Skill-Lyft

Empowering Skills, Elevating Careers

AI-Powered Cybersecurity: Defense and Offense

14 – 15 July 2025 The Majestic Hotel Kuala Lumpur

Sarbojit Madhab Bose
Cybersecurity Advisor & Trainer

1 Course Overview

What if your next cyber defense strategy could be the difference between your organization staying secure or becoming the next headline?

In today's digital battleground, cyber threats evolve at lightning speed, and traditional defenses just can't keep up. Leaders who harness AI-driven cybersecurity don't just react, they predict, prevent, and outsmart attackers before damage happens.

This immersive two-day workshop is designed for cybersecurity professionals, security engineers, analysts, and IT teams ready to level up their skills and **lead the charge against modern cyber threats**.

You'll discover how AI transforms threat detection, accelerates incident response, and sharpens vulnerability assessments, all while understanding the darker side of AI in offensive cyber tactics.

Through hands-on labs, real-world attack simulations, and ethical discussions, you'll walk away equipped to:

- ✓ Detect and **neutralize advanced threats** faster than ever
- ✓ Build AI-powered **defenses** that adapt and learn with every attack
- ✓ Anticipate adversaries **using AI offensively** and prepare countermeasures
- ✓ Develop responsible, **forward-looking AI security** strategies that protect your organization's future

If you want to stay one step ahead in the cyber war and turn AI into your most powerful ally, this is the workshop you can't afford to miss.

2 Course Lead Trainer

Sarbojit Madhab Bose
Cybersecurity Advisor & Trainer

Sarbojit Bose is a highly accomplished Trainer, Facilitator, Mentor and Consultant with deep **expertise in Information Technology**, **Cybersecurity**, **Cloud Security**, **Data Privacy & Protection**, and **Program & Project Management**. His distinguished **career spans 33 years** in the ICT industry, during which he has mastered every functional area of IT – Service Program & Project Delivery, Service Operations, GRC (Governance, Risk & Compliance), Management, Audits, and Assessments.

With 25 years of experience working with top-tier MNCs such as HCL, HP, Tech Mahindra, EDS, Dimension Data, and T-Systems, Sarbojit has delivered impactful results across India, the USA, the UK, South Africa, Japan, Malaysia, Singapore and multiple APAC nations. Currently, he is the owner and general manager of Cyberservices, an IT Training and Consultancy firm, where he collaborates with leading global training and education providers.

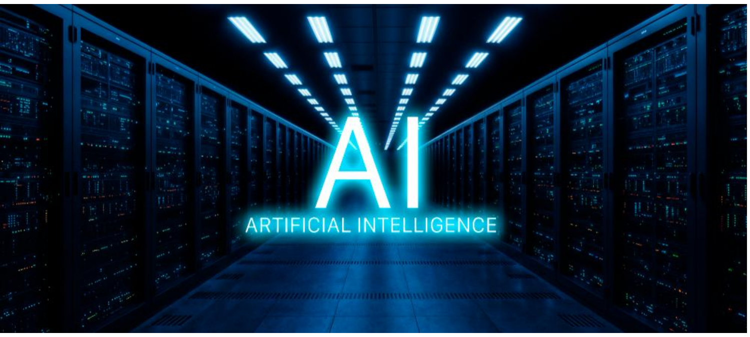
Sarbojit boasts an impressive track record of **over 12,000 hours of training and facilitation of professional courses in the past six years**. Additionally, he has accumulated more than **20,000 hours of consultancy expertise** in IT Security, Cybersecurity, and Curriculum Development over the past 15 years. His core competencies span Cybersecurity, Information Security, IT Service Management, DevSecOps, and Data Privacy, with certifications and affiliations from prestigious organizations such as Cloud Security Alliance (CSA), ISC2, ISACA, APMG, PeopleCert, and PECB.

3 Course Objectives & Benefits

Objectives

By the end of this workshop, you will be able to:

- ✓ Gain a **comprehensive understanding** of how AI is transforming both defensive and offensive strategies.
- ✓ Explore a variety of **AI-driven techniques** specifically designed for threat detection, in-depth analysis, and the automation of rapid response mechanisms.
- ✓ Learn how to effectively leverage AI to proactively **identify potential threats** and detect vulnerabilities before they can be exploited.
- ✓ Develop **well-structured strategies** for the successful implementation of AI-powered security solutions aimed at enhancing cybersecurity resilience.



