FIREEYE | MANDIANT

CATALOG

Training Courses

Catalog of Instructor-Led and Web-Based Training

Contents

Cyber Security Training from Mandiant

Instructor-Led Training Courses

Introductory Courses

Intelligence and Attribution Courses

Incident Response Courses

Malware Analysis Courses

Advanced Acquisition and Testing Techniques

Workshops

Exercises and Preparedness

Introduction

Course Listings
Courses in this catalog are divided into two broad categories:

- Product training from FireEye, which covers the core functionality of FireEye products and solutions, including deployment, administration, usage and troubleshooting during detection, analysis, investigation and response activities
- Cyber security training from Mandiant Solutions covers essential cyber security skills that use free, open-source or existing customer technologies, whether or not they are FireEye solutions

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 the acquisition of practical skills.

All of our instructors are security professionals with years of security experience. FireEye instructors have extensive experience working with FireEye solutions; and Mandiant instructors have applied their skills 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 online courses that can be accessed at any time, from any location. Learners may pause and resume training as their schedule allows. The training is practical and abbreviated; it does not contain hands-on labs or exercises.

Our web-based training is designed to work in modern desktop browsers (Chrome, Firefox, Safari, Internet Explorer 10+ and Microsoft Edge) and tablets (such as iPad) without the use of browser plugins. Technology needs and exceptions are noted in course descriptions when applicable.

The duration of a single web-based training course can range from 45 minutes to a full day.

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 FireEye 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.

Product Training from FireEye	Onsite ILT	Offsite ILT	Virtual ILT	Web-Based Training	Public ILT (Per Seat)	Public VILT (Per Seat)
Alert Analysis and Diagnostics with FireEye Email Security—Server Edition	x	x	x		x	x
Alert Analysis with FireEye Email Security—Cloud Edition	x	x	x		x	x
Alert Analysis with FireEye File Protect	x	x	x		x	x
Alert Triage with FireEye Malware Analysis	x	x	x		x	x
Cyber Threat Hunting	x	x	x		x	x
FireEye Alert Analysis and Endpoint Investigations	x	x	x		x	x
FireEye Email Security—Server Edition Administration and Diagnostics	x	x	x		x	x
FireEye Endpoint Security Administration and Diagnostics	x	x	x		x	x
FireEye Helix	x	x	x		x	x
Fundamentals of Network Traffic Analysis using FireEye Network Forensics	x	x	x		x	x
Helix Threat Analytics	x	x	x		x	x
Investigations with FireEye Endpoint Security	x	x	x		x	x
FireEye Network Security Administration and Diagnostics	x	x	x		x	x
Central Management (CM) Deployment				x		
Email Security—Cloud Edition				x		
Email Security (EX) Deployment				x		
Endpoint Security for Analysts				x		
Endpoint Security for System Administrators				x		
File Content Security (FX) Deployment				x		
Malware Analysis (AX) Deployment				x		
Network Forensics (PX) Deployment				x		
Network Security (NX) Deployment				x		

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				
Analytic Tradecraft Workshop	x	x	x		x	x
Audits and Compliance in the Cyber Domain	x	x				
Business Email Compromise	x	x	x		x	x
Combined Windows-Linux Enterprise Incident Response	x	x	x			
Creative Red Teaming	x	x	x		x	x
Cyber Intelligence Foundations	x	x	x		x	x
Cyber Intelligence Production	x	x	x	x		
Cyber Intelligence Research I—Scoping	x	x	x	x		
Cyber Intelligence Research II—Open Source Intelligence (OSINT)	x	x	x	x		
Cyber Security Awareness	x	x	x	x	x	x
Cyber Security Operations and Organization	x	x	x		x	x
Cyber Security Policy and Implementation	x	x				
Digital Forensics and Incident Response for PLCs	x	x				
Essentials of Malware Analysis	x	x	x		x	x
Fundamentals of Cyber Security	x	x				
Fundamentals of Industrial Control Systems (ICS) Security	x	x	x		x	x
Hunt Mission Workshop	x	x	x		x	x
Introduction to Cyber Crime for Executives	x	x	x		x	x
Introduction to Threat Intelligence and Attribution	x	x	x		x	x
Linux Enterprise Incident Response	x	x	x		x	x
macOS Malware Analysis for Reverse Engineers	x	x				
Malicious Documents Analysis	x	x				
Malware Analysis Crash Course	x	x	x		x	x
Malware Analysis Master Course	x	x				
Mandiant Security Validation Security Instrumentation Platform Bootcamp	x	x	x			
Network Traffic Analysis	x	x	x	x	x	x
Practical Mobile Application Security	x	x				
Router Backdoor Analysis	x	x				
Security and the Software Development Lifecycle	x	x	x		x	x
Senior Executive Mentorshop Program	x	x				
Threatspace: Real-World Attack Scenarios	x	x				
Windows Enterprise Incident Response	x	x	x	x	x	x

Product Training from FireEye
Instructor-Led Training Courses

Alert Analysis and Diagnostics with FireEye Email Security—Server Edition

This two-day course is designed to show analysts and email administrators how to effectively use FireEye Email Security—Server Edition to detect, contain and diagnose email threats.

