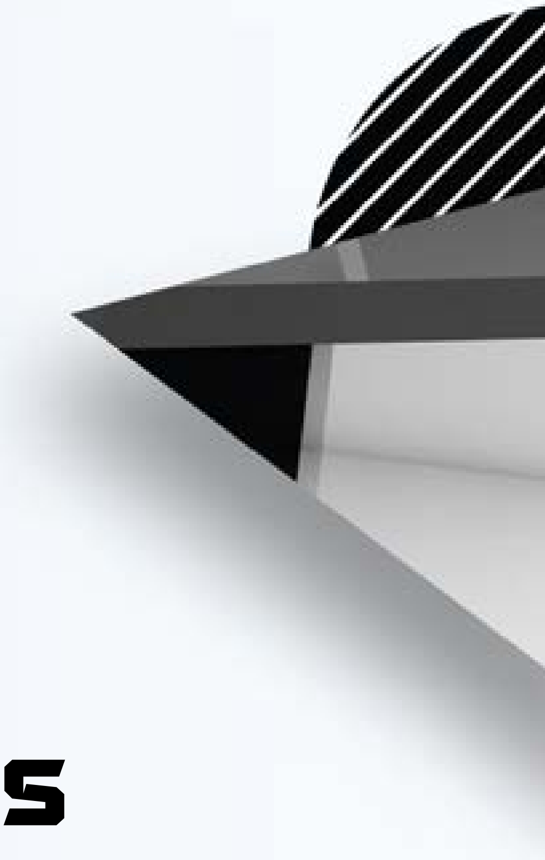
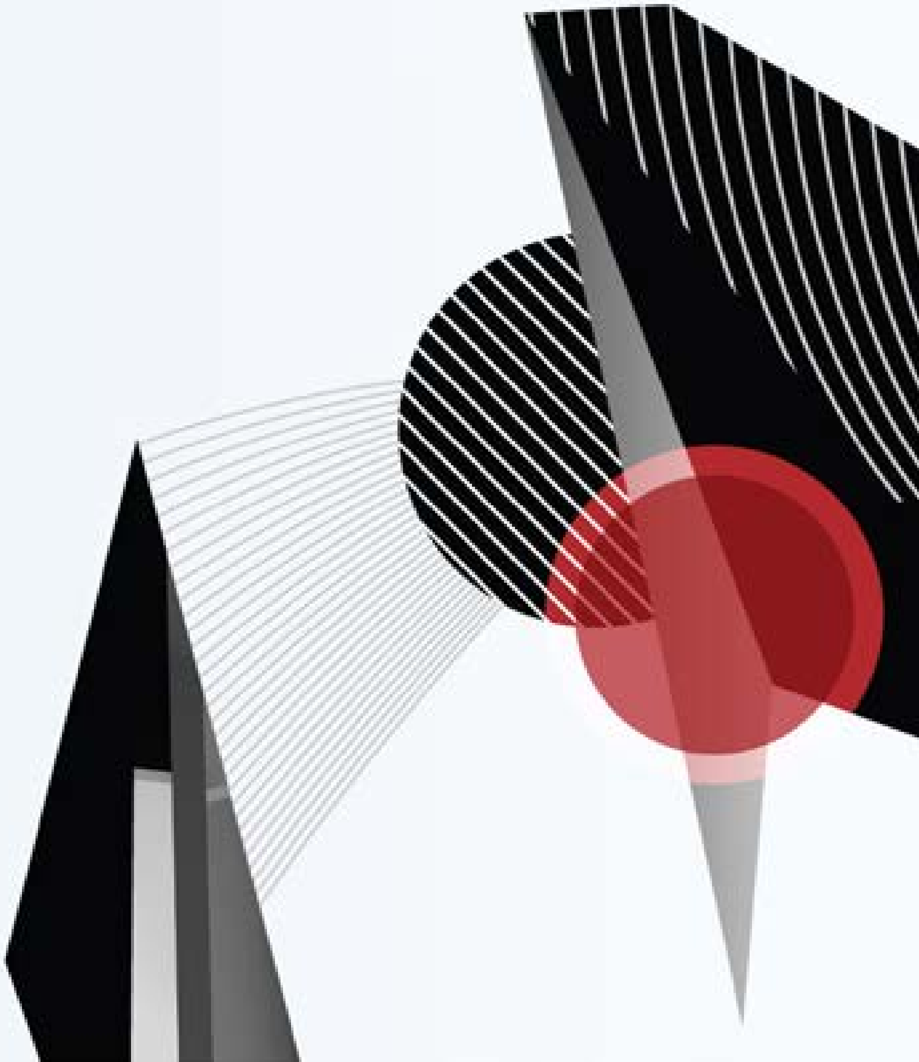
CATALOG

