explain the two modes of analytic thinking and the use of structured analytic techniques
- Detail ways to counter analytic bias
- Explain threat model concepts and why we use them
- State the basics of malware composition
- Describe how intelligence analysts convert raw threat data into actionable intelligence
- Write well-structured intelligence reports and determine improvements to current communications

### Who should attend

Managers of technical information security teams and analytic and technical professionals familiar with threat intelligence.

### Prerequisites

Working understanding of basic information security principles and general understanding of threat intelligence.

### Delivery method

In-person, virtual instructor-led or on-demand training

### Duration

3 days (in-person delivery)
4 days (virtual delivery)

### What to bring

Learners may find it useful to bring a computer with link analysis software.

## Intelligence Research I—Scoping

This foundational course teaches students to analyze, prioritize, and fully understand requests for information (RFIs), and create a research plan that keeps their efforts on track.

Students will learn to uncover stakeholder intent so that their intelligence analysis can be actioned. They will gain the ability to fully interpret implicit and explicit RFIs by identifying relevant context from intelligence requirements, organizational threat profiles, and key stakeholder analysis.

They will also learn how to use a research management system to organize research and avoid information overload, and assess source relevance and trust to ensure efficient and focused collections efforts.

### Learning objectives

After completing this course, learners should be able to:

- Use a structured, repeatable four-step scoping process
- Generate context by referring to the organizational threat profile, key stakeholder analysis, and intelligence requirements (and how to proceed if these aren't available)
- Prepare for collections efforts by developing a research management system
- Proactively assess different kinds of information and sources to avoid wasting time on irrelevant or unreliable sources

### Who should attend

This is a foundational level course for cyber practitioners who must scope and respond to formal and informal requests for information (RFI's).

### Prerequisites

Students should have taken Cyber Intelligence Foundations or have equivalent knowledge.

### Delivery method

In-person, virtual instructor-led or on-demand training

### Duration

1 day (in-person delivery)
2 days (virtual delivery)

## Intelligence Research II—Open Source Intelligence (OSINT)

This foundational course teaches students to identify and develop pivot points or leads in investigations across multiple use cases.

Students will review the basic functions of open source tools and learn when and why to use them in their research. They will apply their skills to several scenarios drawn from frontline experience, including executive-level RFIs, incident response investigations, and information operation campaigns.

As they work through these scenarios in a lab environment, students will apply their knowledge of tools such as VirusTotal, Alienvault, PassiveTotal, and Facebook, and use advanced search engine techniques.

### Learning objectives

After completing this course, learners should be able to:

- Configure their systems to ensure good operational security (OPSEC) and safety while researching
- Keep detailed case notes and avoid getting lost in their research
- Think critically about when and why to use a particular tool within the context of a research task
- Navigate basic functions of several common OSINT tools
- Identify and use investigation pivot points and artifacts

### Who should attend

This is a foundational level course for cyber practitioners who must safely and efficiently conduct research as part of investigations or in response to RFIs.

### Prerequisites

Students should have taken Cyber Intelligence Foundations and Cyber Intelligence Research I—Scoping or have equivalent knowledge.

### Delivery method

In-person, virtual instructor-led or on-demand training

### Duration

2 day (in-person delivery)
3 days (virtual delivery)

## Cyber Intelligence Production

This foundational course teaches students to convey analytic assessments and findings in their intelligence reports and briefings.

Students will be asked to deconstruct intelligence reporting of varying qualities and designed for different stakeholders to identify author intent, methods, and findings.

During these exercises, students will be exposed to various examples of strategic, operational, and technical intelligence products. Intelligence writing and briefing principles, including bottom line up front (BLUF), words of estimative probability (WEPs), and analytic judgments will all be introduced along with potential pitfalls.

The course will also review best practices tied to citations, grammar, style, and peer review. It concludes with an opportunity for students to take provided data and generate an original intelligence product and corresponding briefing.

### Learning objectives

After completing this course, learners should be able to:

- Recognize the critical elements of an intelligence report, and create reports that include those elements
- Identify different types of cyber threat intelligence reports and specify how they differ in type, audience, scope and purpose
- Name, define, and apply various style guidelines
- Interpret a scenario and develop a high quality intelligence product that can be actioned by stakeholders

### Who should attend

This is a foundational level course for cyber practitioners who must produce or assess intelligence reports and briefings.

### Prerequisites

Students should have taken Cyber Intelligence Foundations, Cyber Intelligence I—Scoping and Cyber Intelligence II—Open Source Intelligence or have equivalent knowledge.

### Delivery method

In-person, virtual instructor-led or on-demand training

### Duration

1 day (in-person delivery)
2 days (virtual delivery)

# Incident Response Courses

## Incident Response for Everyone

This two-day course is designed to teach non-technical support staff how to respond to an incident and how to work with investigators during an incident response event. This course includes a series of hands-on exercises that highlight all phases of the investigation life cycle.

Participants will learn how to respond to a detected incident, describe the incident to stakeholders, differentiate among different evidence acquisition methods, understand how investigators conduct an investigation, evaluate different remediation methods, and review an investigative report. By the end of this course, participants will be able to actively provide non-technical support to an investigation by understanding the full scope of incident response processes and procedures.