Day 1 is primarily for analysts who need to derive meaningful, actionable information from FireEye alerts to assess and triage threats to their environment. It introduces FireEye Email Security—Server Edition and its primary capabilities, including detection of malicious files and URLs, email alerts and containment through quarantine.

Day 2 introduces a framework for administration and diagnostics of Email Security—Server Edition. It includes checklists, case studies, lab challenges and guidance for transitioning difficult cases to the FireEye support team. This hand-on workshop gives learners practical experience administering an Email Security appliance and diagnosing common issues.

Learning Objectives
After completing this course, learners should be able to:

- Recognize current malware threats and trends
- Understand the threat detection and prevention capabilities of Email Security – Server Edition
- Locate and use critical FireEye alert information to assess a potential threat
- Examine OS and file changes in alert details to identify malware behaviors
- Identify Indicators of Compromise (IOCs) in a FireEye alert and use them to identify compromised hosts
- Identify common issues and steps for resolution with Email Security deployment
- Perform administration tasks on the Email Security—Server Edition appliance
- Recognize underlying technology and protocols of SMTP email transfer
- Using logs, determine status of email transfer and analysis
- Know when to escalate issues and obtain further assistance from FireEye

Who Should Attend
Security professionals, incident responders and email administrators.

Prerequisites
A working understanding of networking, email security and email support.

Duration
2 days

Alert Analysis with FireEye Email Security—Cloud Edition

This one-day course provides an overview of Email Security—Cloud Edition core functionality, including administration procedures and alert analysis.

Hands-on activities include rule and policy creation, alert generation and the breakdown and analysis of information found in FireEye email alerts that is used in incident reporting.

Learning Objectives

After completing this course, learners should be able to:

- Describe how Email Security detects and protects against malware
- Demonstrate knowledge of the email analysis process
- Configure Email Security settings, policies and notifications
- Describe the various queues used for email management and processing
- Identify alerts correlated with Network Security with and without Central Management
- Find critical alert information on the Dashboard
- Access and manage alerts and quarantined emails
- Examine OS and file changes in alert details to identify malware behaviors and triage alerts

Who Should Attend

Analysts and administrators responsible for the set up and management of Email Security—Cloud Edition.

Prerequisites

A working understanding of networking and network security and Windows operating and file systems.

Duration

1 day

Alert Analysis with FireEye File Protect

This one-day course is designed to prepare analysts to triage and derive meaningful, actionable information from alerts on FireEye File Protect.

A hands-on lab environment presents learners with various types of alerts and real-world scenarios and gives them the opportunity to conduct in-depth analysis on the behavior and attributes of malware to assess real-world threats.

Learning Objectives

After completing this course, learners should be able to:

- Recognize current malware threats and trends
- Understand the threat detection and prevention capabilities of File Protect
- Locate and use critical information in a File Protect alert to assess a potential threat
- Examine OS and file changes in alert details to identify malware behaviors and triage alerts
- Identify Indicators of Compromise (IOCs) in a File Protect alert and use them to identify compromised hosts

Who Should Attend

Security professionals, incident responders and FireEye analysts.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

1 day

Alert Triage with FireEye Malware Analysis

This one-day course is designed to prepare learners to perform alert triage using the FireEye Malware Analysis appliance.

Learners will be able to administrate and use the FireEye Malware Analysis appliance. A hands-on lab environment offers learners an opportunity to submit malware samples for deep analysis and then interpret the results.

Learning Objectives

After completing this course, learners should be able to:

- Describe malware behaviors, stages of an attack (malware lifecycle) and current trends in the threat landscape
- Explain the process and initial steps of conducting malware analysis
- Differentiate between static and dynamic analysis
- Understand the features and functions of the Malware Analysis appliance
- Submit malware samples to the appliance for deep analysis and alert triage
- Locate and use critical information in analysis results to assess a potential threat
- Identify IOCs in analysis results
- Examine the use of YARA rules on FireEye appliances

Who Should Attend

Security analysts or incident responders who are responsible for enterprise threat management.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

1 day

Cyber Threat Hunting

This two-day course covers the fundamentals of threat hunting, how to build out a hunt program in your own environment and how to identify, define and execute a hunt mission. The course introduces essential concepts for network and endpoint hunting and then allows learners to apply techniques to hunt for anomalous patterns. Hands-on activities follow real-world use cases to identify attacker techniques. Learners will leave the course with concrete use cases that they can apply to hunt in their own environment.

