Training Course on Advanced Threat Actor Profiling and Attribution

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's dynamic **cyber threat landscape**, organizations face increasingly sophisticated and **persistent threats** from diverse **threat actors**. Understanding the **motivations, capabilities, and tactics, techniques, and procedures (TTPs)** of these adversaries is no longer a luxury but a critical imperative for robust **cyber defense**. Training Course on Advanced Threat Actor Profiling and Attribution equips security professionals with the **cutting-edge skills** and **actionable intelligence** needed to proactively identify, track, and disrupt malicious activities, transforming reactive incident response into **proactive threat hunting** and **strategic risk mitigation**.

This specialized program delves deep into **cyber threat intelligence (CTI)** methodologies, focusing on the meticulous process of constructing comprehensive **threat actor profiles** and performing accurate **attribution analysis**. Participants will learn to leverage **OSINT (Open Source Intelligence)**, **HUMINT (Human Intelligence)**, and **technical intelligence** to uncover adversary infrastructure, identify **zero-day exploits**, and forecast future attack vectors. By mastering these advanced techniques, security teams can enhance their **situational awareness**, prioritize **vulnerability management**, and implement **threat-informed defense strategies** to safeguard critical assets and ensure business continuity against the most advanced **cyber espionage**, **ransomware**, and **nation-state attacks**.

Programme Curriculum

Training Course on Advanced Threat Actor Profiling and Attribution

Introduction

In today's dynamic **cyber threat landscape**, organizations face increasingly sophisticated and **persistent threats** from diverse **threat actors**. Understanding the **motivations, capabilities, and tactics, techniques, and procedures (TTPs)** of these adversaries is no longer a luxury but a critical

imperative for robust **cyber defense**. Training Course on Advanced Threat Actor Profiling and Attribution equips security professionals with the **cutting-edge skills** and **actionable intelligence** needed to proactively identify, track, and disrupt malicious activities, transforming reactive incident response into **proactive threat hunting** and **strategic risk mitigation**.

This specialized program delves deep into **cyber threat intelligence (CTI)** methodologies, focusing on the meticulous process of constructing comprehensive **threat actor profiles** and performing accurate **attribution analysis**. Participants will learn to leverage **OSINT (Open Source Intelligence)**, **HUMINT (Human Intelligence)**, and **technical intelligence** to uncover adversary infrastructure, identify **zero-day exploits**, and forecast future attack vectors. By mastering these advanced techniques, security teams can enhance their **situational awareness**, prioritize **vulnerability management**, and implement **threat-informed defense strategies** to safeguard critical assets and ensure business continuity against the most advanced **cyber espionage**, **ransomware**, and **nation-state attacks**.

Course Duration

10 days

Course Objectives

1. Master **Adversary Emulation** techniques to simulate real-world attacks.
2. Develop expert-level skills in **Cyber Threat Intelligence (CTI)** collection and analysis.
3. Conduct in-depth **Malware Analysis** and **Reverse Engineering** for attribution.
4. Utilize **Digital Forensics** techniques to uncover attacker footprints.
5. Perform advanced **Network Traffic Analysis** for identifying anomalous behavior.
6. Understand and apply the **MITRE ATT&CK Framework** for TTP mapping.
7. Implement **Behavioral Analytics** to detect sophisticated threat actor movements.
8. Construct detailed **Threat Actor Profiles** focusing on motivations and capabilities.
9. Execute **Attribution Analysis** with high confidence, linking attacks to specific entities.
10. Leverage **Open-Source Intelligence (OSINT)** for enhanced threat hunting.
11. Develop **Proactive Threat Hunting** strategies to anticipate emerging threats.
12. Integrate **Machine Learning** and **AI in Cybersecurity** for automated threat detection.
13. Formulate effective **Strategic Threat Intelligence** reports for executive decision-making.

Organizational Benefits

- Proactively identify and mitigate advanced threats before they cause significant damage.
- Rapidly attribute attacks, enabling faster containment and recovery.
- Prioritize security controls and allocate resources based on actual threat landscape.
- Gain a deeper understanding of organizational vulnerabilities and threat exposures.
- Minimize operational disruption and financial losses due to cyberattacks.
- Meet stringent cybersecurity regulations and demonstrate due diligence.
- Elevate the expertise of internal security teams.
- Provide actionable intelligence to leadership for informed cybersecurity planning.

Target Audience

1. Cyber Threat Intelligence Analysts
2. Incident Response Team Members
3. Security Operations Center (SOC) Analysts
4. Digital Forensics Investigators
5. Red Team and Penetration Testers

6. Security Architects and Engineers
7. CISOs and Security Leadership (for strategic insights)
8. Law Enforcement and Government Agency Personnel specializing in cybercrime.

Course Outline

Module 1: Foundations of Advanced Threat Intelligence

- Understanding the **Cyber Threat Landscape 2025**.
- Defining **Threat Intelligence Lifecycle** and its phases.
- Strategic, Operational, Tactical, and Technical CTI.
- The role of **Indicators of Compromise (IOCs)** and **TTPs**.
- **Case Study:** Analyzing the evolution of ransomware groups and their intelligence requirements.

Module 2: Introduction to Threat Actor Profiling

- What constitutes a **Threat Actor Profile**?
- Components: Motivations, Capabilities, Intent, Infrastructure.
- Types of Threat Actors: Nation-State, Cybercrime, Hacktivist, Insider Threats.
- Building a **Threat Actor Persona**.
- **Case Study:** Profiling a notorious APT group based on leaked reports.