The course is comprised of the following topics with exercises included throughout the course.

- Incident Discovery: Incident Discovery, Notifying Stakeholders, Initial Documentation, Triggered Processes and Procedures
- Incident Description: Describing the Incident, Evidence Collection for Trusted Partners
- Evidence Acquisition: Evidence Collection Capabilities, Trusted Partner Evidence Collection, Evidence Preservation
- Analysis: Planning for Analysis, Analysis Gaps, Analysis Methodologies Remediation: Remediation Plan Concepts, Remediation Plan Customizations, Remediation Timing
- Reporting Results

### Learning objectives

After completing this course, learners should be able to:

- Determine how to respond to an incident immediately after initial notification
- Summarize an incident for relaying to a trusted partner
- Choose an investigation plan most suited to investigate your organization's incident
- Choose a remediation plan most suited to investigate your organization's incident
- Evaluate an investigative report for quality
- Summarize the events described in an incident report

### Who should attend

The audience for this course includes all members of an organization that are commonly asked to work with or as part of an investigative team, such as personnel involved in information security (information security, information technology), counsel (general or third-party, cyber policy lawyers, breach coaches), or communications (internal or external communications).

### Prerequisites

None

### Delivery method

In-person or virtual instructor-led training

### Duration

2 days (in-person delivery)
3 days (virtual delivery)

### What to bring

Students are required to bring their own laptop with an Internet connection and a modern browser.

Learners will receive a lab book and all required class materials.

## Windows Enterprise Incident Response

This intensive three-day course is designed to teach the fundamental investigative techniques needed to respond to today's cyber threats. The fast-paced course is built upon a series of hands-on labs that highlight the phases of a targeted attack, sources of evidence and principles of analysis. Examples of skills taught include how to conduct rapid triage on a system to determine whether it is compromised, uncover evidence of initial attack vectors, recognize persistence mechanisms and investigate an incident throughout an enterprise.

Although the course is focused on analyzing Windows-based systems and servers, the techniques and investigative processes are applicable to all systems and applications. The course includes detailed discussions of common forms of endpoint, network and file-based forensic evidence collection and their limitations as well as how attackers move around in a compromised Windows environment. The course also explores information management that enriches the investigative process and bolsters an enterprise security program. Discussion topics include the containment and remediation of a security incident, and the connection of short-term actions to longer-term strategies that improve organizational resiliency.

### Learning objectives

After completing this course, learners should be able to:

- Describe the incident response process, including the threat landscape, targeted attack life cycle, initial attack vectors used by different threat actors, and phases of an effective incident response process
- Conduct system triage to answer key questions about what transpired across the enterprise during an incident
- Apply lessons learned to proactively investigate an entire environment (including metadata, registry, event logs, services, persistence mechanisms and artifacts of execution) at scale for signs of compromise
- Manage and effectively record information related to ongoing investigations and incidents
- Understand the role of the remediation phase in an enterprise investigation
- Understand how to hunt for threats using threat intelligence, anomaly detection and known threat actor techniques, tactics and procedures (TTPs)

### Who should attend

Incident response team members, threat hunters and information security professionals.

### Prerequisites

Background in conducting forensic analysis, network traffic analysis, log analysis, security assessments and penetration testing, or security architecture and system administration. Learners must have a working understanding of the Windows operating system, file system, registry and use of the command line. Familiarity with Active Directory and basic Windows security controls, plus common network protocols, is beneficial.

### Delivery method

In-person or virtual instructor-led training

### Duration

3 days (in-person delivery)
4 days (virtual delivery)

### What to bring

Students are required to bring their own laptop that meets the following specs:

- Windows 7+
- Core i5 or equivalent processor
- 6 GB (preferably 8 GB) of RAM
- 25 GB free HDD space
- Virtual machines are acceptable provided at least 4 GB or RAM can be allocated
- Microsoft Office installed outside the VM
- Admin/install rights

Learners will receive a lab book and USB thumb drive containing all required class materials and tools.

## Linux Enterprise Incident Response

This three-day course is designed to teach the fundamental investigative techniques needed to respond to today's sophisticated threat actors and their intrusion methods. This course includes a series of hands-on labs that highlight all phases of a targeted attack lifecycle, critical sources of attacker evidence and the forensic analysis required to conduct effective analysis.

Students will learn how to conduct rapid triage to determine system compromise, uncover evidence of initial attack vectors, recognize persistence mechanisms and develop indicators of compromise (IOCs) to further scope an incident.

### Learning objectives

After completing this course, learners should be able to:

- Understand the stages of an effective incident response process including preparation, detection and analysis and remediation
- Recognize the most common forms, benefits and limitations of endpoint forensic evidence collection including forensic imaging and live response acquisition
- Identify and use critical sources of evidence to investigate and analyze a compromised Linux system including EXT3/EXT4 file systems, syslog, audit logs, memory, VPN and web shells
- Audit common Linux applications for databases and web servers including Oracle, MySQL, PostgreSQL, Apache and nginx
- Know how attackers move from system-to-system in a compromised Linux environment through their use of data including credentials, logons, remote command execution and shell artifacts
- Investigate a full environment, at-scale, for signs of compromise with the use of proactive hunting
- Analyze web logs to recognize and interpret common attacker techniques including obfuscation and encoding methods
- Improve logging visibility, prevent evidence tampering and reduce the attack surface by identifying common configuration parameters and logged events that aid effective investigations

### Who should attend

Linux system administrators, incident responders, threat hunters and SOC analysts who need to understand the process involved in performing effective enterprise incident response for Linux systems.

