

ENTERPRISE INCIDENT RESPONSE MANAGEMENT

It is no secret that enterprises are under continuous attack from well-funded and talented attackers. MANDIANT has responded by raising the bar of effective incident response management with our Enterprise Incident Response Management class. This course will help students learn how best to meet the challenges faced by enterprises during incident response. This four day class has been specifically designed for information security professionals who manage incidents and incident response teams. This class introduces tried and true technical response methods and proven incident management techniques used every day by MANDIANT consultants. This class is designed as an operational course using case studies and hands-on lab exercises to ensure attendees are gaining experience in each topic area.

Duration	4 days
Who Should Attend	Information technology managers, information security managers, CERT team managers, or other staff that have a need to perform Incident Response or investigate suspect network and systems use/misuse.
Prerequisites	Students should have a basic understanding of TCP/IP networks and familiarity with Windows and UNIX systems. Familiarity with computer security terminology and concepts would be helpful.
Students Will Learn	<ul style="list-style-type: none">▪ The different phases and activities of the Incident Response process▪ To properly staff and prepare an Incident Response Team▪ To create working documentation and checklists usable during battle▪ How to prepare an enterprise network for agile incident response▪ To rapidly detect and confirm attacks against Windows and Unix systems▪ To find, review, and interpret Windows and Unix log files▪ To perform live response on compromised Windows & UNIX systems▪ To collect the volatile evidence present on a live system must prior to the system being powered down▪ To recover deleted files from Kernel memory on UNIX systems▪ How to dump the memory associated with suspicious processes▪ To detect loadable kernel modules, rootkits, and trojaned files▪ Steps involved in the creation of a secure Incident Response toolkit▪ To find hidden files and export protected files such as hiberfil.sys and pagefile.sys from Windows systems with FTK imager
Exercise Overview	<ul style="list-style-type: none">▪ Exploitation Frameworks▪ Create Trusted Response Kit▪ Windows Incident Response▪ Linux Incident Response▪ Windows Memory Analysis▪ FTK and DD Imaging▪ Find Evil Exercises▪ How to Automate Live Response Data Collection▪ Windows Rootkits▪ Intro to Network Monitoring▪ Final Exercise▪ UNIX rootkits
Course Materials	<ul style="list-style-type: none">▪ Student manual▪ Class handouts▪ MANDIANT gear▪ Free Tools CD with course tools and scripts
Suggested Next Courses	<ul style="list-style-type: none">▪ Advanced Incident Response▪ Malware Analysis I
Contact	1.800.647.7020 education@mandiant.com www.mandiant.com/education.htm

Case Study

A recent Incident will be walked through from the initial Incident discovery to the investigative process used to identify probable cause and how the incident concluded. Actual cleansed case data will be used to illustrate key points.

Exploitation Frameworks

We provide hands on experience and expose the student to the newest forms of automated computer intrusion tools. This section covers the new tools an attacker uses when he wants to "hack" into a computer system. Specifically, attendees will learn about port scanning, banner grabbing, operating system fingerprinting, how the Metasploit Framework helps automate the computer intrusion process, and various delivery mechanisms for spear phishing attacks. Students will get hands on experience performing the steps that the attacker may take prior to and during the exploitation of computer systems.

The Incident Response Process

We formally discuss the different phases of Incident Response, and the activities commonly associated with each phase. Specifically, we outline the process of Incident Response, from Incident Detection through Incident Resolution. We discuss the challenges to each phase, and how understanding the Incident Response process is critical to appropriate pre-incident planning.

Incident Response Program Development

This section presents a framework for incident response program development in the enterprise. This includes documentation, checklists, forms, and the various corporate policies that are essential to posture an organization to prevent, minimize, and recoup losses and foster and more rapid and complete response process. These documents will be used throughout the class to provide a documentation framework for the incident responses that follow. Additional policies will be discussed that can shield a company from liability from various state and federal regulations, and can be used as a sword to preserve companies' options for taking offensive steps when they are the victims.