Module 3: Open-Source Intelligence (OSINT) for Attribution

- Techniques for **OSINT Collection** (web scraping, social media analysis).
- Utilizing search engines and specialized OSINT tools (e.g., Maltego).
- Identifying and verifying public information related to threat actors.
- Ethical and legal considerations in OSINT.
- **Case Study:** Tracing the digital footprints of a hacktivist collective using public data.

Module 4: Technical Intelligence Collection

- Passive vs. Active Reconnaissance techniques.
- Network traffic analysis for threat intelligence (NetFlow, PCAP analysis).
- Endpoint telemetry and log analysis.
- Malware sample collection and initial triage.
- **Case Study:** Collecting technical indicators from a recent phishing campaign.

Module 5: Malware Analysis for Attribution

- Static and Dynamic Malware Analysis techniques.
- Identifying **Malware Families** and their characteristics.
- Extracting **Indicators of Compromise (IOCs)** from malware.
- Understanding common evasion techniques.
- **Case Study:** Dissecting a piece of custom malware and linking it to a known group.

Module 6: Reverse Engineering for Threat Actors

- Introduction to Reverse Engineering principles.
- Tools for **Binary Analysis** (IDA Pro, Ghidra).
- Identifying unique code patterns and shared infrastructure.
- Unpacking and deobfuscating malicious code.

- **Case Study:** Reverse engineering a dropper to uncover its command-and-control infrastructure.

Module 7: Digital Forensics in Attribution

- Forensic artifact collection and preservation.
- Memory forensics and disk forensics for evidence extraction.
- Timeline analysis of events during an intrusion.
- Identifying attacker tools and methodologies on compromised systems.
- **Case Study:** Reconstructing an intrusion event to pinpoint the entry vector and attacker activity.

Module 8: Network Forensics and Traffic Analysis

- Deep packet inspection and protocol analysis.
- Identifying encrypted traffic and tunneling techniques.
- Flow data analysis for anomalous network patterns.
- Correlation of network events with host-based artifacts.
- **Case Study:** Analyzing network captures from a suspected data exfiltration incident.

Module 9: MITRE ATT&CK Framework in Depth

- Mapping threat actor TTPs to the **MITRE ATT&CK Matrix**.
- Utilizing ATT&CK for defensive posture improvement.
- Creating **ATT&CK Navigator** layers for specific threat actors.
- Developing **Threat-Informed Defense** strategies.
- **Case Study:** Mapping a known APT campaign's TTPs to the ATT&CK framework and identifying defensive gaps.

Module 10: Behavioral Analytics and Anomaly Detection

- Establishing baselines for normal user and system behavior.
- Identifying deviations and suspicious activities.
- Leveraging **User and Entity Behavior Analytics (UEBA)**.
- Machine learning models for anomaly detection.
- **Case Study:** Detecting an insider threat based on unusual data access patterns.

Module 11: Attribution Methodologies and Challenges

- Models for attribution: Diamond Model of Intrusion Analysis.
- Levels of confidence in attribution.
- Challenges: False flags, proxy chains, deniable operations.
- Legal and geopolitical implications of attribution.
- **Case Study:** Discussing the complexities and controversies of attributing a high-profile cyberattack.

Module 12: Cyber Espionage and Nation-State Actors

- Understanding the motivations and objectives of **Nation-State APTs**.
- Common TTPs used in state-sponsored espionage.
- Counterintelligence strategies against sophisticated actors.
- Geopolitical context of cyber warfare.
- **Case Study:** Analyzing a major cyber espionage campaign and its impact on international relations.

Module 13: Cybercrime Syndicates and Ransomware

- The business model of **Ransomware-as-a-Service (RaaS)**.
- Tactics of major cybercrime groups.
- Financial motivations and cryptocurrency tracing for attribution.
- Disruption strategies against cybercriminal enterprises.
- **Case Study:** Tracking the affiliates of a prominent ransomware gang and their targeting patterns.

Module 14: Developing Actionable Threat Intelligence

- Structuring and disseminating **Threat Intelligence Reports**.
- Integrating CTI into existing security operations (SIEM, SOAR).
- Creating custom **Threat Feeds**.
- Metrics for measuring the effectiveness of CTI.
- **Case Study:** Developing a concise threat intelligence brief for senior management based on recent findings.

Module 15: Future Trends in Threat Profiling and Attribution

- The impact of **AI and Machine Learning** on threat intelligence.
- **Quantum Computing** and its implications for cybersecurity.
- Emerging attack vectors: IoT, OT, Cloud-Native threats.
- The role of **Human-Machine Teaming** in advanced threat analysis.
- **Case Study:** Predicting future adversary trends based on technological advancements and geopolitical shifts.

Training Methodology

This course employs a highly interactive and practical training methodology, combining theoretical concepts with extensive **hands-on labs** and **real-world case studies**. The approach includes:

- **Instructor-Led Sessions:** Expert-led lectures and discussions.
- **Interactive Workshops:** Collaborative problem-solving and group exercises.
- **Live Demonstrations:** Practical application of tools and techniques.
- **Simulation Exercises:** Realistic cyberattack scenarios for practical experience.
- **Case Study Analysis:** Deep dives into historical and contemporary threat actor campaigns.
- **Tools and Platform Training:** Hands-on experience with industry-standard CTI and forensic tools.
- **Q&A and Discussion Forums:** Facilitating knowledge sharing and clarification.

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	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now