### Delivery method

In-person or virtual instructor-led training

### Duration

3 days (in-person delivery)
4 days (virtual delivery)

### What To bring

Students are required to bring their own laptop that meets the following specs:

- Windows 7+ and MacOS 10.11+
- VMware or VirtualBox installed on system with 2 GB of memory and 2 CPU cores dedicated for the VM (hypervisor software on the USB will be provided for students)
- 50 GB of free HDD space reserved for the VM
- Microsoft Office installed (recommended)
- Admin/install rights
- Wireless connectivity (recommended)

## Combined Windows-Linux Enterprise Incident Response

Attacks against computer systems continue to increase in frequency and sophistication. To effectively defend data and intellectual property, organizations must have the ability to rapidly detect and respond to threats. This intensive course is designed to teach the fundamental investigative techniques needed to respond to today's landscape of threat actors and intrusion scenarios.

The 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.

### Learning objectives

After completing this course, learners should be able to:

- Describe the incident response process, including the threat landscape, targeted attack life cycle, initial attack vectors used by different threat actors, and phases of an effective incident response process
- Conduct system triage to answer key questions about what transpired across the enterprise during an incident
- Apply lessons learned to proactively investigate an entire windows environment (including metadata, registry, event logs, services, persistence mechanisms and artifacts of execution) at scale for signs of compromise
- Identify and use critical sources of evidence to investigate and analyze a compromised Linux system including EXT3/EXT4 file systems, syslog, audit logs, memory, VPN and web shells
- Audit common Linux applications for databases and web servers including Oracle, MySQL, PostgreSQL, Apache and nginx
- Know how attackers move from system-to-system in a compromised Linux environment through their use of data including credentials, logons, remote command execution and shell artifacts
- Analyze web logs to recognize and interpret common attacker techniques including obfuscation and encoding methods
- Manage and effectively record information related to ongoing investigations and incidents
- Understand the role of the remediation phase in an enterprise investigation
- Improve logging visibility, prevent evidence tampering and reduce the attack surface by identifying common configuration parameters and logged events that aid effective investigations
- Understand how to hunt for threats using threat intelligence, anomaly detection and known threat actor techniques, tactics and procedures (TTPs)

### Who should attend

This course is intended for students with some background in conducting security operations, incident response, 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 oversight of forensic analysis and other investigative tasks.

### Delivery method

In-person instructor-led training

### Duration

5 days (in-person delivery)

### What to bring

Students are required to bring their own laptop that meets the following specs:

- Laptop with VMWare installed (VMWare player meets the requirement)
- Specs: Windows 7+ or MacOS 10.11+
- 16GB+ memory
- Core i7+ CPU
- 25GB+ Free HDD space

## Advanced Windows Enterprise Incident Response

This five-day course teaches advanced investigative techniques to incident responders on the frontline to help identify and scope intrusions by government, financial, and political threat groups. The course includes a series of hands-on exercises which will allow the student to explore the foundations of what they have learned and expand on them, directly applying techniques to real world scenarios.

Students will learn how to identify, detect, and hunt for advanced techniques, defeating malware obfuscation and applying hunting techniques at scale across both traditional endpoint and cloud based infrastructure. The course covers historic and live attacker scenarios and techniques that the defender can use during an active firefight to mitigate potential losses for the company.

### Learning objectives

After completing this course, learners should be able to:

- Use ATT&CK framework to guide strategic security decisions for the organization
- Summarize the steps of the Incident Response Process
- Determine how to effectively communicate incident information to leadership and others within your organization
- Demonstrate understanding on advanced techniques used by threat actors
- Discuss non-conventional implant deployment techniques which we come across when facing advanced APT threat actors but are rarely seen leveraged by less sophisticated groups
- Recognize when obfuscation is in use
- Summarize what YARA is and how to develop a YARA rule
- Discover the layout of common memory structure and common memory attack methods
- Explain the pros and cons of different analysis tools
- Provide an overview of the available evidence sources, how to collect evidence, common investigative scenarios and available tools for data analysis and investigation
- Highlight the difference in tempo required when dealing with Live Attackers and the implications to the organization and coordination of the IR team

### Who should attend

This is a fast-paced technical course that is designed to provide hands-on experience with investigating targeted attacks and the analysis steps required to triage compromised systems. The content and pace are intended for students with some background in conducting security operations, incident response, 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 oversight of forensic analysis and other investigative tasks.

### Prerequisites

Students should possess an excellent knowledge of computer and operating system fundamentals. Computer programming fundamentals and Windows Internals experience is highly recommended as well. Completion of Mandiant's Windows Enterprise Incident Response and/or Linux Enterprise Incident Response is highly recommended.

