Certified Threat Intelligence Analyst (CTIA) Training Course

Professional Development Training Course Outline

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

Course Introduction

The contemporary cyber threat landscape is evolving at an unprecedented pace, necessitating a shift from purely reactive security postures to proactive, intelligence-driven defense. Certified Threat Intelligence Analyst (CTIA) Training Course is meticulously designed to equip cybersecurity professionals with a comprehensive, structured methodology for collecting, analyzing, and disseminating timely, actionable intelligence. This program moves beyond simply identifying threats by focusing on understanding the adversary lifecycle, their motivations, and translating raw data from diverse sources including OSINT, HUMINT, and deep/dark web sources into strategic, operational, and tactical intelligence. Successful completion empowers analysts to enhance security operations center (SOC) efficiency, fortify incident response capabilities, and integrate intelligence into holistic risk management frameworks.

The CTIA certification is critical for modern enterprises seeking to achieve a truly predictive security capability. It emphasizes proficiency in key threat modeling frameworks like MITRE ATT&CK and the Cyber Kill Chain, ensuring analysts can precisely map adversary activities and develop robust defensive countermeasures. Through intensive, hands-on lab exercises and real-world case studies, participants will master data processing, structured analysis techniques like ACH (Analysis of Competing Hypotheses), and the effective use of Threat Intelligence Platforms (TIPs). This program not only validates expert knowledge in the threat intelligence lifecycle but also cultivates the critical thinking skills essential to anticipate future attacks and ultimately safeguard an organization's most valuable assets in an increasingly complex and hostile digital environment.

Programme Curriculum

Certified Threat Intelligence Analyst (CTIA) Training Course

Introduction

The contemporary cyber threat landscape is evolving at an unprecedented pace, necessitating a shift from purely reactive security postures to proactive, intelligence-driven defense. Certified Threat Intelligence Analyst (CTIA) Training Course is meticulously designed to equip cybersecurity professionals with a comprehensive, structured methodology for collecting, analyzing, and disseminating timely, actionable intelligence. This program moves beyond simply identifying threats by focusing on understanding the adversary lifecycle, their motivations, and translating raw data from diverse sources including OSINT, HUMINT, and deep/dark web sources into strategic, operational, and tactical intelligence. Successful completion empowers analysts to enhance security operations center (SOC) efficiency, fortify incident response capabilities, and integrate intelligence into holistic risk management frameworks.

The CTIA certification is critical for modern enterprises seeking to achieve a truly predictive security capability. It emphasizes proficiency in key threat modeling frameworks like MITRE ATT&CK and the Cyber Kill Chain, ensuring analysts can precisely map adversary activities and develop robust defensive countermeasures. Through intensive, hands-on lab exercises and real-world case studies, participants will master data processing, structured analysis techniques like ACH (Analysis of Competing Hypotheses), and the effective use of Threat Intelligence Platforms (TIPs). This program not only validates expert knowledge in the threat intelligence lifecycle but also cultivates the critical thinking skills essential to anticipate future attacks and ultimately safeguard an organization's most valuable assets in an increasingly complex and hostile digital environment.

Course Duration

5 days

Course Objectives

1. Master the Threat Intelligence Lifecycle from planning to dissemination.
2. Apply MITRE ATT&CK and Cyber Kill Chain for advanced threat modeling.
3. Execute proficient OSINT and Dark Web data collection methodologies.
4. Develop actionable intelligence for SOC, Incident Response, and Risk Management.
5. Analyze Indicators of Compromise (IoCs) and adversary TTPs using structured techniques.
6. Perform advanced Malware Analysis and threat actor profiling.
7. Integrate and operationalize intelligence using Threat Intelligence Platforms (TIPs).
8. Implement effective Threat Hunting strategies across endpoints and networks.
9. Conduct Strategic, Operational, and Tactical threat intelligence reporting.
10. Utilize Structured Analytical Techniques (SATs) like Analysis of Competing Hypotheses (ACH).
11. Securely share intelligence through established Information Sharing and Analysis Centers (ISACs).
12. Establish a comprehensive, repeatable Threat Intelligence Program within an organization.
13. Leverage threat data for informed Cloud Security and vulnerability management decisions.