Throughout the course, instructors provide guidance on hunting across typical security toolsets such as SIEM, packet capture and endpoint detection and response (EDR). Learners do not need a prior knowledge of specific FireEye technology, but lab activities do use FireEye Helix, FireEye Endpoint Security (HX) and FireEye Network Forensics (PX/IA). For example, endpoint hunting use cases rely on either Endpoint Security, Helix or both, to acquire data used in the hunt mission.

Learning Objectives

After completing this course, learners should be able to:

- Define cyber threat hunting and articulate its value to an organization
- Create or enhance an existing hunting program
- Apply provided use cases for your hunting program
- Build hunt missions for threat hunting in your organization
- Use both endpoint and network data for successful hunting
- Implement a hunting mission to hunt and find threats and automate the hunting process

Who Should Attend

Network security professionals and incident responders who will be using security and logging products to assist with their network and endpoint hunting responsibilities.

Prerequisites

Completion of the **Endpoint Investigations** course in addition to a working understanding of networking and network security and the Windows operating system, file system, registry and regular expressions, as well as basic experience scripting in Python (or similar) language.

Duration

2 days

Cyber Threat Hunting Workshop

This three-day course shows how to shape a sustainable hunting program. Learners with existing hunt programs will learn how to incorporate a repeatable, flexible and efficient process around existing hunting activities, build consistent practices that are based on their organization's threat profile, and measure their capability for success.

Participants learn to proactively detect threats, build out a process workflow and develop use cases that include cyber threat intelligence. FireEye consultants showcase critical knowledge and experience using case studies from the field.

This course introduces essential concepts for network and endpoint hunting and then allows learners to apply techniques to hunt for anomalous patterns. Hands-on activities follow real-world use cases to identify attacker techniques. Learners will leave the course with concrete use cases that they can apply to hunt in their own environment.

Throughout the course, instructors provide guidance on hunting across typical security toolsets such as SIEM, packet capture and endpoint detection and response (EDR). Learners do not need a prior knowledge of specific FireEye technology, but lab activities do use FireEye Helix, FireEye Endpoint Security (HX) and FireEye Network Forensics (PX/IA). For example, endpoint hunting use cases rely on either Endpoint Security, Helix, or both, to acquire data used in the hunt mission.

Learning Objectives

After completing this course, learners should be able to:

- Define cyber threat hunting and articulate its value to an organization
- Create or enhance an existing hunting program
- Build out a repeatable, consistent and efficient hunting process workflow
- Develop hunting use cases based on an organization's threat profile
- Use both endpoint and network data for successful hunting
- Implement a hunting mission to hunt and find threats and automate the hunting process
- Measure the capability and success of a hunting program

Who Should Attend

Learners attempting to build a hunting program or refine an existing hunting program will benefit from this course. The fast-pace and technical content is intended for learners with a background that includes one or more of the following elements: incident response, forensic analysis, network traffic analysis, log analysis, security assessments and penetration testing. Managers or those with oversight of incident response or hunt teams or related investigative tasks will also find this course valuable.

Prerequisites

Completion of the **Endpoint Investigations** course or an equivalent foundation in incident response in addition to a working understanding of networking and network security, the Windows operating system, file system, registry and regular expressions, as well as basic experience scripting in Python (or similar) language.

Duration

3 days

FireEye Alert Analysis and Endpoint Investigations

This three-day course examines how to triage alerts generated by FireEye Network Security, derive actionable information from those alerts and apply the fundamentals of live analysis and investigation to investigate associated endpoints.

Hands-on activities span the entire analysis and live investigation process, beginning with a FireEye-generated alert and continuing to discovery and analysis of the host for evidence of malware and other unwanted intrusion. Analysis is performed using FireEye products and freely available tools.

Investigation techniques highlight FireEye Endpoint Security features such as Triage Summary and Audit Viewer.