### Delivery method

In-person instructor-led training

### Duration

5 days (in-person delivery)

### What to bring

A computer with internet connection and a modern browser (such as Google Chrome).

## Network Traffic Analysis

Sophisticated attackers frequently go undetected in a victim's network for an extended period. Attackers can blend their traffic with legitimate traffic that only skilled network analysts know how to detect. This course shows learners how to identify malicious network activity.

The course provides an overview of network protocols, network architecture, intrusion detection systems, network traffic capture and traffic analysis. Learners review the types of network monitoring and the tools commonly used to analyze captured network traffic. The course also explores the best techniques for investigating botnets and how to use honeypots in network monitoring.

The course includes lectures and hands-on lab sessions to reinforce technical concepts.

### Learning objectives

After completing the course, learners should be able to:

- Understand the network monitoring and incident response processes, and why it's critical in today's network environments
- Discuss the pros and cons of statistical, connection, full content and event monitoring and tools
- Perform event-based monitoring using Snort
- Minimize network traffic with the Snort rule structure and custom rule creation
- Review Snort alerts using the Sguil front end

### Who should attend

Information technology and security staff, corporate investigators and other staff members who need to understand networks, network traffic, network traffic analysis and network intrusion investigations.

### Prerequisites

A basic understanding of TCP/IP and Windows and UNIX platforms. Familiarity with security terminology and a working knowledge of Wireshark is also recommended.

### Delivery method

In-person or virtual instructor-led training

### Duration

3 days (in-person delivery)
4 days (virtual delivery)

### What to bring

Students are required to bring their own laptop that meets the following specs:

- Windows 7+
- Core i5 or equivalent processor
- 6 GB (preferably 8 GB) of RAM
- 25 GB free HDD space
- Virtual machines are acceptable provided at least 4 GB of RAM can be allocated

Learners will receive a lab book and all required class materials and tools, and must be able to either boot from USB or have VMware Player.

## Practical Threat Hunting

The Practical Threat Hunting course is a three-day course that has been designed to teach threat hunters and incident responders the core concepts of developing and executing threat hunts. Through this course students will be able to:

- Apply cyber threat intelligence concepts to hunt for adversary activity in your environment
- Establish a repeatable hunt methodology and develop hunt use cases
- Leverage end point data to hunt
- Establish measures of effectiveness for hunt program

This course includes practical labs that challenge the students to develop hypothesis and hunt missions in order to hunt for evidence of compromise through multiple scenarios including social engineering, network and system compromise, and APT nation-state actors. The labs are designed so that students have an opportunity to experience hunting using environments like the command line, Jupyter Notebook, and forensic tools like Velociraptor.

### Course Description

The course is compromised of the following modules, with labs included through the instruction.

- Introduction to Threat Hunting – Understand the core concepts that constitute threat hunting. An overview of the characteristics of a threat hunt is provided along with the benefits of performing threat hunts and also the challenges that threat hunters should be aware of. The key concept of leveraging threat intelligence is introduced to students.
- Introduction to Threat Modeling – Understand how threat modeling is key to any effective threat hunt. An overview is provided of the basics of threat modeling. Students are then provided a breakdown of the workflow of threat modeling along with how it ties into threat hunting. The importance of using threat intelligence for threat modeling is also discussed.
- Threat Hunt Program Framework- Understand what constitutes a threat hunt program framework. This module is beneficial to understand the requirements of a formal threat hunt program.
- Threat Hunt Operational Drivers- Understand what is needed from a hunt mission capability. An overview is provided of the areas in which an organization needs to have capabilities in order to execute effective threat hunts. Discussions are conducted on the benefits of having these capabilities and challenges if an organization is deficient in any of them.
- A4 Framework – This module introduces the students to the A4 framework of threat hunting. This framework is reinforced for the students through the rest of the course as is it used as part of all the hands on labs.
- Threat Hunt Library – Understand the importance of developing and maintaining a Threat Hunt Library. Students will participate in exercises that will reinforce the importance of developing and maintaining a threat hunt library. As part of the labs students will be asked to develop a threat hunt library that they will be able to take with them at the conclusion of the course.
- Labs – Students will be challenged to complete multiple labs where they will develop hypothesis and hunt missions, using threat intelligence, for specific scenarios. The students will then be provided access to an environment in which they will be able to execute the hunt missions that they design.
- Use case – Gain an understanding of a critical outcome of threat hunts. Understand how threat hunt missions are used to generate use cases. As part of this module an overview of Sigma rules will be provided. Students will then develop use cases based on the hunt missions they developed as part of the hands on labs.

### Who should attend

The content and pace of this course is intended for threat hunters, information security professionals, incident responders, computer security researchers, corporate investigators, or others require an understanding of how threat hunting is performed, and the processes involved in performing threat hunts.

### Prerequisites

Students should possess knowledge of computer and operating system fundamentals. Python programming is not required; however, familiarity with the language or programming concepts will help students when working on some of the labs.

### Delivery method

In-person and virtual instructor-led training

### Duration

3 days (in-person delivery)
4 days (virtual delivery)

### What to bring

Students should bring their own laptop computer with the latest browser of choice and the ability to connect to the Internet.