Target Audience

1. Cyber Threat Intelligence Analysts
2. Security Operations Center (SOC) Analysts
3. Incident Response Team Members
4. Threat Hunters
5. Information Security Managers/Architects
6. Digital Forensics and Malware Analysts
7. Ethical Hackers and Penetration Testers
8. Risk Management Professionals

Course Modules

Module 1: Introduction and Threat Intelligence Lifecycle

- Define Threat Intelligence (CTI) and distinguish it from raw data and information.
- Explore the Intelligence Life Cycle.
- Differentiate between Strategic, Operational, Tactical, and Technical intelligence types.
- Understand Threat Intelligence Maturity Models and organizational capabilities.
- Examine compliance and ethical/legal considerations in intelligence gathering.
- Case Study: Target Data Breach analysis how strategic CTI failure allowed a sophisticated, multi-stage attack to succeed and the lessons learned for the 'Direction' stage.

Module 2: Cyber Threats and Adversary Profiling

- Identify various Cyber Threats and their classification.
- Profile Threat Actors including State-Sponsored, Cyber Criminals, and Hacktivists.
- Deep dive into the Advanced Persistent Threat (APT) lifecycle and characteristics.
- Map adversary actions using the Cyber Kill Chain methodology.
- Utilize the Pyramid of Pain model for IoC prioritization and defensive planning.
- Case Study: APT41 profiling detailed breakdown of their multi-pronged targeting, historical TTPs, and evolution over time.

Module 3: Threat Modeling and Analysis Frameworks

- Apply the MITRE ATT&CK Framework for detailed adversary TTP mapping.
- Learn the structure and application of the Diamond Model of Intrusion Analysis.
- Master the fundamentals of Structured Analytical Techniques (SATs).
- Execute Analysis of Competing Hypotheses (ACH) to reduce cognitive bias in analysis.
- Develop scenario-based threat models for critical business processes.
- Case Study: Analyzing a breach using ATT&CK mapping the stages of the SolarWinds supply chain attack to specific TTPs for defense enhancement.

Module 4: Data Collection and Processing

- Conduct effective Open-Source Intelligence gathering from public sources.
- Acquire technical data from passive and active feeds
- Process bulk data using methods like normalization, sampling, and visualization.
- Explore legal and ethical considerations for Human Intelligence and Cyber Counterintelligence
- Utilize basic Malware Analysis and sandbox reports for IoC extraction.
- Case Study: MISP Platform Utilization using a real-world MISP instance to ingest, correlate, and normalize IoCs from various threat feeds related to a recent ransomware strain.

Module 5: Threat Hunting and Detection

- Define Threat Hunting and differentiate between hypothesis-driven and TTP-driven hunting.
- Develop hunting hypotheses based on collected intelligence and known adversary TTPs.
- Utilize logging sources and query languages for active threat discovery.
- Implement automation for repeatable hunting processes.
- Pivot from initial IoCs to discover new TTPs and wider campaign activity.
- Case Study: Log4Shell Vulnerability Hunting developing and deploying custom Sigma and YARA rules to retrospectively search SIEM/EDR logs for post-exploitation activities and lateral movement.

Module 6: Intelligence Reporting and Dissemination

- Understand the principles of effective Intelligence Reporting
- Structure reports for different audiences.
- Draft Runbooks and update the knowledge base for incident responders.
- Learn secure and efficient intelligence sharing methods and platforms.
- Evaluate and measure the return on investment and effectiveness of CTI.
- Case Study: Executive Briefing Simulation creating a strategic intelligence report on the geopolitical motives and capabilities of a specific nation-state actor for the C-suite.

Module 7: Threat Intelligence Program Management

- Define the requirements, goals, and scope for a new Threat Intelligence Program.
- Identify necessary personnel, skills, and tools for a dedicated team.
- Establish workflows for seamless integration of CTI into SOC Operations.
- Develop a program review, governance, and continuous improvement plan.
- Integrate CTI into Risk Management and Vulnerability Management processes.
- Case Study: Building a CTI Team developing a talent acquisition strategy and defining role responsibilities for a mid-sized financial institution's new intelligence unit.

Module 8: Advanced Topics and Future Trends

- Explore Cloud Threat Intelligence and securing hybrid/multi-cloud environments.
- Analyze emerging threats in IoT and Operational Technology (OT)/Critical Infrastructure.
- Understand the role of Machine Learning and AI in both CTI and adversary tactics.
- Deep dive into supply chain compromise threats and mitigation.
- Review current international threat intelligence sharing regulations.
- Case Study: Colonial Pipeline Attack analyzing the initial compromise vectors, the role of ransomware-as-a-service, and the cascading impact on critical infrastructure.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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