Learning Objectives

After completing this course, learners should be able to:

- Recognize current malware threats and trends
- Interpret alerts from FireEye Network and Endpoint Security products
- Locate and use critical information in FireEye alerts to assess a potential threat
- Define IOCs based on a FireEye alert and identify compromised hosts
- Describe methods of live analysis
- Create and request data acquisitions to conduct an investigation
- Define common characteristics of Windows processes and services
- Investigate a Redline® triage collection using a defined methodology
- Identify malicious activity hidden among common Windows events
- Validate and provide further context for alerts using Redline

Who Should Attend

Network security professionals and incident responders who must use FireEye technologies to detect, investigate and prevent cyber threats.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and regular expressions and experience scripting in Python. The **FireEye Network Security Deployment** and **FireEye Endpoint Security Deployment** courses are recommended.

Duration

3 days

FireEye Email Security - Server Edition Administration and Diagnostics

This one-day course introduces an administration and diagnostics framework for the FireEye Email Security—Server Edition (EX). The course includes checklists, case studies, lab challenges and guidance for transitioning difficult cases to the FireEye support team.

This hands-on workshop gives learners practical experience in administering an Email Security appliance and diagnosing common issues

Learning Objectives

After completing this course, learners should be able to:

- Address issues encountered with Email Security deployment
- Administer the Email Security appliance
- Describe the underlying technology and protocols of SMTP email transfer
- Use logs to determine status of email transfer and analysis
- Identify and resolve common issues
- Obtain further assistance as needed

Who Should Attend

Administrators who must regularly resolve security issues in architectures that include FireEye Email Security—Server Edition appliances.

Prerequisites

Experience with network administration and email support.

Duration

1 day

FireEye Endpoint Security Administration and Diagnostics

This two-day course introduces deployment, configuration and basic administration for FireEye Endpoint Security. From this baseline, the workshop introduces a framework for troubleshooting the FireEye Endpoint Security Server and Agent. The course includes checklists, case studies and guidance for transitioning difficult cases to the FireEye support team. Optional modules expand this workshop to cover FireEye core hardware and virtual appliances.

This hands-on workshop gives learners practical experience administering Endpoint Security, adjusting common configurations and resolving common issues.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components needed to deploy FireEye Endpoint Security
- Identify the main phases of Endpoint Security operation
- Perform the initial configuration of Endpoint Security appliances and hosts
- Create custom rules
- Understand core analyst features of Endpoint Security such as alerting, enterprise search and containing endpoints
- Resolve issues commonly encountered with Endpoint Security Agent policy exclusions
- Validate endpoints to ensure that they are performing as expected
- Use Endpoint Security logs and diagnostics for troubleshooting
- Explore common issues across core installations
- Understand common issues with hardware and virtual appliances

Who Should Attend

Network security professionals and FireEye administrators and analysts who must set up or work with FireEye Endpoint Security

Prerequisites

Experience with network administration and support.

Duration

2 days

FireEye Helix

This primer on FireEye Helix covers the Helix workflow, from triaging Helix alerts, creating and scoping cases and using Helix and Endpoint Security tools to conduct investigative searches across the enterprise. Hands-on activities include writing MQL searches as well as analyzing and validating Helix, Network Security and Endpoint Security alerts.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components needed to deploy Helix
- Determine which data sources are most useful for Helix detection and investigation
- Search log events across the enterprise
- Locate and use critical information in a Helix alert to assess a potential threat
- Pivot between the Helix web console and FireEye Network and Endpoint Security platforms
- Validate Network Security and Endpoint Security alerts
- Use specialized features of Network Security and Endpoint Security to investigate and respond to potential threats across enterprise systems and endpoints

Who Should Attend

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

Prerequisites

Completion of three FireEye web-based training courses prior to the instructor-led portion of the course: Network Security for Helix, Central Management for Helix, FireEye Endpoint Security for Analysts. Details on these courses will be provided to registrants of the FireEye Helix instructor-led training course. Students should have a working understanding of networking and network security, the Windows operating system, file system, registry, and use of the CLI.

Duration

4 days

FireEye Network Security Administration and Diagnostics

This one-day workshop introduces an administration and diagnostics framework for FireEye Network Security (NX) appliances. The course includes checklists, case studies, lab challenges and guidance for transitioning difficult cases to the FireEye support team.

This hands-on workshop gives attendees practical experience administering the appliance and diagnosing common issues.

Learning Objectives

After completing this course, learners should be able to:

- Recognize and understand issues that may arise during Network Security deployment
- Resolve issues commonly encountered in architectures that include Network Security appliances
- Explore common issues across core installations
- Administer the Network Security appliance
- Use logs to determine status
- List their options for obtaining further assistance

Who Should Attend

FireEye Network Security appliance administrators who must regularly resolve network security issues.

Prerequisites

Experience with network administration and support.