Students will receive class handouts, temporary credentials to get access to Mandiant Advantage, and directions on how to connect to the lab environment.

## Digital Forensics and Incident Response for PLCs

Attacks against industrial control systems (ICS) are on the rise. To effectively respond to this emerging threat, organizations must be aware of the challenges that come along with performing digital forensics and incident response (DFIR) for ICS. This course is designed to give ICS security personnel the skills needed to identify and understand threats targeting ICS devices that use embedded operating systems such as VxWorks and Windows CE.

This fast-paced technical course offers learners hands-on experience investigating targeted attacks and guides them through the steps required to analyze and triage compromised ICS.

### Learning objectives

After completing this course, learners should be able to:

- Learn to investigate targeted attacks against ICS
- Understand the steps required to triage compromised ICS

### Who should attend

Incident response team members, threat hunters, information security professionals and industrial control system security professionals.

### Prerequisites

Background in ICS, PLCs and other embedded devices and operating systems. Background in forensic analysis, network traffic analysis, log analysis, security assessments and penetration testing, security architecture, and system administration.

### Delivery method

In-person instructor-led training

### Duration

1 day

### What to bring

Students are required to bring their own laptop that meets the following specs:

- Windows 7+ or Windows 7 Virtual machine
- VMware Player or Workstation
- 20 GB of free HDD space
- Wireless connectivity

# Malware Analysis Courses

## Essentials of Malware Analysis

This 16-hour on-demand course provides a beginner-level introduction to the tools and methodologies used to perform malware analysis on executables found in Windows systems using a practical, virtual hands-on approach. The course introduces students to Disassembly, including subtopics on X86 Architecture, The Stack, C Code Constructs, and an introduction to IDA Pro. The content is developed and taught by FLARE malware analysts who are experienced in analyzing a diverse set of malware.

### Learning objectives

After completing the course, learners should be able to:

- Quickly perform malware triage using a variety of techniques and tools without running the malware
- Analyze running malware by observing file system changes, function calls, network communications and other indicators
- Interpret x86 assembly language
- Utilize and navigate IDA pro

### Who should attend

Information technology staff, information security staff, corporate investigators and others who need to understand how malware functions operate and the processes involved in malware analysis.

### Prerequisites

General knowledge of computer and operating system fundamentals. Exposure to computer programming fundamentals and Windows Internals experience (recommended).

### Delivery method

On-demand training

### Duration

16 hours

Content is available for 3 months from date of enrollment. It can be accessed 24/7 from a standard web browser.

### What to bring

Students are required to bring their own laptop that meets the following specs:

- VMware Workstation 10+ or VMware Fusion 7+
- 30 GB of free HDD space

## Malware Analysis Fundamentals

This course provides a beginner-level introduction to the tools and methodologies used to perform malware analysis on executables found in Windows systems using a practical, hands-on approach. The course introduces students to decompilation with Ghidra and introduces Windows Technologies that are prevalent in malware such as WMI, .NET, and PowerShell. The content is taught by FLARE malware analysts who are experienced in analyzing a diverse set of malware.

### Learning objectives

After completing the course, learners should be able to:

- Quickly perform malware triage using a variety of techniques and tools without running the malware
- Analyze running malware by observing file system changes, function calls, network communications and other indicators
- Learn about code compilation and how to interpret decompiled Windows code
- Analyze basic .NET and PowerShell malware and interpret WMI commands
- Use Ghidra, the open-source disassembler/decompiler

### Who should attend

Information technology staff, information security staff, corporate investigators and others who need to understand how malware functions operate and the processes involved in malware analysis.

### Prerequisites

General knowledge of computer and operating system fundamentals. Exposure to computer programming fundamentals and Windows Internals experience (recommended).

### Delivery method

In-person or virtual instructor-led training

### Duration

2 days (in-person delivery)
4 days (virtual delivery)

### What to bring

Students are required to bring their own laptop that meets the following specs:

- VMware Workstation 10+ or VMware Fusion 7+
- 30 GB of free HDD space

## Malware Analysis Crash Course

This course provides a rapid introduction to the tools and methodologies used to perform malware analysis on executables found in Windows systems using a practical, hands-on approach. The course explains how to find the functionality of a program by analyzing disassembly and seeing how it modifies a system and its resources as it runs in a debugger.

The course discusses how to extract host- and network-based indicators from a malicious program. It also covers dynamic analysis and the Windows APIs most often used by malware authors. Each section includes in-class demonstrations and hands-on labs with real malware so learners can apply their new skills.

### Learning objectives

After completing this course, learners should be able to:

- Quickly perform a malware autopsy
- Understand basic yet effective methods for analyzing running malware in a safe environment, such as virtual machines
- Understand the basics of the x86 assembly language
- Use IDA Pro, the main tool for disassembly analysis
- Understand a wide range of Windows-specific concepts that are relevant to analyzing Windows malware
- 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 and others who need to understand how malware operates and the processes involved in performing malware analysis.

### Prerequisites

Excellent knowledge of computer and operating system fundamentals. Computer programming fundamentals and Windows Internals experience are highly recommended.