FireEye TRAINING COURSES

Catalog of Instructor-Led and Web-Based Training





Contents

Product Training from FireEye

Instructor-Led Training Courses

Web-Based Training Courses

Contents

Cyber Security Training from FireEye Mandiant

Instructor-Led Intelligence and Attribution Courses

Instructor-Led Incident Response Courses

Instructor-Led Malware Analysis Courses

Instructor-Led Advanced Acquisition Techniques

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, a FireEye company, which 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.

Product Training from FireEye

Instructor-Led Training Courses

FireEye Helix

This five-day entry-level 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
- Locate and use critical information in a Helix alert to assess a potential threat
- Comfortably switch between the Helix web console to other FireEye interfaces
- 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
- Actively hunt for unknown attackers

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, Endpoint Security for Helix. 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
5 days

Network Security (NX Series) Deployment

This entry-level course covers deployment options, basic administration and core functionality for FireEye Network Security (NX Series). Hands-on activities include appliance administration, how to read alerts generated by the FireEye Network Security appliance and how to identify systems infected with malware.

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 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
1 day

Email Security (EX Series) Deployment

This entry-level course covers deployment options, basic administration and core functionality for FireEye Email Security (EX Series). Hands-on activities include appliance administration, how to read alerts generated by FireEye Email Security and how to identify recipients of malicious emails.

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

1 day

Central Management (CM Series) Deployment

This entry-level course covers deployment options, basic administration and core functionality for FireEye Central Management (CM Series). Hands-on activities include administering other FireEye appliances (Network Security, Email Security, File Content Security, Malware Analysis) using FireEye Central Management, correlating web and email attacks and submitting malware detected by supported FireEye appliances 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 FireEye Central Management (CM)
- Administer other FireEye appliances using Central Management (CM)
- 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

4 hours

File Content Security (FX Series) Deployment

This entry-level course covers deployment options, basic administration and core functionality for FireEye File Content Security (FX Series). Hands-on activities include appliance administration, reviewing analysis results for file shares and identifying incidents.

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 appliances.

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

Malware Analysis (AX Series) Deployment

This entry-level course covers deployment options, basic administration and core functionality for FireEye Malware Analysis (AX). Hands-on activities include appliance administration and how to submit malware samples to FireEye Malware Analysis for deep forensic analysis.

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 appliances.

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

Endpoint Security (HX Series) Deployment

This entry-level course covers deployment options, basic administration and core functionality for FireEye Endpoint Security (HX Series). Hands-on activities include appliance administration, how to read alerts generated by FireEye Endpoint Security and how to contain infected endpoints.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components needed for FireEye Endpoint Security deployment
- Identify the key phases of Endpoint Security operation
- Perform the initial configuration of Endpoint Security appliances and hosts
- Create custom threat indicators
- Identify critical information in an Endpoint Security alert
- Validate an Endpoint Security alert
- Request and approve hosts for containment

Who Should Attend

Network security professionals and incident responders who must set up and work with FireEye Endpoint Security appliances.