Duration

1 day

Fundamentals of Network Traffic Analysis using FireEye Network Forensics

This course covers the fundamentals of network flow analysis, session analysis, application metadata analysis and reconstruction of data from full content using FireEye Network Forensics, which is comprised of packet capture appliances (PX) and investigation analysis appliances (IA).

Hands-on activities include using FireEye Network Forensics to perform search queries and filtering, and following alerts from integrated FireEye solutions.

Learning Objectives

After completing this course, learners should be able to:

- Describe the deployment of FireEye Network Forensics in the context of FireEye products and services that may be part of the environment used for network traffic monitoring and analysis.
- Define connection, packet, and session data in the context of network traffic analysis.
- Perform network traffic analysis using FireEye Network Forensics.
- Reconstruct files or artifacts from full network packet data from resulting session data events using FireEye Network Forensics.
- Follow threat alerts from integrated FireEye solutions (Email Security, Network Security, Endpoint Security) and intelligence feeds that aid in breach investigation and hunting processes.

Who Should Attend

Network security professionals and incident responders who must work with FireEye Network Forensics packet capture (PX) and investigation analysis (IA) appliances to analyze cyber threats through packet data.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

1 day

Helix Threat Analytics

This course covers the Helix work flow, triaging Helix alerts, creating and scoping cases from an alert, and using Helix Threat Analytics during investigation. Hands-on activities include writing MQL searches, as well as analyzing and validating Helix alerts.

Learning Objectives

After completing this course, learners should be able to:

- Determine which data sources are most useful for Helix detection and investigation
- Search log events across the enterprise
- Locate and use critical information in a Helix alert to assess a potential threat
- Create a case from events of interest
- Create and manage IAM users

Who Should Attend

Network security professionals and incident responders who must work with Threat Analytics to analyze data in noisy event streams.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

2 days

Investigations with FireEye Endpoint Security

This course covers the fundamentals of live analysis forensics and investigation for endpoints.

Hands-on activities span the entire forensics process, beginning with a FireEye-generated alert, leading to discovery and analysis of the host for evidence of malware and other unwanted intrusion. Analysis of computer systems will be performed using FireEye products and freely available tools.

For FireEye Endpoint Security (HX) customers, activities focus on investigation techniques using features such as the Triage Summary and Audit Viewer. Optionally, students can work with the Endpoint Security API to automate actions and explore integrating Endpoint Security with other systems.

Learning Objectives

After completing this course, learners should be able to:

- Describe methods of live analysis
- Use core analyst features of Endpoint Security such as alerting, enterprise search and containing endpoints
- Investigate a Redline triage package using a defined methodology
- Validate and provide further context for FireEye alerts
- Identify malicious activity hidden among common Windows events

Who Should Attend

Network security professionals and incident responders who must use FireEye Endpoint Security to investigate, identify and stop cyber threats.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and regular expressions, and experience scripting in Python.

Duration

2 days

Product Training from FireEye
Web-Based Training Courses

Central Management (CM) Deployment (WBT)

This entry-level self-paced online course covers deployment options, basic administration and core functionality for FireEye Central Management (CM) appliances, the administration of other FireEye appliances (Network Security, Email Security, File Content Security, Malware Analysis) using FireEye Central Management and the submission of malware detected by Network Security, Email Security or File Content Security directly to Malware Analysis using the Central Management user interface.

Learning Objectives

After completing this course, learners should be able to:

- Deploy, install, and configure a FireEye Central Management appliance
- Administer other FireEye appliances using Central Management
- Identify potentially compromised hosts
- Identify recipients of malicious emails
- Correlate web and email attacks
- Submit malware detected by FireEye Network Security, Email Security or File Content Security directly to Malware Analysis using the Central Management web user interface

Who Should Attend

Network security professionals and incident responders who must set up or work with FireEye Central Management.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

45-60 minutes

Email Security—Cloud Edition (WBT)

This self-paced online course provides an overview of the features and detection capabilities of FireEye Email Security—Cloud Edition. It also covers email policy and rule configuration, email quarantine and alert administration.

Learning Objectives

After completing this course, learners should be able to:

- Review common email attack methods
- Describe detection capabilities and benefits of Email Security—Cloud Edition
- Demonstrate knowledge of the email analysis process
- Configure email settings and policies with Email Security—Cloud Edition
- Detail the integration process with FireEye Network Security and be able to identify correlated network and email alerts
- Find critical information on the Email Security dashboard
- Access and manage alerts
- Examine OS and file changes in alert details for malicious behaviors
- Access and manage quarantined emails
- Perform message searches using Email Trace

Who Should Attend

Security analysts and administrators who must set up and mange Email Security—Cloud Edition.

