Training Course on Cyber Threat Intelligence for Proactive Defense

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected digital landscape, **cyber threats** are evolving at an unprecedented pace, demanding a paradigm shift from reactive incident response to **proactive defense**. This shift is powered by **Cyber Threat Intelligence (CTI)**, a critical discipline that transforms raw **threat data** into **actionable insights**. CTI empowers organizations to understand **adversary tactics, techniques, and procedures (TTPs)**, anticipate emerging risks, and strengthen their **security posture** against sophisticated attacks like **ransomware**, **APT campaigns**, and **zero-day exploits**. By leveraging CTI, security teams can move beyond simply reacting to breaches and instead develop **resilient cybersecurity strategies** that mitigate risks before they materialize, ensuring **business continuity** and protecting sensitive assets.

Training Course on Cyber Threat Intelligence for Proactive Defense delves into the foundational principles and advanced practices of CTI, equipping participants with the knowledge and skills to build robust **threat intelligence programs**. From **data collection and analysis** to **threat hunting** and **strategic intelligence dissemination**, the course covers the entire CTI lifecycle. Participants will learn to identify **indicators of compromise (IoCs)**, utilize **threat intelligence platforms (TIPs)**, and integrate CTI into their existing **Security Operations Center (SOC)** and **incident response (IR)** workflows. Through practical **case studies** and **hands-on labs**, attendees will gain the expertise necessary to contribute significantly to their organization's **cyber resilience** and maintain a **proactive defense** against the ever-growing **threat landscape**.

Programme Curriculum

Training Course on Cyber Threat Intelligence for Proactive Defense

Introduction

In today's interconnected digital landscape, **cyber threats** are evolving at an unprecedented pace, demanding a paradigm shift from reactive incident response to **proactive defense**. This shift is powered by **Cyber Threat Intelligence (CTI)**, a critical discipline that transforms raw **threat data** into **actionable insights**. CTI empowers organizations to understand **adversary tactics, techniques, and procedures (TTPs)**, anticipate emerging risks, and strengthen their **security posture** against sophisticated attacks like **ransomware**, **APT campaigns**, and **zero-day exploits**. By leveraging CTI, security teams can move beyond simply reacting to breaches and instead develop **resilient cybersecurity strategies** that mitigate risks before they materialize, ensuring **business continuity** and protecting sensitive assets.

Training Course on Cyber Threat Intelligence for Proactive Defense delves into the foundational principles and advanced practices of CTI, equipping participants with the knowledge and skills to build robust **threat intelligence programs**. From **data collection and analysis** to **threat hunting** and **strategic intelligence dissemination**, the course covers the entire CTI lifecycle. Participants will learn to identify **indicators of compromise (IoCs)**, utilize **threat intelligence platforms (TIPs)**, and integrate CTI into their existing **Security Operations Center (SOC)** and **incident response (IR)** workflows. Through practical **case studies** and **hands-on labs**, attendees will gain the expertise necessary to contribute significantly to their organization's **cyber resilience** and maintain a **proactive defense** against the ever-growing **threat landscape**.

Course Duration

5 days

Course Objectives

1. Master the CTI Lifecycle for effective threat intelligence generation.
2. Analyze adversary TTPs using frameworks like MITRE ATT&CK and the Diamond Model.
3. Implement advanced threat data collection techniques from OSINT, dark web monitoring, and commercial feeds.
4. Conduct in-depth threat analysis to derive actionable intelligence and contextualize threats.
5. Develop effective strategies for proactive threat hunting and detection engineering.
6. Utilize Threat Intelligence Platforms (TIPs) for efficient intelligence management and sharing.
7. Integrate CTI seamlessly into SOC operations for enhanced real-time threat detection.
8. Improve incident response capabilities by leveraging CTI for faster triage and containment.
9. Apply CTI to enhance vulnerability management and prioritize patching efforts.
10. Understand the role of AI and Machine Learning in CTI for predictive analytics and automation.
11. Build robust cyber resilience through a CTI-driven risk management framework.
12. Communicate strategic threat intelligence to executive leadership for informed decision-making.
13. Prepare for and mitigate risks associated with supply chain attacks and critical infrastructure protection.

Organizational Benefits

- Proactively identify and neutralize threats before they impact the organization, reducing breach likelihood.
- Streamline incident analysis and response times, minimizing the impact and cost of security incidents.

- Strengthen overall cybersecurity defenses by understanding adversary motivations and methodologies.
- Prioritize security investments and efforts based on actual threat intelligence and organizational risk.
- Prevent costly data breaches, downtime, and reputational damage associated with cyberattacks.
- Build a more adaptive and robust defense mechanism capable of withstanding evolving cyber threats.
- Provide leadership with actionable insights for better risk management and cybersecurity policy formulation.
- Support regulatory requirements and audit processes with comprehensive threat intelligence.