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

Endpoint Security (HX Series) Comprehensive Investigation

This course covers investigation techniques using FireEye Endpoint Security (HX Series). It also prescribes a methodology for investigating security alerts using both the Endpoint Security triage summary and Redline, a free endpoint security tool from FireEye. Hands-on activities include validating alerts, examining event details using Endpoint Security and Redline, using the Endpoint Security API to automate actions and integrating Endpoint Security with other systems.

Learning Objectives

After completing this course, learners should be able to:

- Investigate a Redline triage package using a defined methodology
- Validate and provide further context for alerts using Redline
- Identify malicious activity hidden among common Windows events recorded in the look-back cache
- Use the API to automate FireEye Endpoint Security functionality

Who Should Attend

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

Prerequisites

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

Duration

1 day

Network Forensics (PX Series) Utilization

This entry-level course covers deployment options, basic administration and core functionality for FireEye Network Forensics (PX Series). Hands-on activities include appliance administration, searching and filtering captured data and reconstruction of sessions from captured packet data.

Learning Objectives

After completing this course, learners should be able to:

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

Who Should Attend

Network security professionals and incident responders who must work with FireEye Network Forensics 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

1 day

Network Forensics (PX Series) and Investigation Analysis (IA Series) Utilization

This course begins with an overview of Network Forensics (PX Series) and Investigation Analysis (IA Series), including common deployment scenarios in a typical network. The Network Forensics Utilization module covers end user tasks, including searching and filtering captured data and the reconstruction of sessions from captured packet data. The Investigation Analysis Utilization module addresses query construction for searching indexed layer 7 data, visualizing parallel queries, filtering of resulting data and extracting pcap files from connected Network Forensics systems.

The course materials include an administration reference section that covers Network Forensics and Investigation Analysis system readiness, integration between the two products and other daily administration tasks.

Learning Objectives

After completing this course, learners should be able to:

- Describe FireEye Network Forensics and Investigation Analysis appliances
- Illustrate how to deploy Network Forensics and Investigation Analysis appliances
- Search and filter connection and session data
- Reconstruct session data for a malicious breach
- Construct layer 7 search queries and filter results
- Extract pcap data from the Network Forensics appliance using the Investigation Analysis appliance as a user interface

Who Should Attend

Network security professionals, incident responders and analysts who must use FireEye Network Forensics and investigation Analysis 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

Threat Analytics Deployment

FireEye Threat Analytics applies threat intelligence, expert rules and advanced security data analytics to noisy event data streams. By revealing suspicious behavior patterns and generating alerts that matter, security teams can prioritize and optimize their response efforts.

This course covers features, benefits, deployment options, basic administration and core functionality for Threat Analytics. Learners will discover the unique strengths of Threat Analytics and understand how it enables real-time situational awareness of both known and unknown network security threats.

Hands-on activities include triaging Threat Analytics alerts, investigating security incidents and hunting for unknown attackers.

Learning Objectives

After completing this course, learners should be able to:

- Correlate live network activity to known threats
- Describe the Threat Analytics architecture
- Determine which data sources are most useful
- Triage Threat Analytics alerts and investigate security incidents
- Differentiate between sources of threat actor intelligence
- Describe the features and benefits of Threat Analytics
- Actively hunt for unknown attackers

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

Alert Analysis

This course covers FireEye-generated alerts. It provides a framework for interpreting callbacks and the results of malware binary analysis. Hands-on activities include analyzing alert data to determine the significance of alerts.

Learning Objectives

After completing this course, learners should be able to:

- Distinguish FireEye alert types
- Locate and use critical information in a FireEye alert to assess a potential threat
- Use indicators of compromise (IOCs) in a FireEye alert to identify the threat on compromised hosts

Who Should Attend

Network security professionals, incident responders and FireEye administrators and analysts who must work with alerts generated by FireEye products.

Prerequisites

Completion of at least one instructor-led or web-based FireEye deployment training course or experience administering FireEye appliances. A working understanding of networking and network security, the Windows operating system, file system, registry and use of the CLI.