Prerequisites

None

Duration

51 minutes

Email Security (EX) Deployment (WBT)

This entry-level self-paced online course covers deployment options, basic administration and core functionality for FireEye Email Security (EX) appliances.

Learning Objectives

After completing this course, learners should be able to:

- Deploy, install and configure a FireEye Email Security appliance
- Administer FireEye Email Security appliances
- Identify recipients of malicious emails

Who Should Attend

Network security professionals, incident responders and FireEye administrators and analysts who must set up or work with a FireEye Email Security appliance.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

45-60 minutes

Endpoint Security for Analysts (WBT)

This entry-level online course covers core functionality of FireEye Endpoint Security, including features, operational workflows, alert analysis and containment.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components of Endpoint Security
- Describe the communication between the Endpoint Security Server and Agent
- Describe the function of the ring buffer
- Create hosts sets
- Create custom threat indicators
- Identify critical information in an Endpoint Security alert
- Request and approve hosts for containment
- Use Enterprise Search to find artifacts on managed hosts
- Acquire files and triages from hosts
- Review a triage or acquisition using Audit Viewer

Who Should Attend

Analysts and incident responders who use FireEye Endpoint Security.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, and Windows registry.

Duration

2-2.5 hours

Endpoint Security for System Administrators (WBT)

This entry-level online course covers deployment options, basic administration and core functionality for FireEye Endpoint Security.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components needed for Endpoint Security
- Identify the critical phases of Endpoint Security operation
- Perform the initial configuration of Endpoint Security Server
- Configure the Endpoint Agent and create custom policies
- Configure Malware Protection
- Create host sets
- Create custom threat indicators
- Request and approve hosts for containment
- Review high-level alert details
- Use Enterprise Search to find artifacts on managed hosts
- Request files and triage packages for hosts

Who Should Attend

System administrators and security professionals who must set up and work with FireEye Endpoint Security.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

2-2.5 hours

File Content Security (FX) Deployment (WBT)

This entry-level self-paced online course covers deployment options, basic administration and core functionality for FireEye File Content Security (FX) appliances.

Learning Objectives

After completing this course, learners should be able to:

- Deploy, install and configure FireEye File Content Security appliances
- Administer File Content Security appliances
- Configure a file share for remote scan
- Schedule recurring file share scans
- Review the results of a network file share scan

Who Should Attend

Network security professionals and incident responders who must set up or work with FireEye File Content Security.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

45-60 minutes

Malware Analysis (AX) Deployment (WBT)

This entry-level self-paced online course covers deployment options, basic administration and core functionality for FireEye Malware Analysis (AX) appliances.

Learning Objectives

After completing this course, learner should be able to:

- Deploy, install and configure a FireEye Malware Analysis appliance
- Administer Malware Analysis appliances
- Submit malware samples for deep inspection
- Review the results of malware analysis

Who Should Attend

Network security professionals, incident responders and FireEye administrators and analysts who must set up or work with FireEye Malware Analysis.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

45-60 minutes

Network Forensics (PX) Deployment (WBT)

This entry-level self-paced online course covers deployment options, basic administration and core functionality for the FireEye Network Forensics packet capture (PX) appliances.

Learning Objectives

After completing this course, learners should be able to:

- Describe the FireEye Network Forensics packet capture appliance
- Illustrate how the packet capture appliance is deployed in a typical network
- Search and filter connection and session data using the packet capture appliance
- Reconstruct session data for a malicious breach using the packet capture appliance

Who Should Attend

Network security professionals and incident responders who must work with FireEye Network Forensics packet capture appliances (PX) to process large amounts of high-speed packet data.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

2.5-3 hours

Network Security (NX) Deployment (WBT)

This entry-level self-paced online course covers deployment options, basic administration and core functionality for FireEye Network Security (NX) appliances.

Learning Objectives

After completing this course, learners should be able to:

- Deploy, install and configure a FireEye Network Security appliance
- Administer FireEye Network Security appliances
- Identify potentially compromised hosts

Who Should Attend

Network security professionals, incident responders and FireEye administrators and analysts who must set up or work with a FireEye Network Security.

Prerequisites

A working understanding of networking and network security, the Windows operating system, file system, registry and use of the command line interface (CLI).

Duration

45-60 minutes

Cyber Security Training from Mandiant
Instructor-Led Training Courses

Introductory Courses

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-classroom or virtual instructor-led training

REGISTER FOR WEB-BASED TRAINING

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

Cyber Security Operations and Organization

This course orients senior leaders on effective cyber security operations, how to organize and equip a security operations center and the role every department within the organization plays in defending the enterprise. It also reviews critical considerations for a governance and policy program and details the intricacies of a risk management program from a cyber security perspective.