### Delivery method

In-person or virtual instructor-led training

### Duration

3 days (in-person delivery)
4 days (virtual delivery)

### What to bring

Students are required to bring their own laptop that meets the following specs:

- VMware Workstation 10+ or VMware Fusion 7+
- 30 GB of free HDD space

## Malicious Documents Analysis

This course provides a rapid introduction to the file formats, tools, and methodologies used to perform malware analysis on malicious documents using a practical hands-on approach. Students will learn to pinpoint and analyze the most suspicious document components and how to extract host and network-based indicators from them. This course includes demonstrations and hands-on labs that contain real malware.

### Learning objectives

After completing this course, learners should be able to:

- Dissect and analyze malicious document formats
- Extract network and host-based indicators
- Extract noteworthy components that require further isolated analysis
- Detect suspicious patterns and common exploitation techniques
- Utilize modern analysis tools including Offvis and 010 editor
- Create and automate custom tools for your specific organization

### Who should attend

Malware researchers, software developers, information security professionals, incident responders, computer security researchers, corporate investigators and others who need to understand how malware operates and the processes involved in performing malware analysis.

### Prerequisites

General knowledge of computer and operating system fundamentals. Exposure to programming fundamentals is recommended.

### Delivery method

In-person instructor-led training

### Duration

2 days (in-person delivery)
3 or 4 days (virtual delivery)

### What to bring

Students are required to bring their own laptop that meets the following specs:

- VMware Workstation Pro 12.5 or newer (installed with the ability to run a VM)
- At least 30 GB of free HDD space

## Advanced Red Teaming Techniques: Malware Authoring and Repurposing

Malware techniques used to perform malicious actions are often similar to those used by antivirus and security products. Understanding how to write and design malware helps security analysts rapidly identify patterns of code when investigating a malicious binary.

Knowing how to design and develop each part of a payload enables red team members to reuse, debug, fix, or rewrite a solution.

Students will learn how to produce a shellcode blob capable of loading and injecting multiple malicious binaries via techniques repurposed from existing malicious samples. This course includes APIs and techniques used to perform common malicious functionality and extends these techniques to produce reliable payloads that function across operating system versions and limit exposure to security products.

The hands-on labs for this course are development-focused through use of C and Intel Assembly.

### Learning objectives

After completing this course, learners should be able to:

- Develop malicious applications using the Windows SDK
- Create position independent code (PIC) using C and Intel Assembly
- Write malicious code to perform code injection and modify a running application in-memory
- Analyze and modify a malicious binary to reuse functionality
- Design and write reliable payloads across a variety of operating system versions
- Use proven techniques to execute injections, hooking, and fingerprinting across various systems

### Who should attend

Software developers, information security professionals, incident responders, computer security researchers, corporate investigators and others who require an understanding of malware inner workings, crafting reliable shellcode and payloads, and rapid repurposing of malware samples.

### Prerequisites

Advanced knowledge of computer and operating system fundamentals and Windows internals. Familiarity with reverse engineering, Windows SDK and proficiency at developing in C is recommended.

### Delivery method

In-person instructor-led training

### Duration

4 days

### What to bring

Students are required to bring their own laptop that meets the following specs:

- VMware Workstation Pro 12.5 or newer (installed with the ability to run a VM)
- At least 30 GB of free HDD space

## Malware Analysis Master Course

Designed for experienced malware analysts, this course focuses on advanced topics related to combating a wider variety of more complex malware and malware defense mechanisms. It covers how to combat anti-disassembly, anti-debugging and anti-virtual machine techniques. It also discusses how to defeat packed and armored executables, analyze encryption and encoding algorithms and defeat various obfuscation techniques. Additional topics include malware stealth techniques (process injection and rootkit technology), analyses of samples written in alternate programming languages (C++) and popular software frameworks (.NET).

Learners will be taught to use existing tools and techniques as well as research and develop their own IDA Pro scripts and plugins. All concepts and materials are reinforced with demonstrations, real-world case studies, follow-along exercises and student labs to allow learners to practice new skills. Instructors are senior FLARE malware analysts who are experienced in fighting through state-of-the-art malware armor.

### Learning objectives

After completing this course, learners should be able to:

- Understand how malware hides its execution, including process injection, process replacement and user-space rootkits
- Grasp how shellcode works, including position independence, symbol resolution and decoders
- Comprehend the inner workings and limitations of disassemblers such as IDA Pro as well as how to circumvent the anti-disassembly mechanisms that malware authors use to thwart analysis
- Automate IDA Pro using Python and IDC to help analyze malware more efficiently
- Understand how to combat anti-debugging, including bypassing timing checks, Windows debugger detection and debugger vulnerabilities
- Fool malware so it cannot detect what is running in your safe environment
- Understand how malware analysis is influenced by C++ concepts like inheritance, polymorphism and objects
- Recognize common C++ structures from the disassembly
- Use disassembler features to enhance the reverse engineering process of C++ binaries
- Unpack manually by studying various packer algorithms and generic techniques to quickly defeat them
- See how x64 changes the game for malware analysis, including how WOW64 works and the architecture changes from x86
- Grasp string obfuscation techniques that are commonly used by malware, then take malware communications and analyze network packet captures
- Reverse engineer .NET bytecode and work with obfuscation techniques used by attackers

### Who should attend

Intermediate-to-advanced malware analysts, information security professionals, forensic investigators and others who need to understand how to overcome difficult and complex challenges in malware analysis.