Duration

2 days

Forensics Fundamentals

This course covers the fundamentals of computer forensics investigation, including legal and ethical considerations. Hands-on activities span the entire forensics process: FireEye-generated alerts, discovery and analysis of the host for evidence of malware and other unwanted intrusion and findings reports. Learners will analyze computer systems using freely available tools.

Learning Objectives

After completing this course, learners should be able to:

- Describe the basic ethics and laws of computer and malware forensics
- Describe methods of criminal, civil and administrative investigations
- Demonstrate the ability to plan, execute and report on a digital forensic examination

Who Should Attend

Network security professionals and incident responders who must use alerts generated by FireEye products to conduct cyber forensics.

Prerequisites

Completion of the Alert Analysis course. Windows systems administration skills. Familiarity with basic command line interface (CLI) commands.

Duration

3 days

Core Appliance Troubleshooting

This course introduces a framework for troubleshooting FireEye Network Security (NX Series), Email Security (EX Series), File Content Security (FX Series), Malware Analysis (AX Series) and Central Management (CM Series) appliances. The course includes checklists, case studies and guidance for transitioning difficult cases to the FireEye support team. Hands-on activities will give learners experience resolving common issues.

Learning Objectives

After completing this course, learners should be able to:

- Find and remediate common issues without escalating to FireEye Customer Support
- Follow the escalation process for sending more difficult cases to FireEye Customer Support
- Follow up on support cases using the FireEye Customer Portal

Who Should Attend

IT administrators and customer IT support representatives who must resolve issues with FireEye appliances during day-to-day work.

Prerequisites

Completion of the relevant appliance deployment courses. Experience with network administration and support.

Duration

1 day

Endpoint Security (HX Series) Appliance Troubleshooting

This course introduces a framework for troubleshooting the FireEye Endpoint Security (HX Series) appliance. The course includes checklists, case studies and guidance for transitioning difficult cases to the FireEye support team. Hands-on activities will give learners experience resolving common issues.

Learning Objectives

After completing this course, learners should be able to:

- Resolve issues commonly encountered with XAgent whitelisting
- Validate endpoints to ensure that they are performing as expected
- Use Endpoint Security logs and diagnostics for troubleshooting

Who Should Attend

FireEye Endpoint Security appliance administrators who must regularly resolve FireEye Endpoint Security issues.

Prerequisites

Completion of the Endpoint Security Deployment course. Experience administering Windows-based systems.

Duration

1 day

Product Training from FireEye

Web-Based Training Courses

Network Security (NX Series) Deployment (WBT)

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

Email Security (EX Series) Deployment (WBT)

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

File Content Security (FX Series) Deployment (WBT)

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

Central Management (CM Series) Deployment (WBT)

This entry-level self-paced online course covers deployment options, basic administration and core functionality for FireEye Central Management (CM Series) 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

Malware Analysis (AX Series) Deployment (WBT)

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

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

Learning Objectives

After completing this course, learners should be able to:

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

Who Should Attend

Network security professionals and incident responders who must work with FireEye Network Forensics 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

Endpoint Security (HX Series) Deployment (WBT)

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

Learning Objectives

After completing this course, learner should be able to:

- Identify the components needed for FireEye Endpoint Security appliance deployment
- Identify the key phases of Endpoint Security appliance operation
- Perform the initial configuration of Endpoint Security appliances and hosts
- Create custom threat indicators
- Identify critical information in an Endpoint Security alert
- Validate an Endpoint Security alert
- Request and approve hosts for containment

Who Should Attend

Network security professionals and incident responders who must set up and work with FireEye Endpoint Security appliances.

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

Email Security – Cloud Edition (WBT)

This self-paced online course covers the basic features, benefits, deployment and administration options of FireEye Email Security – Cloud Edition. It also discusses alert administration and configuration settings within the FireEye Email Security – Cloud Edition portal.