Enterprise Preparation

Students will learn what methods are commonly used by MANDIANT to quickly prepare a network for host-based and network-based indicator detection. This section includes discussion on current security technologies and their strengths and weaknesses as they relate to finding evil and solving crime on a network.

Windows Incident Response

Students learn the steps required during a live response on a compromised Windows system. The "live response" introduces a method to obtain all volatile information in a forensically sound manner. Students review this information to identify rogue processes (backdoors or sniffers...) on a system, capture all the current network connections for later review, and basically retrieve all pertinent data that would be lost if the system was simply powered down. Different depths of the live response will be discussed to facilitate a complete, "live" investigation when forensic duplication is not an option for the responder.

Windows Exercise

Students will respond to a windows intrusion and will be guided through the response process including live response analysis, forensic preservation, case documentation and reporting. Evil will be found, and crime will be solved.

Scenario Challenges

It is important for students to be faced with the most common types of incidents they will actually encounter in the field. MANDIANT leverages its experience to discuss two cases, one dealing with evidence discovery, and the other dealing with incident response. Students will be challenged to handle the incident in accordance with best practices and their own policies and procedures. Discussion points include comprehension of the actual issues, proper documentation and risks, identification of the "bar of disclosure" and the challenges with incident response and electronic evidence discovery.

Unix Incident Response

We cover the commands and methods used to perform live response on a UNIX system. This includes a review of the `/proc` file system as well as acquiring volatile system information. We discuss the review of the volatile data collected during the live response process. Students also learn to script the live response process in an effort to minimize response times. This section provides an intense primer on over 30 important UNIX commands that security experts and investigators need to know.

Students learn how to find and review important UNIX log files and system files. As an example, students learn how to review the `/etc/passwd` file to look for unauthorized user accounts or privileges, review the `/etc/shadow` file to ensure every account requires password authentication, the `/etc/groups` file to look for escalation in privileges and scope of access, and the `/etc/hosts` file to list the local DNS entries. Students also learn how to interpret other important configuration files, and how attackers often manipulate these files.

UNIX Exercise

Students will perform a lab exercise where they review data collected from a compromised UNIX system, find evil and solve crime.

Network Monitoring

Students will learn how to monitor their network for additional signs of compromise using information gained during the Incident Response process. This includes discussion of several types of monitoring including statistical, connection based, full content and event based (IDS) monitoring.

Introduction to Computer Forensics

Students will learn how to use common UNIX utilities to create bit-for-bit forensic images. Students will also learn how to access protected files on windows systems including memory and SAM files for storage and analysis. Proper evidence handling and documentation will be discussed.

Rootki

This section begins with a discussion of “kernel” space and “user” space, and how operating systems function. It dovetails into how attackers use “kernel” space tools to hide their malicious code, as well as cover their tracks when they exploit systems. Since “kernel” space backdoors are growing in popularity, there is an in-depth discussion of how to detect “kernel” level malicious code, including cross-view diffs, reviewing a system for hooks, verifying system integrity, and preventing “kernel” level attacks by protecting the install path. Students perform an exercise where they execute a kernel level program and learn how such attacks undermine current “user” space responses.

Memory Analysis and Rootkit Detection

Once students have learned the basics of rootkits, the final rootkit detection mechanism, memory analysis, is discussed in depth. Students will be introduced to memory analysis, and perform an exercise where they conduct memory analysis and identify hidden processes.

Introduction to Malware Analysis

Students are given a high level overview of malware analysis so they are equipped to understand the advantages and challenges with malware analysis during incident response.

Final Exercise

Students will be presented with a “live” compromised system (frozen in a state of compromise within VMware) and perform Live Response to determine the scope and nature of the compromise using a trusted incident response kit contained within a CDROM ISO image.

Pre-captured Live Response data will also be made available to facilitate student’s completion of this module.