Learners will see how to incorporate cyber security principles in enterprise architecture and exactly how a robust vulnerability management program can reduce their attack surface to improve their security posture. They will examine the value of augmenting cyber security staff by training all employees to recognize and report cyber threats. Learners will also walk through the incidence response process to gain an high-level understanding of how threat intelligence contributes to the threat hunting process.

Learning Objectives

After completing this course, learners should be able to:

- Effectively write, publish, enforce and socialize security policy
- Identify common risk management principles and establish a risk management program
- Describe basic security architecture and ask essential questions during architecture planning
- Apply a robust vulnerability management program to help reduce their attack surface
- Establish a well-organized and effective security awareness program
- Explain the challenges an organization faces after its computer security defenses are breached

Who Should Attend

Cyber security directors, managers, senior cyber security analysts and other information technology leaders in cyber security roles, or other leadership roles supporting cyber security functions.

Prerequisites

A solid understanding of security operation center operations and functional roles is recommended, but not required.

Delivery Method

In-classroom and virtual instructor-led training

Duration

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

Fundamentals of Industrial Control Systems (ICS) Security

This three-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-classroom and virtual instructor-led training

Duration

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

Technical Requirements

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-classroom 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-classroom 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-classroom instructor-led training

Duration

5 days

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 FireEye 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-classroom or virtual instructor-led training

Duration

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

Hunt Mission Workshop

This fast paced entry-level workshop teaches the fundamentals of creating a structured, repetitive, and documented intel-led hunt in your own organization.

Students will learn how to employ a process framework to scope, execute, and validate the results of a network hunting operation and ensure each hunt mission is used to improve the organization's overall network security posture.

Learning Objectives

After completing this course, learners should be able to:

- Describe how to integrate a hunt capability into their conventional cyber security operations
- Conduct gap analysis
- Utilize a hunt process framework for repeated, structured hunts
- Develop a custom workflow for their own environments

Who Should Attend

SOC managers, intelligence analysts, threat hunters, and anyone interested in creating a structured hunt program.

Delivery Method

In-classroom or virtual instructor-led training

Duration

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

Analytic Tradecraft Workshop

This entry-level online workshop covers essential cyber threat intelligence concepts and best practices. Students will apply structured analytic techniques to understand the nature of modern cyber threats.

The workshop culminates in a guided capstone exercise where students utilize Threat Modeling for risk mitigation.

Learning Objectives

After completing this course, learners should be able to:

- State what cyber intelligence is and why it matters
- Describe how attackers plan, prepare, and execute campaigns against victims
- Identify key analytic tools that add value to your security environment
- Tailor communication to the needs of key stakeholders to drive decision advantage

Who Should Attend

Cyber intelligence analysts, cyber threat analysts security analysts, penetration testers, and anyone looking for a short introduction to cyber intelligence analysis.

Delivery Method

In-classroom or virtual instructor-led training

Duration

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

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-classroom or virtual instructor-led training

Duration

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

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 for operationalizing 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-classroom or virtual instructor-led 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.

Cyber 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 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-classroom, virtual instructor-led training or on-demand

Duration

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

Cyber 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-classroom, virtual instructor-led training or on-demand

Duration

2 day (in-person delivery)
4 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-classroom, virtual instructor-led training or on-demand

Duration

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

Incident Response Courses

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-classroom or virtual instructor-led training

REGISTER FOR WEB-BASED 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-classroom 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 three-day 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-classroom or virtual instructor-led training

Duration

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

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-classroom 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

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-classroom, virtual instructor-led training, and web-based training

REGISTER FOR WEB-BASED 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 USB thumb drive containing all required class materials and tools, and must be able to either boot from USB or have VMware Player.

Malware Analysis Courses

Essentials of Malware Analysis

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 learners to disassembly, preparing them for topics covered in more advanced courses. This 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 a malware autopsy 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
- Review the basics and build a foundation of the x86 assembly language
- Recognize code constructs in the disassembly
- Use IDA Pro, the main tool for disassembly analysis

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-classroom 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-classroom 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. Students will be taught common exploitation techniques used by malware authors and how to spot them within malicious documents. 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 templates
- Disassemble and program ActionScript3 language (used in Flash)
- 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-classroom 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 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-classroom 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

macOS Malware Analysis for Reverse Engineers

Most malware analysts and incident responders either lack the equipment or knowledge to dissect macOS malware. With increasing corporate use of macOS devices, organizations must be prepared to analyze malware and threats that target macOS.

