AI and Generative AI for Cybersecurity 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 digital battlespace is undergoing a paradigm shift with the rapid deployment of Artificial Intelligence and Generative AI. Traditional perimeter defense models are proving insufficient against AI-enabled threats like polymorphic malware and sophisticated deepfake phishing campaigns. This course addresses the critical need for security professionals to master the dual nature of this technology: leveraging AI for proactive defense while simultaneously fortifying systems against Adversarial AI. The future of Cyber Threat Intelligence and Incident Response is being written by machine learning, making this expertise non-negotiable for maintaining a robust security posture in the era of hyper-automation.

AI and Generative AI for Cybersecurity Training Course provides a deep, hands-on exploration of integrating Large Language Models and other generative models into the Security Operations Center Participants will gain practical skills in implementing AI for anomaly detection, automating vulnerability management, and conducting AI Red Teaming exercises to find model weaknesses before attackers do. By synthesizing Data Science principles with core cybersecurity frameworks, this curriculum ensures graduates are equipped to lead the charge in deploying Adaptive Security Measures that turn the tide against the most complex, rapidly evolving Zero-Day attacks.

Programme Curriculum

AI and Generative AI for Cybersecurity Training Course

Introduction

The contemporary digital battlespace is undergoing a paradigm shift with the rapid deployment of Artificial Intelligence and Generative AI. Traditional perimeter defense models are proving insufficient against AI-enabled threats like polymorphic malware and sophisticated deepfake phishing campaigns. This course addresses the critical need for security professionals to master the dual nature of this technology: leveraging AI for proactive

defense while simultaneously fortifying systems against Adversarial AI. The future of Cyber Threat Intelligence and Incident Response is being written by machine learning, making this expertise non-negotiable for maintaining a robust security posture in the era of hyper-automation.

AI and Generative AI for Cybersecurity Training Course provides a deep, hands-on exploration of integrating Large Language Models and other generative models into the Security Operations Center Participants will gain practical skills in implementing AI for anomaly detection, automating vulnerability management, and conducting AI Red Teaming exercises to find model weaknesses before attackers do. By synthesizing Data Science principles with core cybersecurity frameworks, this curriculum ensures graduates are equipped to lead the charge in deploying Adaptive Security Measures that turn the tide against the most complex, rapidly evolving Zero-Day attacks.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Evaluate the dual-use nature of Generative AI in both offensive and proactive cyber defense strategies.
2. Design and deploy AI-driven anomaly detection systems for real-time User and Entity Behavior Analytics
3. Implement Large Language Models for threat intelligence summarization and automated incident response playbook generation.
4. Master the principles of Adversarial AI and execute techniques like model inversion and data poisoning to test defense resilience.
5. Apply secure Prompt Engineering techniques to GenAI tools to prevent Prompt Injection and data leakage attacks.
6. Develop and secure machine learning models against Evasion Attacks and implement robust AI Model Governance frameworks.
7. Automate routine Vulnerability Management and triage tasks using intelligent AI/ML workflows.
8. Conduct AI Red Teaming simulations to proactively identify and mitigate vulnerabilities in deployed AI systems.
9. Utilize synthetic data generation via Generative Adversarial Networks for secure and realistic Security Operations Center (SOC) training.
10. Analyze the impact of AI on specialized threats, including deepfake phishing and polymorphic malware generation.
11. Integrate AI/ML outputs effectively into existing Security Information and Event Management and Security Orchestration, Automation, and Response platforms.
12. Comply with emerging global regulations like the EU AI Act and established frameworks such as MITRE ATLAS?äó for AI security.
13. Contribute to building a secure, AI-ready Enterprise Security Architecture that is both scalable and compliant.

Target Audience

1. Cybersecurity Analysts/Engineers.
2. Security Operations Center Teams.
3. Threat Intelligence Specialists.
4. Penetration Testers & Red Teamers.
5. Security Architects.

