Training Course on Human-Machine Teaming in Digital Forensics and Incident Response (AI Augmentation)

Professional Development Training Course Outline

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

Course Introduction

Training Course on Human-Machine Teaming in Digital Forensics and Incident Response (AI Augmentation) delves into the transformative intersection of Artificial Intelligence (AI) and the critical domains of Digital Forensics (DFIR). As cyber threats grow in sophistication and volume, human analysts alone struggle to keep pace with the sheer amount of data and the complexity of attack vectors. This program champions a paradigm shift towards Human-Machine Teaming (HMT), empowering forensic investigators and incident responders with cutting-edge AI tools to augment their capabilities, accelerate investigations, and enhance the accuracy and efficiency of their responses. Participants will gain practical skills in leveraging AI for automated threat detection, intelligent data analysis, predictive insights, and streamlined evidence collection, fostering a collaborative synergy between human expertise and machine intelligence to combat advanced cybercrime effectively.

The course emphasizes a hands-on approach, providing participants with the knowledge and practical experience to implement AI-driven solutions within their DFIR workflows. We will explore the latest advancements in machine learning, deep learning, and natural language processing tailored for forensic applications, ensuring that attendees are equipped to navigate the evolving threat landscape with confidence. By fostering a strong understanding of both the capabilities and limitations of AI in DFIR, this training prepares professionals to optimize their operational efficiency, reduce human error, and achieve superior outcomes in incident resolution and evidence-based investigations, ultimately bolstering organizational cybersecurity posture in the digital age.

Programme Curriculum

Training Course on Human-Machine Teaming in Digital Forensics and Incident Response (AI Augmentation)

Introduction

Training Course on Human-Machine Teaming in Digital Forensics and Incident Response (AI Augmentation) delves into the transformative intersection of Artificial Intelligence (AI) and the critical domains of Digital Forensics (DFIR). As cyber threats grow in sophistication and volume, human analysts alone struggle to keep pace with the sheer amount of data and the complexity of attack vectors. This program champions a paradigm shift towards Human-Machine Teaming (HMT), empowering forensic investigators and incident responders with cutting-edge AI tools to augment their capabilities, accelerate investigations, and enhance the accuracy and efficiency of their responses. Participants will gain practical skills in leveraging AI for automated threat detection, intelligent data analysis, predictive insights, and streamlined evidence collection, fostering a collaborative synergy between human expertise and machine intelligence to combat advanced cybercrime effectively.

The course emphasizes a hands-on approach, providing participants with the knowledge and practical experience to implement AI-driven solutions within their DFIR workflows. We will explore the latest advancements in machine learning, deep learning, and natural language processing tailored for forensic applications, ensuring that attendees are equipped to navigate the evolving threat landscape with confidence. By fostering a strong understanding of both the capabilities and limitations of AI in DFIR, this training prepares professionals to optimize their operational efficiency, reduce human error, and achieve superior outcomes in incident resolution and evidence-based investigations, ultimately bolstering organizational cybersecurity posture in the digital age.

Course Duration

10 days

Course Objectives

1. Develop proficiency in integrating Artificial Intelligence and Machine Learning models into Digital Forensics and Incident Response workflows.
2. Implement AI for real-time anomaly detection, advanced threat intelligence correlation, and proactive identification of sophisticated cyberattacks.
3. Utilize AI and Natural Language Processing (NLP) for rapid analysis, prioritization, and summarization of massive forensic datasets.
4. Leverage AI for predictive analytics, anticipating future attack vectors and strengthening proactive cybersecurity measures.
5. Apply AI-powered tools for efficient and comprehensive digital evidence acquisition across diverse platforms including cloud and IoT.
6. Understand and optimize the symbiotic relationship between human analysts and AI algorithms for improved investigative outcomes.
7. Analyze the ethical considerations, bias mitigation strategies, and legal implications of deploying AI in forensic investigations.
8. Explore AI applications for automated artifact extraction and analysis in complex cloud environments.
9. Employ AI for dynamic malware analysis, behavioral profiling, and rapid classification of emerging threats.
10. Design and implement AI-driven Security Orchestration, Automation, and Response (SOAR) playbooks.
11. Conduct advanced threat hunting operations leveraging AI-powered behavioral analytics and pattern recognition.

12. Master techniques for analyzing large-scale unstructured forensic data using AI and distributed computing.
13. Develop strategies for integrating AI tools and developing custom machine learning models for organizational security needs.