Benefits to Your Company

In today's cyber battlefield, AI isn't just an upgrade, it's your frontline defense. This course builds teams who can:

- ✓ **Fortify your cybersecurity fortress** by embedding cutting-edge AI solutions that boost resilience and protect your critical assets.
- ✓ **Automate threat detection** and response so attacks are stopped in their tracks before they escalate into costly breaches.
- ✓ Stay **ahead of the hackers' playbook** by proactively hunting sophisticated threats and spotting vulnerabilities before adversaries do.
- ✓ Craft **AI-driven strategies** designed to outsmart evolving cyberattacks and keep your defenses one step ahead.
- ✓ Champion **responsible AI** use by balancing innovation with ethics to minimize risks and build trust across your security ecosystem.

Result? **Faster responses. Stronger defenses. Reduced risks.**

4 Course Agenda Day 1

Module 1: AI Fundamentals for Cybersecurity

- Key AI concepts: machine learning, deep learning, natural language processing, computer vision.
- Applications of AI in cybersecurity: threat detection, vulnerability assessment, incident response, security automation.
- Activity: "**AI Use Case Brainstorming**" - Group discussion on potential AI applications in cybersecurity.

Module 2: AI-Driven Threat Detection and Analysis

- Anomaly detection using machine learning.
- Malware analysis and classification with AI.
- Threat intelligence and prediction using AI.
- Activity: "**Anomaly Detection with AI**" - Hands-on exercise using AI tools to analyze network traffic and identify anomalies.

Module 3: AI-Powered Incident Response and Automation

- Automating incident response with AI.
- AI-driven security orchestration, automation, and response (SOAR) solutions.
- Using AI for threat hunting and vulnerability discovery.
- Activity: "**Incident Response Simulation**" - Group exercise simulating a cyberattack and using AI tools for response and mitigation.

Module 4: Building AI-Powered Security Defenses

- Designing and implementing AI-based security solutions.
- Integrating AI with existing security infrastructure.
- Evaluating the effectiveness of AI-powered security controls.
- Activity: "**AI Security Solution Design**" - Group project designing an AI-powered security solution for a specific scenario.

Module 5: Hands-on with AI Security Tools

- Exploring AI-powered security tools and platforms.
- Practical exercises in using AI for threat detection, analysis, and response.
- Q&A and open discussion on challenges and opportunities in AI-driven security.

Course Schedule:

08:30-09:00	09:00-10:30	10:30-11:00	11:00-13:00	13:00-14:00	14:00-15:30	15:30-16:00	16:00-17:00
Registration	Upskilling	Break	Upskilling	Break	Upskilling	Break	Upskilling

Note:

All modules will be delivered across Day 1 and Day 2. However, the trainer may adjust the sequence, modify content, or emphasize specific topics based on the delegates' skills and experience.

5 Course Agenda Day 2

Module 6: AI in Offensive Security

- AI-powered penetration testing and vulnerability scanning.
- Using AI for social engineering and phishing attacks.
- AI-driven malware generation and evasion techniques.
- Activity: "**AI-Powered Vulnerability Scanning**" - Hands-on exercise using AI tools to scan for vulnerabilities in web applications.

Module 7: Adversarial AI and Countermeasures

- Understanding adversarial attacks against AI systems.
- Defending against AI-powered attacks.
- Building robust and resilient AI models for security.
- Activity: "**Adversarial Attack Simulation**" - Group exercise simulating an adversarial attack against an AI-powered security system.

Module 8: Ethical Considerations of AI in Cybersecurity

- The potential for bias and discrimination in AI systems.
- The risks of AI-driven cyber warfare and autonomous weapons.
- The importance of responsible AI development and deployment.
- Activity: "**Ethical Debate**" - Group discussion on the ethical implications of AI in cybersecurity offense and defense.

Module 9: The Future of AI in Cybersecurity

- Emerging trends and advancements in AI for cybersecurity.
- The evolving role of AI in the cybersecurity landscape.
- The future of human-AI collaboration in cybersecurity.
- Activity: "**Future Scenario Planning**" - Group brainstorming on potential future applications and challenges of AI in cybersecurity.

Module 10: Building a Responsible AI-Powered Security Strategy

- Developing a comprehensive AI security strategy that incorporates ethical considerations.
- Implementing safeguards and controls to mitigate potential risks.
- Promoting transparency and accountability in AI-driven security solutions.

Course Schedule:

08:30-09:00	09:00-10:30	10:30-11:00	11:00-13:00	13:00-14:00	14:00-15:30	15:30-16:00	16:00-17:00
Registration	Upskilling	Break	Upskilling	Break	Upskilling	Break	Upskilling

Note:

All modules will be delivered across Day 1 and Day 2. However, the trainer may adjust the sequence, modify content, or emphasize specific topics based on the delegates' skills and experience.