Learning Objectives

After completing this course, learners should be able to:

- Recognize the features and benefits of Email Security – Cloud Edition
- Research deployment options
- Review basic details of an Email Security – Cloud Edition alert
- Review other Email Security – Cloud Edition functions: email quarantine, reporting and tracing
- Configure Email Security – Cloud Edition settings and perform basic administration tasks

Who Should Attend

Any FireEye customer

Prerequisites

None

Duration

45-60 minutes

Introduction to FireEye Security Orchestrator (WBT)

This self-paced online course introduces FireEye Security Orchestrator and covers plug-ins used to interface with external applications, courses of action (COA) used for security process implementation and the management of cases generated from a COA.

Learning Objectives

After completing the course, learners should be able to:

- Provide an overview of FireEye Security Orchestrator
- Describe the components that enable Security Orchestrator to interface with external applications
- Provide an analysis of a COA by describing the function of each component of the COA
- Manage cases that are generated after executing a COA

Who Should Attend

Tier 1 and Tier 2 security managers, incident responders and analysts who expect to work with FireEye Security Orchestrator appliances.

Prerequisites

Completion of at least one FireEye product deployment course or experience administrating a FireEye appliance. Familiarity with networking technologies and network security is beneficial.

Duration

2-3 hours

Introduction to Malware Binary Analysis (WBT)

This self-paced online course covers the analysis of malicious files. Topics include file pre-analysis, file identification via antivirus scanning tools, dynamic and static malware analysis techniques, and packing and obfuscation techniques that are intended to make analysis more difficult. Examples discussed include Windows PE files and PDF documents.

Learning Objectives

After completing this course, learners should be able to:

- Summarize the requirements for a malware analysis lab
- Identify methods of analyzing malicious files
- Understand how to pre-analyze files
- Describe the use of scanning tools to identify known malware samples
- Recognize dynamic and static analysis techniques that malware analysts use to document malware capabilities
- Describe packing and obfuscation techniques used to disguise malware
- Examine Windows PE files and PDF documents for evidence of malware

Who Should Attend

Any FireEye customer

Prerequisites

Familiarity with x86 assembly language (32-bit) and a higher-level compiled programming language such as C or C++ and its calling conventions. Experience with basic use of a debugger on object code, and basic Windows operation and system administration. Some experience with a disassembler and writing Windows programs may be helpful.

Duration

60–90 minutes

Technical Requirements

This course includes animation with audio narration and requires Adobe Flash Player and speakers or headphones.

Introduction to Malware Forensics (WBT)

This online course explains how to determine whether a Windows system is infected with malware. It covers the tools that computer forensics practitioners use to examine a system, build a timeline of events and preserve the state of the system or data they are examining. Common malware attachment points in the Windows operating system are also described.

Learning Objectives

After completing this course, learners should be able to:

- Describe processes and tools used for the preservation of evidence
- Create and preserve disk images
- Understand common methods of malware infection
- Describe basic file system analysis
- Understand general investigative techniques
- Describe malware artifacts on the Windows OS

Who Should Attend

Any FireEye customer

Prerequisites

Background in computer science recommended but not required.

Duration

8-9 hours

Technical Requirements

This course includes animation with audio narration and requires Adobe Flash Player and speakers or headphones.

Cyber Security Training from FireEye Mandiant

Instructor-Led 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.

Duration

1 day

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.

Duration

1 day

Cyber Intelligence Foundations

This three-day course introduces the discipline of cyber intelligence with a focus on the cyber intelligence lifecycle. It covers current technology trends, common vulnerabilities and a review of noteworthy cyber breaches and adversary activity. It also summarizes relevant U.S. and international standards and policies.

Learning Objectives

After completing this course, learners should be able to:

- Clearly define cyber security intelligence and articulate the importance and staffing of cyber threat intelligence (CTI) capability
- Identify and develop source data for CTI
- Explain the concepts and interactions between cyber key terrain, cyber security intelligence, quality assessments, indicators of compromise and threat modeling
- Document threats effectively to develop raw data into minimally viable intelligence and write better intelligence reports
- Detail ways to counter analytical biases and explain the FireEye Threat Model to better identify malware
- Understand how intelligence analysts convert raw threat data into actionable intelligence

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.

