Training Course on Open-Source Intelligence for Threat Hunting

Professional Development Training Course Outline

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

Course Introduction

Training Course on Open-Source Intelligence for Threat Hunting provides cybersecurity professionals with the essential skills and cutting-edge methodologies to leverage Open-Source Intelligence (OSINT) for proactive **threat hunting**. In today's dynamic threat landscape, where **adversaries** constantly evolve their **TTPs (Tactics, Techniques, and Procedures)**, the ability to **collect, analyze, and interpret publicly available information** is paramount. Participants will gain hands-on experience with leading OSINT tools and techniques, empowering them to **identify emerging threats**, **uncover hidden vulnerabilities**, and **enhance their organization's defensive posture**. This course goes beyond basic data collection, focusing on **actionable intelligence** that directly supports **incident response** and **proactive cyber defense strategies**.

The program is meticulously designed to bridge the gap between raw data and **strategic intelligence**, enabling participants to think like an **attacker** while acting as a **defender**. Through practical exercises, **real-world case studies**, and interactive labs, attendees will master the art of transforming disparate public information into **actionable insights** for **cyber threat intelligence (CTI)**. This foundational knowledge in OSINT is critical for **security analysts**, **incident responders**, and **threat hunters** aiming to strengthen their capabilities in **digital forensics**, **vulnerability management**, and **proactive security operations**.

Programme Curriculum

Training Course on Open-Source Intelligence for Threat Hunting

Introduction

Training Course on Open-Source Intelligence for Threat Hunting provides cybersecurity professionals with the essential skills and cutting-edge methodologies to leverage Open-Source Intelligence (OSINT) for proactive **threat hunting**. In today's dynamic threat landscape, where

adversaries constantly evolve their **TTPs (Tactics, Techniques, and Procedures)**, the ability to **collect, analyze, and interpret publicly available information** is paramount. Participants will gain hands-on experience with leading OSINT tools and techniques, empowering them to **identify emerging threats**, **uncover hidden vulnerabilities**, and **enhance their organization's defensive posture**. This course goes beyond basic data collection, focusing on **actionable intelligence** that directly supports **incident response** and **proactive cyber defense strategies**.

The program is meticulously designed to bridge the gap between raw data and **strategic intelligence**, enabling participants to think like an **attacker** while acting as a **defender**. Through practical exercises, **real-world case studies**, and interactive labs, attendees will master the art of transforming disparate public information into **actionable insights** for **cyber threat intelligence (CTI)**. This foundational knowledge in OSINT is critical for **security analysts**, **incident responders**, and **threat hunters** aiming to strengthen their capabilities in **digital forensics**, **vulnerability management**, and **proactive security operations**.

Course Duration

5 days

Course Objectives

1. Comprehend the core principles, **ethical considerations**, and legal boundaries of Open-Source Intelligence.
2. Utilize **Google Dorking**, advanced operators, and specialized search engines for deep web reconnaissance.
3. Extract and analyze data from social media platforms to identify **threat actors**, **misinformation campaigns**, and **insider threats**.
4. Navigate and gather intelligence from **dark web forums**, marketplaces, and hidden networks for **cybercrime monitoring** and **breached data analysis**.
5. Conduct comprehensive OSINT to map an organization's **digital footprint**, identify exposed assets, and manage **vulnerability surface**.
6. Develop detailed profiles of **adversary groups** (APTs, cybercriminals) using OSINT to understand their **motivations, infrastructure, and TTPs**.
7. Apply **geospatial tools** and publicly available imagery to pinpoint locations and analyze events.
8. Leverage and customize popular OSINT tools like **Maltego, Shodan, Recon-ng, and SpiderFoot** for efficient data collection and analysis.
9. Employ techniques for structuring, analyzing, and visualizing OSINT data to derive **actionable intelligence**.
10. Seamlessly incorporate OSINT findings into existing **threat hunting methodologies** and **security operations workflows**.
11. Utilize OSINT to discover **zero-day vulnerabilities**, track **exploit kits**, and monitor **vulnerability intelligence feeds**.
12. Implement strategies to minimize an organization's and individuals' public digital footprint and enhance **operational security (OpSec)**.
13. Transform raw OSINT into high-fidelity, contextualized **threat intelligence reports** for strategic and tactical decision-making.

Organizational Benefits

- Proactively identify and neutralize threats before they impact critical assets.
- : Uncover and mitigate exposed vulnerabilities and sensitive information.

- Accelerate incident investigation and remediation through enriched intelligence.
- Gain deeper insights into emerging threats and adversary capabilities to inform risk mitigation strategies.
- Prevent costly breaches and minimize recovery expenses by proactively addressing security gaps.
- Provide security leadership with actionable intelligence for better resource allocation and security posture improvements.
- Build a more robust and adaptive security defense against evolving cyber threats.
- Stay ahead of adversaries by understanding their methods and anticipating their next moves.

