Skill-Lyft

*Empowering Skills, Elevating Careers*

**2025 Workshop Series**

# AI-Powered Cybersecurity: Defense and Offense

26 – 27 May 2025
The Majestic Hotel Kuala Lumpur, Autograph Collection

**Sarbojit Bose**
*Cybersecurity Advisor & Corporate Trainer*

HRD Corp Claimable Course (SBL-KHAS) Scheme
Employer-Specific Course

# COURSE Lead Trainer

**Sarbojit Bose**
*Cybersecurity Advisor & Corporate 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.

With his extensive experience and authoritative presence in the field, Sarbojit M. Bose is a trusted industry leader, dedicated to empowering professionals and organizations worldwide with cutting-edge knowledge and skills in IT security and management.

# COURSE Overview

In an era where cyber threats are rapidly evolving, Artificial Intelligence (AI) is transforming both defensive and offensive cybersecurity strategies. This two-day course is designed to equip cybersecurity professionals, security engineers, analysts, and IT professionals with the knowledge and hands-on experience needed to leverage AI in modern cybersecurity operations.

Participants will explore the about AI in cybersecurity, learning how AI enhances threat detection, incident response, and vulnerability assessment while also examining its role in offensive security tactics. Through interactive sessions, hands-on exercises, and ethical discussions, attendees will gain a deep understanding of AI-powered cybersecurity solutions and their implications for the future.

Additionally, the course will delve into the latest AI-driven attack methodologies and countermeasures, providing participants with insight into adversarial AI tactics. By the end of this course, attendees will be well-prepared to implement AI-powered security frameworks, develop responsible AI security strategies, and defend against evolving cyber threats.

# COURSE Objectives

By the end of this course, delegates will be able to:

1. Gain a comprehensive understanding of how artificial intelligence is transforming both defensive and offensive strategies in the field of cybersecurity.
2. Explore a variety of AI-driven techniques specifically designed for threat detection, in-depth analysis, and the automation of rapid response mechanisms.
3. Learn how to effectively leverage artificial intelligence to proactively identify potential threats and detect vulnerabilities before they can be exploited.
4. Develop well-structured strategies for the successful implementation of AI-powered security solutions aimed at enhancing cybersecurity resilience.
5. Engage in discussions regarding the ethical considerations, potential risks, and broader implications associated with integrating AI into cybersecurity frameworks.

# BENEFITS to the Company

1. Strengthen the overall cybersecurity infrastructure by integrating advanced artificial intelligence-driven solutions that enhance protection and resilience against cyber threats.
2. Automate the processes of threat detection and incident response using AI technologies, thereby significantly reducing potential damage and minimizing security breaches.
3. Stay ahead of increasingly sophisticated cybercriminal activities by leveraging artificial intelligence for proactive threat hunting and early identification of vulnerabilities.
4. Implement well-structured AI-based strategies specifically designed to counter adversarial attacks and mitigate evolving cybersecurity threats effectively.
5. Promote the responsible deployment of artificial intelligence in cybersecurity operations while actively working to minimize biases, risks, and unintended consequences.

Skill-Lyft
Empowering Skills, Elevating Careers

# COURSE Agenda – Day 1

***Event Schedule***

**08:30 – 09:00**
Registration, Refreshments

**09:00 – 10:30**
Learning & Development

**10:30 – 10:45**
Refreshments, Networking

**10:45 – 12:00**
Learning & Development

**12:00 – 13:00**
Lunch Break, Networking

**13:00 – 15:45**
Learning & Development

**15:45 – 16:00**
Refreshments, Networking

**16:00 – 17:00**
Learning & Development

*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.*

## AI for Cybersecurity Defense

**Introduction**
- "The AI-Powered Security Landscape" - Interactive discussion on current cybersecurity challenges and the potential of AI.
- Course overview and objectives.

**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 Agenda – Day 2

***Event Schedule***

**08:30 – 09:00**
Registration, Refreshments

**09:00 – 10:30**
Learning & Development

**10:30 – 10:45**
Refreshments, Networking

**10:45 – 12:00**
Learning & Development

**12:00 – 13:00**
Lunch Break, Networking

**13:00 – 15:45**
Learning & Development

**15:45 – 16:00**
Refreshments, Networking

**16:00 – 17:00**
Learning & Development

*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.*

## AI for Cybersecurity Offense and Ethical Considerations

**Recap of Day 1**
- Review key concepts and applications of AI in cybersecurity defense.
- Questions and discussion on Day 1 activities.

**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 Wrap-up, Q&A, & Feedback**
- Final questions and discussion on the course topics.
- Course feedback and evaluation.
- Distribution of resources and further learning opportunities on AI in cybersecurity.