Duration

3 days

What to Bring

Learners will need to bring a computer with Windows 7 or newer operating system installed, Core i5 or equivalent processor, 6 GB (preferably 8 GB) of RAM and 25 GB or more of free HDD space.

Virtual machines are acceptable provided at least 4 GB of RAM can be allocated. Learners must provide their own copies of and licenses for Windows.

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

Instructor-Led 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.

Duration

3 days

What to Bring

Learners will need to bring a computer with Windows 7 or newer operating system installed, Core i5 or equivalent processor, 6 GB (preferably 8 GB) of RAM and 25 GB or more of free HDD space.

Virtual machines are acceptable provided at least 4 GB of RAM can be allocated. Learners must provide their own copies of and licenses for Windows.

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

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.

Duration

1 day

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.

Duration

3 days

Instructor-Led 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).

Duration

2 days

What to Bring

Laptop computer with VMware Workstation 10+ or VMware Fusion 7+, and at least 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.

Duration

3 days

What to Bring

Laptop computer with VMware Workstation 10+ or VMware Fusion 7+ and 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.

Course 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.

Course Duration

2 days

What to Bring:

Students must bring their own MacBook with VMware Fusion 7+ installed. Laptops should have at least 30GB of free space. A currently licensed copy of a fully-updated IDA Pro that supports the x86_64 architecture is required. It can be for any OS, as long as it is 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.

Duration

5 days

Course Requirements

Laptop computer with VMware Workstation 10+ or VMware Fusion 7+, and at least 30 GB of free HDD space. A licensed copy of IDA Pro is highly recommended to participate in all labs, but the free version can be used in most cases.

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.

Duration

2 days

What to Bring

Laptop with VMware Workstation, Server or Fusion (VMware Player is acceptable, but not recommended), and at least 20 GB of free HDD space. A licensed copy of IDA Pro that supports the MIPS architecture is required; the free version of IDA Pro will not suffice. If purchasing, the IDA Professional Edition is needed.

Instructor-Led Advanced Acquisition Techniques

Wireless Security

Wireless computing devices are everywhere and new products seem to appear daily, which poses significant security risks to an organization. As a result, network and information security staff must understand the risks inherent in wireless computing. This course is intended for professionals who support, design or assess IEEE 802.11 wireless environments, commonly known as Wi-Fi.

Hands-on activities are presented from the attacker's perspective to help learners understand a wireless attacker's methodology. The course will present a variety of case studies, accompanied by numerous lab exercises to reinforce wireless security concepts and materials.

Learning Objectives

After completing the course, learners should be able to:

- Find and access wireless access points using free tools
- Identify "cloaked" or non-broadcasting access points
- Defeat common security features
- Explore brute force attacks against WPA/WPA2-PMK
- Forcefully disassociate a client from an access point
- Adopt best practices on how to defeat WEP encryption
- Understand how attackers use wireless access points as an initial entry point during a network security breach
- Recognize common attack vectors used after accessing a wireless network
- Discuss common misconceptions about wireless technologies and why it can be nearly impossible to locate an attacker

Who Should Attend

Information technology, information security and corporate investigative team members, as well as other staff members who need to perform security audits on their wireless infrastructures.

Prerequisites

A basic understanding of TCP/IP networks and proficiency with Linux systems. Familiarity with computer security terminology and concepts is also recommended.

Duration

2 days

What to Bring

On-site requirements vary based on client environment. Contact course coordinator for specific equipment requirements.

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.

Duration

4 days

What to Bring

A laptop with a USB port (for installing software provided on a USB stick), an Ethernet port (or adapter), and local administrator rights to the host OS and VMs.

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

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

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.