### Prerequisites

Robust skill set in x86 architecture and the Windows APIs. Exposure to software development is highly recommended. Completion of Malware Analysis Crash Course is recommended but not required.

### Delivery method

In-person instructor-led training

### Duration

5 days

### What to bring

Students are required to bring their own laptop that meets the following specs:

- VMware Workstation Pro 12.5 or newer (installed with the ability to run a VM)
- At least 30 GB of free HDD space
- A licensed copy of IDA Pro that supports the MIPS architecture is recommended. The free version of IDA Pro will suffice.

# Advanced Acquisition and Testing Techniques

## Creative Red Teaming

Mandiant red teams have conducted hundreds of covert red team operations. This course draws on that knowledge to help learners improve their ability to prevent, detect, and respond to threats in an enterprise network.

Learners will better understand advanced threat actor behavior that Mandiant experts have observed through incident response investigations. Learners will also see how Mandiant red teams refine advanced attacker tools, tactics and procedures (TTPs) for use by red teams in their attempts to emulate advanced threat actors. Learners will develop the ability to think like an attacker and creatively use these TTPs to accomplish response goals while avoiding detection.

Mandiant red team leads conduct this fast-paced technical course with presentations and scenario-based labs based on frontline expertise and intelligence-based security research. Learners receive hands-on experience conducting covert cyber attack simulations that mimic real-world threat actors. They will learn how to bypass advanced network segmentation, multi-factor authentication and application whitelisting, abuse web applications, escalate privileges and steal data while circumventing detection methods.

### Learning objectives

After completing this course, learners should be able to:

- Identify, fingerprint and compromise a target with custom-crafted payloads while bypassing antivirus (AV) detection
- Deploy creative tactics—from older techniques to newer ones—to maintain access to any compromised machine
- Understand the tools and methods attackers use to exploit the lowest-level user privileges to gain higher, administrative privileges and move laterally throughout a network while avoiding security alerts
- Avoid and bypass various challenges such as application whitelisting, encryption, multi-factor authentication, sandboxes and more
- Exfiltrate data from "secure" networks undetected, without triggering firewalls or generating alerts
- Identify the goals and challenges of managing a red team operation, including risk measurement and reporting

### Who should attend

Red team members, penetration testers, defenders wanting to understand offensive tactics techniques and procedures (TTPs) and information security professionals looking to expand their knowledge base.

### Prerequisites

A background in conducting penetration tests, security assessments, IT administration, and/or incident response. Working knowledge of the Windows operating system, file systems, registry and use of the Windows command line. Experience with, Active Directory, basic Windows security controls, common network protocols, Linux operating systems, Scripting languages (PowerShell, Python, Perl, etc.) and assessment of web applications using the OWASP top 10.

### Delivery method

In-person or virtual instructor-led training

### Duration

4 days (in-person delivery)
5 days (virtual delivery)

### What to bring

Students are required to bring their own laptop that meets the following specs:

- USB port (for installing software provided on a USB stick)
- Ethernet port or adapter
- Local administrator rights to the host OS and VMs

## Practical Mobile Application Security

Smartphones have become an integral component of peoples' lives, both personally and in the business world—but application security is suspect.

This four-day course is designed to teach students the fundamentals of mobile application security for Google Android and Apple iOS mobile operating systems. It provides learners with the methodology, tools, and experience to assess the security of mobile applications.

### Learning objectives

After completing this course, learners should be able to:

- Describe device and application security models for the Android and iOS operating systems and their security features
- Build and configure a testing environment for both Android and iOS platforms with an awareness of jailbreaking, rooting, and other concepts
- Perform static analysis on APK and IPA files in a hands-on lab environment that covers Android Dalvik Bytecode, and Apple-compiled Swift and Objective-C assembly
- Understand what and where data should be stored, how it should be accessed, and what pitfalls are associated with improper data storage
- Analyze inter-process communication by interfacing with and fuzzing exposed components across both platforms
- Reliably intercept and modify network communications to bypass security features such as certificate pinning, taking into account the overlap and differences in mobile application API testing and traditional web application assessment
- Use common dynamic binary instrumentation (DBI) tools for application testing and data and code analyses in scenarios such as bypassing jailbreak/root detection or certificate pinning
- Compromise a test application, enumerate as many vulnerabilities as possible and consider recommendations for improving application security

### Who should attend

Security engineers, application developers, and penetration testers.

### Prerequisites

Background in security fundamentals, threat modeling, Linux CLI, object-oriented programming, and web application testing.

Recommended, but not required:

- ARM/AARCH64 assembly familiarity
- Java, Kotlin, Swift, or Objective-C programming experience
- Experience testing thick-client applications
- Web services (REST, SOAP, JSON) testing experience

### Delivery Method

In-person instructor-led training

### Duration

4 days

# Workshops

## Business Email Compromise

Business Email Compromise is a highly personalized two-to-four hour seminar in which students will develop the skills necessary to protect themselves and their organizations from email-based social engineering and malware.

