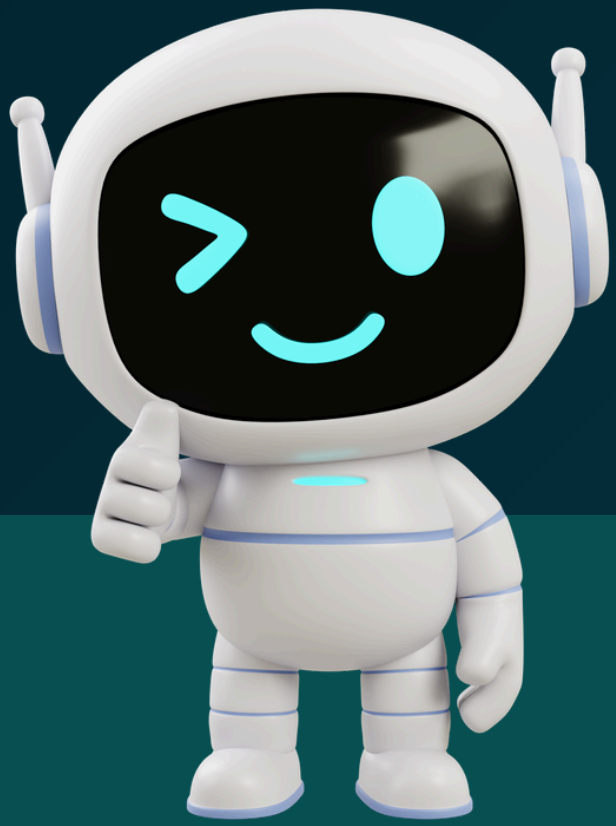
Programme ID: 10001636560

Leveraging AI and Machine Learning in CYBERSECURITY

Learn how to apply AI and machine learning techniques to enhance cybersecurity measures and protect your organisation from threats.



7th JULY

9am-5pm

Concorde Hotel, Kuala Lumpur

Early Bird: RM1,660

Normal Fee: RM1,960

**including 8% SST*

Symphony Digest

MyCoID: 870359P

HRDCORP CLAIMABLE

Alisa: 016-606 2816 | alisa@symphonydigest.com
Farrah: 018-948 2800 | farrah@symphonydigest.com

symphonydigest.com
doshu.com.my

Leveraging AI and Machine Learning in Cybersecurity

Module 1: Introduction to AI & ML in Banking Cybersecurity

- The evolving threat landscape in Malaysian financial institutions
- How AI and ML strengthen cybersecurity defence layers
- Threat types where AI is most effective: phishing, fraud, malware, insider threats, reconnaissance
- Use Case: AI-enabled phishing detection and email classification
- Use Case: Identifying anomalous login and transaction patterns
- Hands-on: Analyse sample logs using GenAI to extract Indicators of Compromise

Module 2: Machine Learning Techniques for Threat Detection

- Key ML approaches: supervised models, anomaly detection, clustering, behavioural analytics
- Use Case: Transaction anomaly detection for retail/mobile banking fraud
- Use Case: Detecting unusual network behaviour via clustering or baseline comparison
- Use Case: Malware classification using behavioural ML signals
- Hands-on: Interpret ML intrusion detection outputs and classify alerts

Module 3: AI for SOC (Security Operations Centre) Efficiency

- How GenAI improves SOC productivity: alert triage, event summarisation, threat intel extraction
- Use Case: Using AI to correlate multi-source alerts
- Use Case: Summarising SIEM alerts into prioritised review notes
- Handson: Build an "AI SOC Analyst Assistant" to summarise alerts and recommend actions

Module 4: Cyber Threat Intelligence (CTI) with AI

- Leveraging AI to interpret CTI feeds, advisories, and attack patterns
- Use Case: Extracting relevant threat actors and vulnerabilities from CTI sources
- Use Case: AI-assisted monitoring of global vulnerabilities relevant to banking
- Hands-on: Create a CTI Summary Generator and map threats to MITRE ATT&CK

Module 5: Using AI for Incident Response & Forensics Support

- How AI accelerates investigation cycles through log analysis and timeline reconstruction
- Use Case: AI-assisted interpretation of firewall and authentication logs
- Use Case: Drafting incident summaries and forensics notes
- Hands-on: Generate a preliminary investigation note from raw logs with GenAI

Module 6: Cybersecurity Governance, Risks & Safe Use of AI

- Responsible AI usage aligned with BNM RMiT, internal security policies, and data protection requirements
- Risks: hallucination, model poisoning, data leakage, privacy exposure
- Use Case: Evaluating high/medium/low risk for AI-driven cybersecurity applications
- Activity: Develop a Secure AI Usage Checklist and draft a Cyber AI SOP

Nur Alisa
alisa@symphonydigeest.com | 016-6062816

Farrah Sureina
farrah@symphonydigest.com | 018-948 2800

Leveraging AI and Machine Learning in Cybersecurity

TRAINER'S PROFILE

The Trainer is the Lead Trainer and Data Science Lead where he designs and delivers interactive corporate training programs in AI, data science, and machine learning. He also spearheads the development of AI-driven frameworks and prototypes, enabling organizations to integrate emerging technologies seamlessly into their operations. With a versatile background across academia, entrepreneurship, and industry, he has previously lectured at UniRazak and served as a vocational trainer at New Era Institute of Vocational and Continuous Education (Kajang). He has also founded and led software development teams in fintech and edtech startups, drawing on his deep expertise in marketing, software engineering, and artificial intelligence to craft impactful, scalable solutions. He brings extensive corporate training experience across sectors such as manufacturing, fintech, and financial services. He has led specialized upskilling programs for manufacturing giants, empowered fintech teams with AI automation and fraud detection tools, and conducted strategic workshops on data and AI adoption for banks and financial institutions. His cross industry exposure also includes roles in robotics and mechatronics engineering within the oil & gas and manufacturing sectors, including at Flextronics. As a consultant and coach, he has helped organizations such as Beyond Insights, Plus Minus Zero, and Watson-Marlow leverage data and AI to drive business transformation.

REGISTRATION DETAILS

PARTICIPANT DETAILS

Name:

Position:

Department:

Contact Number:

Email:

Name:

Position:

Department:

Contact Number:

Email:

ADMIN DETAILS

Name:

Position:

Department:

Company:

Contact Number:

Email:

Address:

Payment Method: ☐ Direct Payment ☐ Claim HRD

Notes:

- *Cancellations made less than 14 days before the training date or non-attendance on the day of training are non-refundable. Substitution is allowed.*
- *Once registration is confirmed, the client is fully liable for the course fee, regardless of whether payment is made directly or through the HRDC grant, and even if participants do not attend the training.*
- *Clients who opt for direct payment must ensure full payment is made before the training date.*
- *HRDC grant applications must be submitted and approved before the training day. The maximum claimable amount is RM1,750 per participant per day. Any shortfall between the approved grant and the course fee must be topped up by the client.*
- *Should the number of confirmed participants be too low to ensure a meaningful learning experience, Symphony reserves the right to postpone or cancel the training.*

Nur Alisa
alisa@symphonydigeest.com | 016-6062816

Farrah Sureina
farrah@symphonydigest.com | 018-948 2800