Training Course on Threat Hunting with Malware Analysis Techniques

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's ever-evolving cyber threat landscape, organizations face sophisticated adversaries leveraging advanced malware to breach networks undetected. Training Course on Threat Hunting with Malware Analysis Techniques is designed to equip cybersecurity professionals with hands-on skills in proactive threat detection and malware reverse engineering. Utilizing cutting-edge tools, behavioral analysis, and threat intelligence, this course empowers participants to anticipate and neutralize cyber threats before they cause harm.

Combining threat hunting methodologies with malware analysis techniques, this course provides an immersive experience into identifying Indicators of Compromise (IOCs), detecting persistent threats, dissecting malicious code, and strengthening organizational cyber defense. With real-world case studies, practical labs, and actionable frameworks, this course enhances your ability to predict, prevent, and respond to emerging cyber threats effectively.

Programme Curriculum

Training Course on Threat Hunting with Malware Analysis Techniques

Introduction

In today's ever-evolving cyber threat landscape, organizations face sophisticated adversaries leveraging advanced malware to breach networks undetected. Training Course on Threat Hunting with Malware Analysis Techniques is designed to equip cybersecurity professionals with hands-on skills in proactive threat detection and malware reverse engineering. Utilizing cutting-edge tools, behavioral analysis, and threat intelligence, this course empowers participants to anticipate and neutralize cyber threats before they cause harm.

Combining threat hunting methodologies with malware analysis techniques, this course provides an immersive experience into identifying Indicators of Compromise (IOCs), detecting persistent threats, dissecting malicious code, and strengthening organizational cyber defense. With real-world case studies, practical labs, and actionable frameworks, this

course enhances your ability to predict, prevent, and respond to emerging cyber threats effectively.

Course Objectives

1. Understand the fundamentals of proactive threat hunting in modern SOC environments.
2. Apply malware analysis techniques for identifying evasive malware strains.
3. Perform behavioral and static analysis using industry-standard tools.
4. Identify and extract Indicators of Compromise (IOCs) and TTPs.
5. Utilize MITRE ATT&CK for mapping adversary behavior.
6. Develop automated threat detection rules and YARA signatures.
7. Conduct memory forensics and live system investigations.
8. Apply sandboxing and reverse engineering techniques to unknown samples.
9. Integrate threat intelligence feeds for enhanced hunting capabilities.
10. Investigate APT campaigns and understand attacker lifecycle.
11. Deploy deception technologies to enhance hunting accuracy.
12. Build resilient detection and response strategies using AI and ML.
13. Create post-incident threat reports for organizational awareness.

Target Audiences

1. SOC Analysts
2. Incident Responders
3. Malware Analysts
4. Threat Intelligence Analysts
5. Cybersecurity Engineers
6. Penetration Testers
7. Digital Forensics Investigators
8. Cybersecurity Enthusiasts and Students

Course Duration: 5 days

Course Modules

Module 1: Introduction to Threat Hunting and Cyber Kill Chain

- Define threat hunting and its importance in cybersecurity.
- Explore the cyber kill chain model and attacker lifecycle.
- Understand threat hunting maturity models.
- Identify hunting methodologies and frameworks.
- Tools overview for threat hunting (ELK, Splunk, etc.).
- **Case Study:** Detecting lateral movement using endpoint telemetry.

Module 2: Fundamentals of Malware and Malware Types

- Overview of malware classification and behavior.
- Recognizing fileless and polymorphic malware.
- Key malware delivery techniques.
- Importance of understanding malware intent and impact.
- Use of anti-virus evasion methods.
- **Case Study:** Analyzing the impact of Emotet across a financial network.

Module 3: Static Malware Analysis Techniques

- Introduction to static analysis tools (PE Studio, Exeinfo PE).
- Understanding PE file format and header analysis.

- String extraction and hash calculation.
- Identifying embedded resources and suspicious APIs.
- Analyzing metadata and obfuscation signs.
- **Case Study:** Reverse engineering a Trojan downloader.

Module 4: Dynamic Malware Analysis Techniques

- Setting up a secure sandbox environment.
- Monitoring malware behavior with tools (ProcMon, Wireshark).
- Network traffic analysis for malware C2 detection.
- API call tracing and registry modifications.
- Memory dump analysis with Volatility.
- **Case Study:** Behavioral analysis of a ransomware variant.

Module 5: Threat Intelligence and IOC Extraction

- Integrating threat intelligence with threat hunting.
- Gathering data from open-source threat feeds (OSINT).
- Identifying IOCs: hashes, IPs, domains.
- Correlating IOCs with malware samples.
- Automating IOC detection using SIEM platforms.
- **Case Study:** Tracking a phishing campaign using IOC correlation.

Module 6: Reverse Engineering and Code Dissection

- Introduction to assembly and disassemblers (IDA Pro, Ghidra).
- Analyzing control flow and function calls.
- Identifying encryption routines and payloads.
- Deobfuscating packed executables.
- Creating custom YARA rules for detection.
- **Case Study:** Deconstructing a nation-state backdoor malware.

Module 7: Advanced Threat Hunting with MITRE ATT&CK

- Mapping adversary TTPs with MITRE ATT&CK.
- Creating detection rules based on ATT&CK techniques.
- Hunting for privilege escalation and persistence mechanisms.
- Using Sigma and YARA with ATT&CK.
- Visualizing threat detection coverage.
- **Case Study:** APT group mapping using MITRE ATT&CK navigator.

Module 8: Incident Response and Post-Hunt Reporting

- Documentation and analysis of threat hunting results.
- Constructing incident timelines.
- Integrating hunting outcomes into IR playbooks.
- Reporting for different stakeholders (executives, SOC, devs).
- Continuous improvement from hunt findings.
- **Case Study:** End-to-end incident response from zero-day exploit.

Training Methodology

- **Hands-On Labs and Virtual Machines** for safe malware handling
- **Instructor-led Lectures** with real-world threat scenarios
- **Interactive Demos** of tools and live hunts
- **Assignments and Challenges** to reinforce concepts

- **Downloadable Resources** including scripts, rules, and cheat sheets
- **Assessment and Certification** upon course completion

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com