The instructor will walk through a presentation of the technical information needed to avoid email threats, and will also host a Q&A session to ensure that your organization's specific concerns can be addressed.

Social engineering takes place in more than 90% of business compromises, and email is the most popular vector by far. Business Email Compromise training will help your organization be better protected from one of the greatest threats in the cyber security landscape.

### Learning objectives

After completing this course, learners should be able to:

- Identify the risks associated with BEC
- Avoid common pitfalls which make you vulnerable to Phishing and other social engineering attacks
- Define key terms so that the audience can make informed decisions regarding their email safety

### Who should attend

Any corporate employee in need of email security training or a refresher of the same.

### Delivery method

In-person or virtual instructor-led training

### Duration

2–4 hours (virtual delivery)

# Exercises and Preparedness

## ThreatSpace: Real-World Attack Scenarios

This intense three-day training covers the most modern, sophisticated attacks used by advanced persistent threat (APT) actors, and teaches students how to engage in effective analysis and incident response against real world threats.

Using a virtualized environment that simulates typical IT infrastructure such as network segments, workstations, servers and applications, teams use ThreatSpace to assess their technical capabilities, processes and procedures as they investigate simulated attack scenarios.

After a brief classroom session, two days of hands-on exercises take students through examples of real adversary activity and the process of responding to a nation-state level threat—all without actual risk. Students will perform triage and analysis, create timelines of activity, and report findings in real-time.

Experienced incident response practitioners facilitate the exercise and share practical experiences from the field. All exercises are conducted on-site using a cloud-based cyber range.

### Learning objectives

After completing this course, learners should be able to:

- Describe primary sources of data in incident response
- Perform triage and in-depth analysis of an affected enterprise network
- Effectively structure and organize a response team across multiple disciplines
- Identify malicious behavior and create useful timelines of activity

### ThreatSpace scenario samples

The scenarios, based on extensive Mandiant incident response experience responding to thousands of breaches, include the latest adversary tactics, techniques and procedures (TTPs) and test an organization's ability to detect, scope and remediate a targeted attack. Throughout the process, Mandiant incident response experts provide real-time feedback and coaching to help improve your security team's ability to respond to cyber attacks.

**Reconnaissance by Insider Threat**

This scenario emulates an insider threat with a valid user already on a system. This user opens a reverse shell session on the initial access host and uses it to discover information about the entire network.

**Beaconer Deployment**

This scenario imitates an attacker gaining access to a host via a spearphishing attachment. It opens a bypass session on that host and gathers information and deploys a beacon.

**Ransomware**

A domain user is compromised allowing the threat to access the system before moving laterally, conducting internal reconnaissance and establishing persistence. Once initial compromise is secured, the attacker deploys ransomware and runs malware on multiple mission critical systems.

**Active Directory**

A threat actor gains access to a host and begins discovery before conducting a Kerberoast attack and further reconnaissance of the domain. The actor then compromises the domain controller, exfiltrates passwords and disrupts normal business operations.

### Deliverables

• Half-day training and range familiarization.
• Two days of hands-on investigation of a simulated attack that progresses through the phases of the attack lifecycle. Mandiant incident responders provide real-time feedback and coaching to your incident responders and cyber threat analysts throughout the scenario.
• Debriefs to review team achievements and strengths as well as gaps in training, and processes and procedures, with recommendations for improvements.

After the engagement, you receive a report that identifies observed strengths and recommended enhancements to your organization's incident response capabilities.

### Who should attend

Incident responders at all skill levels, professionals who want to understand incident response in the context of APT attacks.

### Prerequisites

Familiarity with the incident response concepts, experience as an incident response team member.

### Delivery method

In-person or virtual instructor-led training

### Duration

3 days

## Senior Executive Mentorship Program

The Mandiant mentorship program is a one-on-one engagement that delivers high-level cyber security knowledge and understanding to organizational executives. By raising awareness of security risks and cyber attacks, it can help significantly reduce organizational risk.

Executives enrolled in this course will learn about critical cyber security concepts including international cyber law, the evolving role of government in cyber security operations, and the use of cyber threat intelligence as a force multiplier to limit business and organizational risk.

### Learning objectives

After completing this course, learners should be able to:

- Describe the core concepts of today's cyber security landscape
- Explain the impact of cyber security on the decision making process in the modern enterprise
- Understand how leaders must operate to be successful in the threat landscape relevant to their vertical market
- Grasp the process by which frontline experts can improve an organization's risk posture

### Who should attend

Executives and senior managers involved in the decision making processes for enterprises.

### Delivery method

In-person instructor-led training

### Duration

1 day

Learn more at **www.mandiant.com/academy**

**Mandiant**
11951 Freedom Dr, 6th Fl, Reston, VA 20190
703.935.1700
833.3MANDIANT (362.6342)
info@mandiant.com

**About Mandiant**

Since 2004, Mandiant has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
NOW PART OF Google Cloud