Organizational Benefits

- Significantly reduce mean time to detect (MTTD) and mean time to respond (MTTR) to cyber incidents.
- Automate repetitive tasks, allowing human analysts to focus on complex analytical and strategic aspects.
- Leverage AI's ability to identify subtle patterns and anomalies often missed by human analysis.
- Transition from reactive incident handling to predictive threat identification and prevention.
- Optimize resource allocation and reduce operational costs associated with manual data processing and analysis.
- Handle increasing volumes of digital evidence and alerts effectively.
- Minimize burnout by automating mundane tasks and prioritizing critical alerts.
- Generate comprehensive and data-driven forensic reports for legal and internal stakeholders.
- Stay ahead of evolving cyber threats by embracing cutting-edge AI technologies.

Target Audience

1. Digital Forensics Investigators
2. Incident Response Team Members
3. Security Operations Center (SOC) Analysts
4. Cybersecurity Engineers.
5. Threat Hunters
6. IT Security Managers.
7. Legal and Compliance Professionals.
8. Security Consultants

Course Outline

Module 1: Introduction to Human-Machine Teaming in DFIR

- Define Human-Machine Teaming (HMT) and its relevance in modern DFIR.
- Overview of the evolving cyber threat landscape and limitations of traditional DFIR.
- Exploring the synergy: how AI augments human capabilities in forensics and response.
- Discussion of key concepts: AI, Machine Learning, Deep Learning, and their applications.
- *Case Study:* Analyzing a large-scale data breach where manual efforts were overwhelmed, and discussing how HMT could have improved response time and accuracy.

Module 2: Fundamentals of AI and Machine Learning for DFIR

- Introduction to core AI and ML concepts: supervised, unsupervised, and reinforcement learning.
- Key ML algorithms relevant to DFIR: classification, clustering, anomaly detection.
- Data preprocessing, feature engineering, and model training in a forensic context.
- Understanding common AI frameworks and libraries
- *Case Study:* Using a simple ML model to classify malicious files based on static analysis features.

Module 3: AI-Powered Threat Detection and Anomaly Analysis

- Implementing AI for network intrusion detection and host-based anomaly detection.
- Leveraging behavioral analytics to identify deviations from normal baselines.
- Utilizing AI for real-time alert prioritization and false positive reduction.
- Integrating AI with SIEM and EDR platforms for automated threat correlation.
- *Case Study:* Detecting a sophisticated ransomware attack by identifying unusual file access patterns and network communication via AI-driven anomaly detection.

Module 4: Intelligent Data Triage and Evidence Processing

- Applying Natural Language Processing (NLP) for automated log analysis and summarization.
- AI-driven entity extraction and relationship mapping from unstructured data.
- Automated categorization and indexing of digital artifacts.
- Techniques for reducing data volume while preserving forensic integrity using AI.
- *Case Study:* Expediting an insider threat investigation by using NLP to quickly parse and categorize thousands of employee communications for suspicious keywords and sentiment.

Module 5: AI in Cloud Forensics

- Challenges of digital forensics in multi-cloud and hybrid cloud environments.
- AI techniques for collecting and analyzing cloud-native logs and artifacts.
- Automated identification of misconfigurations and unauthorized access in cloud infrastructure.
- Leveraging cloud provider APIs and AI services for forensic investigations.
- *Case Study:* Investigating a compromised AWS S3 bucket by employing AI to analyze cloud trail logs and identify the root cause and exfiltrated data.

Module 6: AI for Malware Analysis and Reverse Engineering

- AI-driven classification and clustering of malware samples.
- Automated behavioral analysis of suspicious executables in sandboxed environments.
- Using AI to identify obfuscation techniques and unpack packed malware.
- Predictive modeling for identifying new malware families and variants.
- *Case Study:* Utilizing an AI model to quickly classify a new strain of polymorphic malware, enabling rapid signature generation and defensive measures.

Module 7: Human-in-the-Loop (HITL) DFIR Operations

- Designing effective HITL workflows for optimal human-AI collaboration.
- Strategies for human oversight, validation, and refinement of AI outputs.
- Addressing trust and transparency issues in AI-assisted investigations.
- Feedback loops and continuous learning for improving AI model performance.
- *Case Study:* A team of forensic analysts collaborating with an AI system to investigate a complex APT attack, with the AI identifying initial leads and the human analysts conducting in-depth verification and strategic planning.