Target Audience

1. Security Analysts and SOC (Security Operations Center) Analysts
2. Incident Responders and Forensics Investigators
3. Threat Hunters and Cyber Threat Intelligence (CTI) Analysts
4. Penetration Testers and Red Teamers
5. Vulnerability Management Specialists
6. Security Consultants and Auditors
7. Law Enforcement and Intelligence Professionals (focused on cybercrime)
8. IT Security Managers and CISOs (for strategic oversight)

Course Outline

Module 1: Foundations of OSINT for Cybersecurity

- Definition and principles of Open-Source Intelligence (OSINT) in a cybersecurity context.
- Legal and ethical considerations, including privacy, data protection, and responsible disclosure.
- Understanding the OSINT cycle: Planning, Collection, Processing, Analysis, Dissemination.
- Introduction to the various layers of the internet: Surface, Deep, and Dark Web.
- **Case Study**: Analyzing a major data breach announcement and identifying initial public information that could have been used by threat actors for reconnaissance.

Module 2: Advanced Web & Search Engine OSINT

- Mastering advanced search operators and **Google Dorking** for specific file types, directories, and sensitive information.
- Utilizing specialized search engines and archives (e.g., WayBack Machine, Common Crawl, Shodan) for historical and IoT device data.
- Leveraging passive DNS, WHOIS, and domain registration information for infrastructure reconnaissance.
- Techniques for overcoming CAPTCHAs and anti-scraping mechanisms.
- **Case Study**: Using advanced search techniques to discover inadvertently exposed internal documents or network diagrams of a simulated target organization.

Module 3: Social Media & Human Intelligence (HUMINT) via OSINT

- Techniques for effective **Social Media Intelligence (SOCMINT)** across platforms like LinkedIn, Twitter, Facebook, and specialized forums.
- Analyzing social media profiles for personal identifiable information (PII), professional connections, and potential insider threat indicators.
- Creating and managing **sock puppet accounts** for safe and anonymous investigation.
- Leveraging open-source tools for social media data extraction and sentiment analysis.

- **Case Study**: Tracing the online presence and connections of an individual suspected of spear-phishing based on publicly available social media data.

Module 4: Dark Web & Deep Web Investigations

- Understanding the architecture and risks associated with the **Dark Web** (Tor, I2P) and **Deep Web** (databases, private networks).
- Safe and ethical access to dark web marketplaces and forums for **cybercrime monitoring**.
- Identifying and analyzing leaked credentials, stolen data, and exploit sales.
- Utilizing specialized dark web search engines and intelligence feeds.
- **Case Study**: Monitoring dark web discussions for mentions of a specific company's name or its executives, and identifying potential plans for targeted attacks.

Module 5: OSINT for Digital Footprinting & Attack Surface Mapping

- Systematic approach to mapping an organization's **digital footprint** (domains, subdomains, IP ranges, cloud assets).
- Identifying exposed services, open ports, and vulnerable software versions using tools like **Shodan** and Censys.
- Analyzing public code repositories (GitHub, GitLab) for leaked API keys, credentials, or sensitive configurations.
- Techniques for discovering and assessing third-party vendor risks through OSINT.
- **Case Study**: Performing an external **attack surface assessment** on a simulated company to identify publicly accessible misconfigurations or vulnerable web applications.

Module 6: OSINT for Threat Actor Profiling & Attribution

- Methods for collecting information on **Advanced Persistent Threats (APTs)**, cybercriminal groups, and their **TTPs**.
- Analyzing malware samples, exploit details, and campaign reports from public sources.
- Leveraging threat intelligence platforms and frameworks (e.g., MITRE ATT&CK) with OSINT data for attribution.
- Understanding geopolitical influences and motivations behind state-sponsored attacks.
- **Case Study**: Utilizing OSINT to gather information on a known ransomware group's recent activities, including their preferred initial access vectors and evasion techniques.

Module 7: OSINT Tools & Automation for Threat Hunters

- Hands-on training with powerful OSINT tools: **Maltego** (link analysis), **Recon-ng** (web reconnaissance framework), **SpiderFoot** (automated scanning).
- Scripting and automation techniques for repetitive OSINT tasks (e.g., Python, Bash).
- Integrating OSINT tools with existing security information and event management (SIEM) systems and threat intelligence platforms.
- Data visualization techniques for complex OSINT findings.
- **Case Study**: Building an automated OSINT workflow to continuously monitor for new infrastructure related to a specific threat group.

Module 8: OSINT in Action: Threat Hunting & Incident Response

- Developing **hypothesis-driven threat hunts** using OSINT leads.
- Correlating OSINT findings with internal security logs and telemetry for proactive detection.
- Utilizing OSINT during active **incident response** to enrich alerts and guide investigations.

- Best practices for documenting OSINT investigations and generating **actionable threat intelligence reports**.
- **Case Study**: Simulating a real-world **phishing attack** and using OSINT to investigate the attacker's infrastructure, social engineering tactics, and potential origin.

Training Methodology

This course adopts a highly interactive and **hands-on learning** approach. The methodology includes:

- **Instructor-Led Sessions**: Expert-led lectures with real-world examples and interactive discussions.
- **Practical Labs**: Extensive hands-on exercises using dedicated virtual environments and industry-standard OSINT tools.
- **Real-World Case Studies**: In-depth analysis of actual cyber incidents where OSINT played a crucial role, fostering critical thinking and problem-solving.
- **Group Activities & Collaboration**: Encouraging participants to work together on simulated investigations, sharing insights and techniques.
- **Live Demonstrations**: Showing the practical application of tools and methodologies.
- **Q&A Sessions**: Dedicated time for participants to ask questions and receive personalized guidance.
- **Continuous Assessment**: Practical challenges and a final capstone project to solidify learning and demonstrate proficiency.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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