Mastering 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 advent of Generative AI, particularly Large Language Models, marks a paradigm shift in the global cybersecurity landscape. Mastering Generative AI for Cybersecurity Training Course is designed to equip cybersecurity professionals and business leaders with the essential knowledge and hands-on skills required to both leverage GenAI for proactive cyber defense and to safeguard organizational assets against AI-powered threats. We address the critical need for a workforce that can transition from reactive defense to AI-driven security operations, focusing on practical application, ethical AI governance, and securing the complex AI development lifecycle. This course is your definitive path to becoming a frontrunner in the next generation of digital defense.

This intensive, cutting-edge curriculum delves into the dual nature of Generative AI as a powerful security multiplier and as an amplified threat vector. Participants will master prompt engineering for threat intelligence gathering, automate incident response workflows, and build resilient defenses against novel attacks like deepfakes, prompt injection, and polymorphic malware. Through real-world case studies and immersive virtual lab environments, you will gain the competence to strategically integrate GenAI tools into your Security Operations Center, ensuring data privacy and maintaining regulatory compliance in the AI era.

Programme Curriculum

Mastering Generative AI for Cybersecurity Training Course

Introduction

The advent of Generative AI, particularly Large Language Models, marks a paradigm shift in the global cybersecurity landscape. Mastering Generative AI for Cybersecurity Training Course is designed to equip cybersecurity professionals and business leaders with the essential knowledge and hands-on skills required to

both leverage GenAI for proactive cyber defense and to safeguard organizational assets against AI-powered threats. We address the critical need for a workforce that can transition from reactive defense to AI-driven security operations, focusing on practical application, ethical AI governance, and securing the complex AI development lifecycle. This course is your definitive path to becoming a frontrunner in the next generation of digital defense.

This intensive, cutting-edge curriculum delves into the dual nature of Generative AI as a powerful security multiplier and as an amplified threat vector. Participants will master prompt engineering for threat intelligence gathering, automate incident response workflows, and build resilient defenses against novel attacks like deepfakes, prompt injection, and polymorphic malware. Through real-world case studies and immersive virtual lab environments, you will gain the competence to strategically integrate GenAI tools into your Security Operations Center, ensuring data privacy and maintaining regulatory compliance in the AI era.

Course Duration

5 days

Course Objectives

1. Master Prompt Engineering for AI-driven threat intelligence gathering and analysis.
2. Design and implement secure LLM deployments and GenAI application security architectures.
3. Analyze and mitigate AI-specific vulnerabilities, including prompt injection and data poisoning attacks.
4. Develop automated incident response playbooks using Generative AI for faster triage and remediation.
5. Leverage GenAI for advanced malware analysis and polymorphic threat detection.
6. Apply Generative AI to enhance vulnerability management and automated code review in DevSecOps pipelines.
7. Construct realistic AI-powered phishing and social engineering defense strategies, including deepfake detection.
8. Understand the principles of Adversarial AI and implement effective robustness training countermeasures.
9. Integrate GenAI tools for improving Security Information and Event Management and Security Orchestration, Automation, and Response (SOAR) capabilities.
10. Establish and enforce an ethical AI governance framework to ensure responsible AI use and compliance.
11. Utilize GenAI to create synthetic data for effective, privacy-preserving security testing and model training.
12. Conduct AI red teaming and AI blue teaming exercises to validate model security posture.
13. Analyze the impact of GenAI on cyber risk management and enterprise-wide security strategy.

Target Audience

1. Security Operations Center (SOC) Analysts and Managers
2. Threat Intelligence Analysts and Hunters
3. Security Architects and Engineers
4. Chief Information Security Officers (CISOs) and Security Leaders
5. Application Security (AppSec) and DevSecOps Professionals
6. Incident Response and Digital Forensics Teams
7. Ethical Hackers and Penetration Testers
8. Risk Management and Compliance Officers

Course Modules

Module 1: Generative AI and LLMs: Foundations for Cybersecurity

- Concepts & Architecture
- Cybersecurity Applications.
- Security of LLMs.
- Hands-on Tooling.
- Case Study: Analyzing a major breach where a compromised LLM API exposed sensitive organizational data.

Module 2: Prompt Engineering for Threat Intelligence and Defense

- Advanced Prompting Techniques.
- Threat Intel Generation.
- Vulnerability & Exploit Research.
- Prompt Injection Defense.
- Case Study: Developing a custom security GPT to summarize all indicators of compromise from live security news feeds.

Module 3: Defending Against AI-Powered Malicious Content

- Automated Phishing and Social Engineering.
- Deepfake Detection Methods.
- Malicious Code Generation
- Content Moderation & Filtering.
- Case Study: Simulating an executive deepfake fraud attempt and outlining the necessary technical and procedural response.

Module 4: Securing the Generative AI Lifecycle (SecMLOps)

- Data Security
- Model Hardening.
- Deployment Security.
- Monitoring and Governance.
- Case Study: Mitigating a successful data poisoning attack on a fraud detection model and restoring model integrity.

Module 5: AI-Driven Security Operations and Automation

- SIEM/SOAR Augmentation.
- Incident Response (IR) Playbooks.
- Threat Hunting.
- Automated Vulnerability Remediation.
- Case Study: Using a GenAI-powered assistant to reduce Mean Time To Detect and Mean Time To Respond during a large-scale network intrusion.

Module 6: Adversarial AI and Model Attack Surfaces

- Model Inversion Attacks.
- Model Theft and Extraction.
- Evasion Attacks
- Defensive Measures.
- Case Study: Demonstrating an evasion attack against an image-based CAPTCHA or a network traffic anomaly detector.

Module 7: Legal, Ethical, and Compliance Implications

- Ethical AI Principles.
- Data Privacy & Compliance.
- Transparency and Auditability.
- Policy Development.
- Case Study: Reviewing the legal and ethical fallout from an AI system generating biased or discriminatory security decisions.

Module 8: Advanced Topics and Future Trends

- Generative AI in Penetration Testing.
- Cybersecurity Mesh Architecture.
- AI Blue Teaming.
- Future of Autonomous Security Agents.
- Case Study: Designing and executing an AI red teaming exercise against a mock financial services application.

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