6. Data Scientists/ML Engineers in Security.
7. Vulnerability Management Teams.
8. IT/Security Managers & CISOs.

Course Modules

Module 1: Foundations of AI and GenAI in Cyber Defense

- Machine Learning, Deep Learning, and the distinction of Generative AI
- The evolution of the threat landscape with AI.
- Understanding the AI Attack Surface.
- Key AI-Native security tools and their role in the modern SOC
- Case Study: Analyzing how a major financial institution leveraged LLMs to achieve a 40% reduction in False Positives during initial alert triage.

Module 2: Securing the Generative AI Pipeline

- Data Poisoning and Model Inversion Attacks on training data and deployed models.
- Techniques for Data Masking and synthetic data generation for privacy-preserving AI training.
- Introduction to AI Model Governance, reproducibility, and auditable logging.
- Secure MLOps.
- Case Study: The mitigation strategy for a supply chain firm hit by a targeted data poisoning attack that corrupted its fraud detection model.

Module 3: Prompt Engineering for Defensive & Offensive Use

- Mastering foundational and advanced Prompt Engineering techniques for security tasks.
- Identifying and preventing Prompt Injection attacks, including direct and indirect techniques.
- Using LLMs for code analysis, security vulnerability discovery, and generating proof-of-concept exploits
- Developing security-focused agents using LLM orchestration and function calling.
- Case Study: A hands-on lab simulating a successful indirect prompt injection attack via a malicious web page and the LLM defensive hardening steps.

Module 4: AI for Advanced Threat Detection and Anomaly Detection

- Implementing User and Entity Behavior Analytics using clustering and deep learning.
- AI-driven detection of Zero-Day and Polymorphic Malware by analyzing code mutation patterns.
- Building effective ML classifiers for network traffic analysis and Intrusion Detection Systems
- Feature engineering and dataset preparation for optimal ML model performance in threat hunting.
- Case Study: Deployment of an LSTM-based deep learning model to detect a novel Domain Generation Algorithm botnet activity in a global enterprise network.

Module 5: AI Red Teaming and Adversarial Resilience

- The methodology and phases of a professional Adversarial AI Red Team exercise.
- Techniques for generating Adversarial Examples to test the robustness of target ML models.
- Adversarial Training, input sanitization, and model monitoring for drift.
- Mapping AI-related threats to the MITRE ATLAS?äó framework for standardized reporting.
- Case Study: A mock red team engagement demonstrating an Evasion Attack on an image-based CAPTCHA using minor pixel perturbations and the subsequent model hardening.

Module 6: Automation and Orchestration with AI in the SOC

- Leveraging AI to automate Threat Intelligence gathering, analysis, and report summarization.
- Integrating AI into Security Orchestration, Automation, and Response platforms for automated playbooks.
- AI-assisted Incident Triage and prioritizing alerts based on projected business impact.
- Utilizing GenAI for generating customizable, plain-language Post-Incident Reports.
- Case Study: Automation of a spear-phishing incident response, from detection and email isolation to ticket generation and CTI lookup, reducing response time by 75%.

Module 7: Specialized Generative AI Attack and Defense

- Defense against Deepfake Phishing and Voice Cloning.
- Detecting AI-generated malicious code and scripts using natural language processing security models.
- The offensive use of LLMs for rapid Exploit Generation and fuzzing.
- Securing Cloud-Native AI deployments and addressing vendor-specific AI platform risks
- Case Study: Evaluating the efficacy of an AI-driven email gateway in identifying a state-sponsored, highly customized deepfake voice phishing attempt targeting executive leadership.

Module 8: Ethical, Legal, and Strategic AI in Cybersecurity

- AI Ethics and bias in security models.
- Understanding the legal and compliance landscape.
- Developing an AI Risk Management Framework and responsible AI use policy for the enterprise.
- Strategic roadmap for adopting AI-ready Enterprise Security Architecture and required skill sets.
- Case Study: Discussion of a major regulatory fine due to an AI system's lack of explainability and the steps taken to achieve compliance post-breach.

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