This course uses a practical, hands-on approach to introduce the tools and methodologies learners need to analyze malware that targets the macOS platform.

Course topics include macOS specific static and dynamic analysis tools and techniques to quickly uncover host and network-based indicators, analysis of compiled Objective-C code and Cocoa applications using IDA Pro and the use of the lldb debugger in dynamic analysis. Demonstrations and hands-on labs with real malware will enable learners to immediately apply this knowledge.

Learning Objectives

- Learn macOS internals relevant to malware analysis.
- See how to create a safe malware analysis environment in macOS.
- Explore the tools and methodologies used to perform basic analysis, and extract host and network-based indicators from malware without running it.
- Discover tools and methodologies used to analyze malware behavior by executing it in a safe environment.
- Acquire disassembly techniques specific to Objective-C executables.
- Practice malware debugging in the macOS environment and how it can be used to monitor and change its behavior at run time.

Who Should Attend

Malware analysts, incident responders, Intel analysts, information security staff, forensic investigators, or others requiring an understanding of how macOS specific malware works and how to analyze it.

Prerequisites

Training or experience in Windows malware analysis, familiarity with object-oriented programming, the x86 architecture, IDA Pro and Unix-like operating systems is required.

Delivery Method

In-classroom instructor-led training

Duration

2 days

What to Bring

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

- MacBook with VMware Fusion 7+
- 30 GB of free HDD space
- Licensed copy of fully updated IDA Pro that supports x86_64 architecture (for any OS, as long as it's accessible on the MacBook)

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-classroom 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.

Router Backdoor Analysis

With access to a router, an attacker can control the network and manipulate and copy traffic as needed. Router implants such as SYNful Knock, a serious and imminent threat, can be difficult to detect and analyze due to their location within the network. A direct analysis of the router image may be critical to mitigate a router-based attack, especially for edge routers positioned outside of network monitoring devices.

This course explains the purpose of the Cisco IOS image format, as well as how to modify the image. It describes how to effectively dissect an IOS image using IDA Pro for static analysis and how to debug a running router for active analysis. Course topics include how to configure and load a router for analysis, and take and analyze core memory dumps.

Learners will perform hands-on analyses of Cisco IOS images using a live router running in a lab environment. Hands-on labs include an opportunity to analyze and determine the function of backdoored router firmware.

Learning Objectives

After completing this course, learners should be able to:

- Conduct hands-on Cisco IOS malware analysis
- Understand the MIPS architecture
- Understand Cisco IOS image formatting and how routers load the images
- Analyze an IOS image using IDA Pro
- Identify modifications to a Cisco IOS image and focus analysis efforts
- Obtain and analyze memory dumps of a running router
- Perform dynamic analysis on a live system

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

Intermediate to advanced malware analysis skills, computer programming experience and comfort with IDA Pro.

Delivery Method

In-classroom instructor-led training

Duration

2 days

What to Bring

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

- VMware Workstation, Server or Fusion
- At least 20 GB of free HDD space

Advanced Acquisition and Testing Techniques

Creative Red Teaming

FireEye 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-classroom 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-classroom instructor-led training

Duration

4 days

Security and the Software Development Lifecycle

Software developers and security professionals have historically had an adversarial relationship. Software developers may believe security professionals get in the way of productivity while security professionals know that vulnerabilities get introduced in the software development lifecycle.

Fortunately, the barriers between these two disciplines are breaking down as companies recognize the importance of introducing security early in the software development lifecycle. This course covers different software development methodologies as well as the different places that good security practices can be introduced in any software development methodology as well as how to implement them.

Learning Objectives

After completing this course, learners should be able to:

- Demonstrate how security can be introduced into common software development methodologies
- Identify capabilities necessary to improve existing practices within their organizations
- Examine elements of a simplified methodology to apply those elements to methodologies and processes already in place in their organizations.
- Suggest security controls that can be applied within development processes in their own environment

Who Should Attend

Anyone who is now or may in the future be part of a software development project. This may be, for example, developers who want to know more about security, security people who want to understand software development processes or project managers who want to understand both better.

Delivery Method

In-classroom or virtual instructor-led training

Duration

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

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. Mandiant's 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-classroom or virtual instructor-led training

Duration

2–4 hours (in-person delivery)
2–4 hours (virtual delivery)

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-classroom or virtual instructor-led training

Prerequisites

Varies based on audience

Duration

2 days

Registration Instructions

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

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.

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

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-classroom instructor-led training

Duration

3 days

Senior Executive Mentorship Program

The FireEye 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-classroom instructor-led training

Duration

1 day

To learn more, visit **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye
At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at **www.FireEye.com**.

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.