# WHO Should Attend

This course has been well-prepared for professionals who are seeking to integrate AI into their security strategies, including but not limited to:

- Cybersecurity analysts
- Security engineers
- SOC (Security Operations Center) professionals
- IT security managers
- Ethical hackers and penetration testers
- Threat intelligence analysts
- Chief Information Security Officers (CISOs)
- Incident response teams
- Digital forensic specialists
- Network security professionals
- Cloud security engineers
- AI and data science professionals working in cybersecurity
- Compliance officers focusing on cybersecurity regulations
- Risk management professionals
- DevSecOps engineers
- Cybersecurity consultants
- IT auditors and governance professionals
- Software security architects
- Cyber law and policy professionals
- Government and defense cybersecurity personnel

Here are some industries that could benefit from joining this course, including but not limited to:

- Banking and Financial Services
- Telecommunications
- Healthcare and Pharmaceuticals
- Government and Public Sector
- Defense and Military
- Energy and Utilities
- Technology and IT Services
- Manufacturing and Industrial Control Systems
- Retail and E-Commerce
- Transportation and Logistics
- Education and Research Institutions
- Media and Entertainment
- Insurance
- Real Estate and Property Management
- Consulting and Advisory Services
- Cybersecurity and Risk Management Firms
- Aerospace and Aviation
- Hospitality and Travel
- Supply Chain and Procurement
- Cryptocurrency and Blockchain Industry

Skill-Lyft

*Empowering Skills, Elevating Careers*

Skill Lyft (M) Sdn. Bhd. is a registered Training Provider under Human Resource Development Corporation (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

*All information is correct at the time of publication. Published March 2025.*

Skill-Lyft

| | |
|---|---|
| **Early Bird Registration**<br>3 Mar – 11 Apr 2025 | RM3,499 / pax |
| **Regular Registration**<br>12 Apr – 16 May 2025 | RM4,099 / pax |
| **Group Registration**<br>12 Apr – 16 May 2025 | RM3,699 / pax |

* Above fees are per delegate & inclusive of 8% SST.
* Group registration is only for 3 delegates and above.
* Maximum HRD Corp claimable amount is RM1,750/pax/day for Employer-Specific Course.

# 2025 Workshop Series Registration Form

# 2-DAY COURSE

## AI-Powered Cybersecurity: Defense and Offense

*26 – 27 May 2025*

*The Majestic Hotel Kuala Lumpur, Autograph Collection*

HRD Corp Claimable Course (SBL-KHAS) Scheme
**Employer-Specific Course, No. : 10001532271**

☐ **Please tick (√) the box if you are applying for HRD Corp grant.**

## ORGANISATION INFORMATION

Name

Address

Postcode

Email

Phone

## DELEGATE INFORMATION

Please tick (√) below box if you have more than 3 delegates.
☐ Yes, please refer to the additional copy of this registration form.

Name
Designation
Department
Email
Mobile No.
Dietary Concerns: Vegetarian / Allergies

Name
Designation
Department
Email
Mobile No.
Dietary Concerns: Vegetarian / Allergies

Name
Designation
Department
Email
Mobile No.
Dietary Concerns: Vegetarian / Allergies

## FASTEST WAY TO REGISTER

1. Complete the Workshop Series Registration Form
2. Kindly email it to us at registration@skill-lyft.com

## PAYMENT METHOD

**Online Banking / Bank Transfer**

*Hong Leong Islamic Bank Berhad*

| | |
|---|---|
| Bank Address | : No. 5, Jalan P16, Presint 16, 62150 Putrajaya, Wilayah Persekutuan Putrajaya, MALAYSIA |
| Account Name | : Skill Lyft (M) Sdn. Bhd. |
| Account No. | : 363-01-08956-6 |
| Swift Code / BIC | : HLIBMYKL |

## TERMS & CONDITIONS

**1. Replacement Policy**
Delegates may request a replacement at no additional cost, provided Skill-Lyft is notified at least three (3) working days before the event.

**2. Cancellation Policy**
All cancellations must be submitted in writing via email to Skill-Lyft. The following charges apply based on the time of cancellation:
- More than 15 working days before the event: Full refund with no charges.
- 8 to 14 working days before the event: 50% of the registration fee will be charged.
- Within 7 working days before the event: 100% of the registration fee will be charged.

**3. No-Show Policy**
Delegates who do not attend the event will be charged the full registration fee.

**4. Skill-Lyft's Rights**
Skill-Lyft reserves the right to cancel or reschedule events. Delegates will be informed promptly of any changes. Please note that Skill-Lyft will not be responsible for airfare, hotel accommodations, or other travel-related expenses incurred by delegates.

**5. HRD Corp Grant**
If the approved HRD Corp grant amount is less than the course fee, the company will be invoiced for the difference.

**6. Invoice & Payment Policy**
All invoices must be settled within 14 days of the invoice date or at least one (1) working day before the event, whichever comes first. Delegates will not be allowed entry to the course if payment has not been received.

**7. Data Privacy**
Skill-Lyft (M) Sdn Bhd acts as the data controller for this information. Your details will be stored in our database and used to fulfill our legitimate interests in event administration.

## AUTHORISATION & INVOICE

Signatory must be authorised to sign on behalf of the organisation.

Name
Designation
Email
Phone
Signature

*By signing, I hereby acknowledge that I have thoroughly read and fully understand the Terms & Conditions stated in this registration form.*

Invoice should be directed to:

Name
Designation
Email
Phone

** Skill Lyft (M) Sdn Bhd acts as the data controller for this information.*
*Your details will be stored in our database and will be used to fulfill our legitimate interests in event administration.*

Skill-Lyft
**FOR OFFICE USE**

Course Coordinator
Course Code: WS2512
Date Received