Module 8: Ethical Considerations and Bias in AI for DFIR

- Understanding potential biases in AI models and their impact on forensic outcomes.
- Strategies for ensuring fairness, accountability, and transparency in AI deployments.
- Legal and privacy implications of using AI in digital investigations.
- Data governance and responsible AI development in a forensic context.
- *Case Study:* Discussing a hypothetical scenario where an AI model showed bias in flagging certain user activities as suspicious, and how to mitigate such biases through data diversity and algorithmic transparency.

Module 9: Advanced AI Techniques: Deep Learning & Generative AI

- Introduction to Deep Learning architectures (e.g., CNNs, RNNs, Transformers) for complex data analysis.
- Applying Generative AI (e.g., LLMs) for summarizing forensic reports and generating investigative hypotheses.
- Deep learning for image and video forensics.
- Reinforcement learning for adaptive incident response playbooks.
- *Case Study:* Using a Large Language Model to rapidly summarize thousands of pages of network logs and security alerts, providing a concise overview for incident commanders.

Module 10: AI in IoT and Mobile Forensics

- Challenges of data extraction and analysis from diverse IoT devices.
- AI techniques for correlating data from multiple IoT sources.
- Automated analysis of mobile device artifacts and application data.
- Leveraging AI for location tracking and behavioral profiling from mobile data.
- *Case Study:* Reconstructing a timeline of events in a smart home intrusion by analyzing data from interconnected IoT devices) using AI.

Module 11: Predictive Analytics and Threat Intelligence Augmentation

- Building predictive models to anticipate future cyberattacks and vulnerabilities.
- AI-driven enrichment and correlation of threat intelligence feeds.
- Identifying emerging attack trends and threat actor methodologies.
- Developing proactive defense strategies based on AI-generated insights.
- *Case Study:* Using AI to predict the next target of a known threat group based on their past attack patterns and industry-specific vulnerabilities, allowing for proactive defensive measures.

Module 12: Security Orchestration, Automation, and Response (SOAR) with AI

- Designing and implementing AI-powered SOAR playbooks for automated incident response.
- Integrating AI modules into existing SOAR platforms.
- Automated containment, eradication, and recovery actions.
- Workflow automation and alert enrichment using AI.
- *Case Study:* Automating the response to a phishing incident, where AI identifies the malicious email, isolates affected endpoints, and triggers an automated forensic image collection process.

Module 13: Building an AI-Driven DFIR Lab and Toolkit

- Setting up an AI-ready forensic workstation and lab environment.
- Overview of open-source and commercial AI tools for DFIR.
- Developing custom AI scripts and models using Python and relevant libraries.
- Best practices for data collection, storage, and management for AI training.
- *Case Study:* Designing a scalable AI-driven forensic analysis pipeline for a large enterprise, including hardware, software, and data flow considerations.

Module 14: Advanced Threat Hunting and Digital Evidence Correlation with AI

- Leveraging AI for proactive threat hunting beyond signature-based detection.
- Graph analytics and AI for identifying complex attack chains and lateral movement.
- Correlating disparate digital evidence sources using machine learning.

- Identifying subtle indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs).
- *Case Study:* Uncovering a previously undetected advanced persistent threat (APT) by using AI to analyze seemingly unrelated log entries and network flows, revealing a sophisticated multi-stage attack.

Module 15: Future Trends and Evolution of Human-Machine Teaming in DFIR

- Emerging AI technologies and their potential impact on DFIR
- The evolving role of the human analyst in an AI-augmented DFIR landscape.
- Challenges and opportunities in integrating AI into legal and regulatory frameworks.
- The future of autonomous incident response and predictive forensics.
- *Case Study:* Exploring a hypothetical future scenario where fully autonomous AI agents handle initial incident triage and containment, leaving only highly complex and nuanced cases for human intervention.

Training Methodology

- **Instructor-Led Sessions:** Expert-led lectures with real-world examples and interactive discussions.
- **Hands-on Labs and Exercises:** Extensive practical exercises using industry-standard tools and custom AI scripts on simulated forensic environments.
- **Case Study Analysis:** In-depth examination of real-world cyber incidents and how AI could be applied or has been applied.
- **Group Projects and Collaborative Learning:** Participants will work in teams to solve complex DFIR challenges using AI.
- **Live Demonstrations:** Showcase of cutting-edge AI tools and platforms in action.
- **Q&A and Discussion Forums:** Dedicated time for participants to ask questions and share insights.
- **Post-Training Resources:** Access to course materials, lab guides, and recommended readings for continued learning.

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.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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