Introduction to Malware Forensics (WBT)

Self-paced online training

HIGHLIGHTS

Duration
8 – 9 hours

Prerequisites
Background in computer science recommended but not required.

How to Register
Please contact your FireEye account representative for pricing options

Alternate Formats
An instructor-led version of this course is also available. Visit https://www.fireeye.com/services/training/courses/ for more details.

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.

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

Course Outline

1. Initial Incident Response Processes and Preservation of Evidence
2. Preserving Memory
3. Creating and Preserving Disk Images
4. Common Methods of Malware
5. Investigative Techniques
6. Reporting

For more details, or to view our full course catalog, please visit https://www.fireeye.com/services/training/

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.