DATA SHEET

Malware Analysis Fundamentals

Instructor-Led Training

Highlights

Duration

4 days

Prerequisites

Students taking this course should have a working knowledge of Windows/Linux/macOS operating systems, and network technologies. Basic understanding of information security, command line syntax, malware, and analytical thinking recommended.

How to Register

This course is available for purchase at https://training-catalog.trellix.com.

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://training- catalog.trellix.com.

This entry-level course in malware analysis provides foundational knowledge in malware history, safe malware sample handling, analysis methodologies and techniques, sandboxing, triage, and countermeasures. This course employs open-source tools in hands-on labs to analyze samples including packed executables, cross-platform, Office, PDF and more.

This course is part of the Trellix Cyber Operations team's Foundations in Incident Response Education (FIRE) track of general defensive security training. Learners are provided a blend of lecture, discussions, and hands-on labs.

Learning Objectives

After completing this course, learners should be able to:

- Define key malware types and terms in analysis
- Describe the "4 Stages" methodology for analysis
- Apply safe handling guidelines
- Explain triage techniques and tools
- Identify key indicators of "maliciousness" in malware samples
- List at least two defensive techniques used by malware
- Describe the history of malware
- Map malware techniques to MITRE ATT&CK

Who Should Attend

This course is intended for incident responders, information security staff, auditors, SOC analysts, investigators, and consultants responsible for digital forensics and incident response or malware analysis.

Course Outline

1. Course Introduction
2. Malware Overview
3. Malware Lab Construction
4. Analysis Techniques
5. Network Analysis
6. Delivery Vectors
7. Executables
8. Defensive Techniques of Malware
9. Modern OS Defenses