6 Who Should Attend

This workshop is suitable for both **experienced professionals** seeking to deepen their knowledge and those **new to the field** looking to build a strong foundation in AI-powered cybersecurity, including but not limited to:

Role	Relevancy	Why?
Cybersecurity Analysts	⭐⭐⭐	Provides practical AI tools and techniques to strengthen real-time monitoring, threat detection, and response capabilities.
Security Engineers	⭐⭐⭐	Equips them with AI-based frameworks to design and implement advanced, proactive security systems.
SOC (Security Operations Center) Teams	⭐⭐⭐	Enhances their ability to rapidly detect, assess, and neutralize threats using AI-driven automation and analytics.
IT Security Managers	⭐⭐⭐	Offers strategic insights to integrate AI into the organization's cybersecurity roadmap and improve operational resilience.
Incident Response Teams	⭐⭐⭐	Simulates AI-assisted attack scenarios and teaches automated response strategies for faster mitigation.
Ethical Hackers / Penetration Testers	⭐⭐⭐	Demonstrates how AI is used for offensive security, including phishing, malware generation, and vulnerability scanning.
Threat Intelligence Analysts	⭐⭐⭐	Strengthens threat modeling and prediction by incorporating AI to uncover and assess evolving attack vectors.
Cloud Security Engineers	⭐⭐⭐	Helps identify and respond to cloud-specific threats using AI-powered tools and detection models.
Risk Management Professionals	⭐⭐⭐	Equips them to assess emerging AI-related cyber risks and embed resilience into governance structures.
AI / Data Science Professionals	⭐⭐⭐	Bridges AI skills with cybersecurity applications, offering real-world use cases and ethical considerations.
DevSecOps Engineers	⭐⭐⭐	Enables seamless integration of AI into DevSecOps pipelines for continuous security monitoring and compliance.
Compliance & Governance Officers	⭐⭐	Improves their understanding of AI's role in enforcing cybersecurity compliance and ethical risk controls.
IT Auditors	⭐⭐	Introduces AI-based monitoring and threat analysis tools to support audit objectives around cybersecurity.
CISOs & Senior IT Leaders	⭐⭐	Provides high-level strategic guidance on leveraging AI for enterprise-wide cyber defense and innovation.
Digital Forensics Specialists	⭐⭐	Adds AI-enhanced investigation techniques for breach analysis, data recovery, and adversarial behavior detection.
Software Security Architects	⭐⭐	Supports the design of AI-enhanced secure architecture for both infrastructure and applications.
Cyber Law & Policy Professionals	⭐⭐	Offers awareness of ethical implications, regulatory impacts, and governance related to AI-powered cyber tools.
Investigative Journalists	⭐	May gain insight into AI-generated cyber threats but requires prior tech background to fully benefit.
General IT Professionals	⭐	Some exposure to cybersecurity, but this course assumes a foundational understanding of threat landscapes.

⭐⭐⭐ **Highly Relevant** ⭐⭐ **Relevant** ⭐ **Somewhat Relevant**

Let’s Level Up!

Are you ready to empower your skills and ultimately elevate your career?

Standard Fee	**: RM3,500/pax**
Group Fee	**: RM3,350/pax (min 3 pax)**

✓ Fees are per participant & inclusive of 8% SST.
✓ This course is **100% claimable** through HRD Corp Claimable Course (SBL-KHAS) Scheme: Employer-Specific Course

Step 1: Click the registration link here:

→ https://www.skill-lyft.com/workshop-series-registration-form or scan the QR code below and complete the online form.

Step 2: We’ll review your submission and email the relevant documents:

→ If applying for HRD Corp grant: You’ll receive supporting documents to complete your grant application.
→ If not applying for grant: You’ll receive an invoice for direct payment.

Need help or have questions?
Reach out to us at registration@skill-lyft.com

Skill Lyft (M) Sdn. Bhd. is a registered Training Provider under HRD Corp.
All courses approved by HRD Corp.

For more information / enquiries, please contact:

Skill Lyft (M) Sdn. Bhd. 202201042066 (1487763-T)
Level 3, Wisma Suria, Jalan Teknokrat 6, Cyber 5, 63000 Cyberjaya, Selangor, Malaysia.

☎ +60 11 3613 4122 ✉ hello@skill-lyft.com 🌐 www.skill-lyft.com