Target Audience

1. Security Operations Center (SOC) Analysts
2. Incident Responders
3. Threat Hunters
4. Security Engineers
5. Security Architects
6. Cybersecurity Analysts
7. Information Security Managers
8. Risk Management Professionals

Course Outline

Module 1: Introduction to Cyber Threat Intelligence (CTI)

- Defining CTI: From raw data to actionable insights.
- The CTI Lifecycle: Planning, Collection, Processing, Analysis, Dissemination, Feedback.
- Types of CTI: Strategic, Operational, Tactical, and Technical Intelligence.
- The importance of CTI in a proactive defense strategy.
- **Case Study:** Analyzing a major ransomware attack (e.g., WannaCry) and how CTI could have aided in early detection and mitigation.

Module 2: Understanding the Threat Landscape and Adversaries

- Deep dive into various **threat actors**: Nation-states, organized crime, hacktivists, insiders.
- Exploring common **attack vectors** and **threat methodologies**.
- Introduction to **Cyber Kill Chain** and **MITRE ATT&CK Framework**.
- Analyzing **vulnerabilities** and **exploits** in the context of threat intelligence.
- **Case Study:** Mapping a recent APT campaign (e.g., SolarWinds) to the MITRE ATT&CK framework to understand adversary TTPs.

Module 3: Threat Data Collection and Sources

- Open Source Intelligence (**OSINT**) techniques for gathering public threat data.
- Utilizing commercial **threat intelligence feeds** and subscriptions.
- Deep and **Dark Web monitoring** for emerging threats and compromised data.
- Internal data sources: Logs, SIEM alerts, vulnerability scans, network traffic.
- **Case Study:** Leveraging OSINT to track a phishing campaign targeting a specific industry.

Module 4: Threat Intelligence Analysis and Enrichment

- Data normalization, enrichment, and correlation techniques.
- Identifying and categorizing **Indicators of Compromise (IoCs)**.
- Applying analytical models: **Diamond Model of Intrusion Analysis**.
- Contextualizing threat data for relevance and actionability.
- **Case Study:** Analyzing a collection of IoCs from a recent breach and enriching them with external threat intelligence to identify the threat actor.

Module 5: Threat Intelligence Platforms (TIPs) and Tools

- Overview of leading **Threat Intelligence Platforms (TIPs)** and their functionalities.
- Integrating TIPs with existing security tools (SIEM, SOAR, EDR).
- Automating intelligence ingestion, processing, and dissemination.
- Building custom dashboards and reporting for various stakeholders.
- **Case Study:** Demonstrating the use of a TIP to manage and share threat intelligence during a simulated incident.

Module 6: Proactive Threat Hunting and Detection Engineering

- Principles and methodologies of **threat hunting**.
- Developing effective **detection rules** based on CTI.
- Utilizing CTI for proactive searching of malicious activity within networks.
- Leveraging CTI to fine-tune security controls and reduce false positives.
- **Case Study:** Conducting a threat hunt for specific TTPs associated with a known threat group using historical logs and CTI.

Module 7: CTI in Security Operations and Incident Response

- Integrating CTI into **SOC workflows** for real-time monitoring and alerting.
- Applying CTI to accelerate **incident triage** and investigation.
- Using CTI for effective **containment, eradication, and recovery** strategies.
- Post-incident analysis and feeding lessons learned back into the CTI cycle.
- **Case Study:** Simulating an incident response scenario where CTI is crucial for rapid identification and mitigation of a targeted attack.

Module 8: Building a CTI Program and Future Trends

- Establishing a **CTI program**: Requirements, staffing, governance.
- Measuring the effectiveness and ROI of CTI initiatives.
- Legal and ethical considerations in threat intelligence sharing.
- Emerging trends: **AI in CTI**, **machine learning for predictive analysis**, **Extended Threat Intelligence (XTI)**.
- **Case Study:** Developing a roadmap for implementing a comprehensive CTI program within a mid-sized enterprise.

Training Methodology

This training course employs a **blended learning approach**, combining **interactive lectures** with extensive **hands-on labs** and **real-world case studies**. Participants will engage in:

- **Instructor-led discussions:** Covering theoretical concepts and best practices.
- **Practical exercises:** Applying CTI techniques using industry-standard tools and platforms.
- **Simulated environments:** Experiencing realistic threat scenarios for practical skill development.

- **Group activities:** Fostering collaboration and knowledge sharing among participants.
- **Q&A sessions:** Addressing specific challenges and clarifying complex topics.
- **Post-training resources:** Providing access to tools, templates, and further reading materials.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100

Start Date	End Date	Location	Price
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100

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

Register Online Now

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