Asian Institute of Insurance
(Formerly known as Malaysian Insurance Institute)

DELIVERY PARTNER:
CYBERARMOUR

Be Cyber Ready!

FSF
FUTURE SKILLS FRAMEWORK MALAYSIA

Cybersecurity Simulation Workshop

Step into the frontline of cyber defense with a high-stakes, hands-on war room simulation led by top cybersecurity experts.

REGISTERED HRD CORP TRAINING PROVIDER

HRD CORP CLAIMABLE

Training Programme no: 10001536971

16 July 2025
Level 6, Asian Institute of Insurance, AICB Building, KL

3 Industry Simulation War Room Choices

Financial Services
Banking, Insurance, Capital Market Players, Fintech

Public Sector
GLC, Government Bodies, Regulators

Healthcare
Hospitals, Healthcare Service Providers and Vendors

Expert facilitators

Danny Kim
Co-Founder of FullArmor Corp & CEO of Cyberarmour

Jeremiah Abraham
Cybersecurity Consultant at CyberArmour

Jenko Hwong
Head of Products & Threat Research, WideField Security

(Virtual/Video Address)

PROGRAMME OVERVIEW

The Cyber Security Act 2024, Securities Commission's Guidelines For Technology Risk Management (GTRM) and Bank Negara's RMiT all call for enhanced Cybersecurity Awareness, Preparedness and Governance Training and Upskilling of Board Members and Senior Management teams.

This "Be Cyber Ready" programme is an immersive experience where Participants will **experience a live cyber breach scenario**, assume industry-specific roles, make decisions affecting the outcome, conduct forensic analysis, and receive AI-driven performance feedback.

Critical insights on Zero Trust strategies, Attack Surface Removal, Cyber Threat Detection using AI and Cyber Attack Chain strategies would be introduced in this programme for participants to learn, experience and learn to mobilise the require defence.

PROGRAMME OBJECTIVE

Participants will learn best practices for cyber defense, improve their crisis leadership skills, and develop a stronger organisational security posture. By the end of the simulation, attendees will be better equipped to defend against cyber threats, respond to incidents effectively, and lead their organisations through complex cybersecurity challenges. They will have hands on experience in the following :

- **Understanding and comprehension of initial Threat Intelligence and System Logs**
- **Analysing events, Incident escalation and Critical Decision making with accountability for consequences**
- **Developing a Crisis Response Plan, Containment strategy and Damage Mitigation**
- **Manage key stakeholders : Regulatory Bodies, Customers, Public and Media**
- **Conduct Forensic Analysis and Root Cause Investigations**

PROGRAMME CONTENT

Group 1

Time **: 8:30am – 1:00pm**
CPD Hour : 4 Hours

Each war room will run concurrently, and participants would pre-book their selected **2 war rooms** with a limited **capacity of 12 pax per room**.

3 Industry Simulation War Room Choices:

Financial Services
Banking, Insurance, Capital Market Players, Fintech

Public Sector
GLC, Government Bodies, Regulators

Healthcare
Hospitals, Healthcare Service Providers and Vendors

Time	Session
8:30 am	Registration
9:00 am	Opening Keynote: The Global Landscape of Cybersecurity
Cyber War Room Session 1: Breakout to Participant Selected War Room	
9:45 am	**1. Scenario Introductions & Threat Intel** • Introduction to the real-world breach that matches their industry. • Hands-on Analysis and Interpretation of the crisis
9:55 am	**2. Incident Escalation & Decision Making with AI Branching Progression** • Hands on Analysis on breach event • Group Discussion and Response: Critical decisions, Adaptive Response , Incident Escalation and Choices
10:20 am	**3. Crisis Management & Containment Strategies** • Develop and execute a response • Handling unexpected developments

PROGRAMME CONTENT

Group 1

Time	Session
10:40 am	**4. Forensic Analysis & Root Cause Investigation** • Teams analyse logs, trace attack vectors, and determine how the breach occurred
10:55 am	**5. AI Performance Review & Expert Insights** • AI-generated analysis on team performance based on: • Threat identification • Decision effectiveness • Incident containment speed • Forensic accuracy Feedback and Learning capture.
Cyber War Room Session 2: Breakout to Participant Selected War Room	
11:15 am	**1. Scenario Introductions & Threat Intel** **2. Incident Escalation & Decision Making with AI Branching Progression** **3. Crisis Management & Containment Strategies** **4. Forensic Analysis & Root Cause Investigation** **5. AI Performance Review & Expert Insights**
12:45 pm	Closing & Reflections
1.00 pm	Networking Lunch with Group 2 Participants
2:00 pm	End for Group 1

PROGRAMME CONTENT

Group 2

Time **: 12:30pm – 6:00pm**
CPD Hour : 4 Hours

Each war room will run concurrently, and participants would pre-book their selected **2 war rooms** with a limited **capacity of 12 pax per room**.

3 Industry Simulation War Room Choices:

Financial Services
Banking, Insurance, Capital Market Players, Fintech

Public Sector
GLC, Government Bodies, Regulators

Healthcare
Hospitals, Healthcare Service Providers and Vendors

Time	Session
12:30 pm	Registration
1:00 pm	Networking Lunch with Group 1 Participants
2:00 pm	Opening Keynote: The Global Landscape of Cybersecurity
Cyber War Room Session 1: Breakout to Participant Selected War Room	
2:45 pm	**1. Scenario Introductions & Threat Intel** • Introduction to the real-world breach that matches their industry. • Hands-on Analysis and Interpretation of the crisis
2:55 pm	**2. Incident Escalation & Decision Making with AI Branching Progression** • Hands on Analysis on breach event • Group Discussion and Response: Critical decisions, Adaptive Response , Incident Escalation and Choices
3:20 pm	**3. Crisis Management & Containment Strategies** • Develop and execute a response • Handling unexpected developments

PROGRAMME CONTENT

Group 2

Time	Session
3:40 pm	**4. Forensic Analysis & Root Cause Investigation** • Teams analyse logs, trace attack vectors, and determine how the breach occurred
3:55 pm	**5. AI Performance Review & Expert Insights** • AI-generated analysis on team performance based on: • Threat identification • Decision effectiveness • Incident containment speed • Forensic accuracy Feedback and Learning capture.
Cyber War Room Session 2: Breakout to Participant Selected War Room	
4:15 pm	**1. Scenario Introductions & Threat Intel** **2. Incident Escalation & Decision Making with AI Branching Progression** **3. Crisis Management & Containment Strategies** **4. Forensic Analysis & Root Cause Investigation** **5. AI Performance Review & Expert Insights**
5:45 pm	Closing & Reflections
6:00 pm	End for Group 2

FACILITATOR PROFILE

DANNY KIM

Co-Founder of FullArmor Corp & CEO of Cyberarmour

Danny Kim is a technology leader and innovator with over 30 years of experience in the enterprise and cyber security industry. Danny is a recognised industry expert on Enterprise Security, Active Directory, Datacenter Automation, and Cloud Computing.

As the Founder and CTO of FullArmor Corp, he has been at the forefront of developing security, compliance, and access management products. He pioneered FullArmor's strategy to partner with leading tech firms like Microsoft, Citrix, and F5, successfully scaling products to market. FullArmor Corp. has been a Microsoft Gold Certified Partner for over 20 years and has won several awards for its products and services.

Danny has taken on a new venture in South East Asia as the CEO of CyberArmour based out of Malaysia, with the vision to empower and build communities of Cybersecurity Professionals, STEAM based learning communities and Entrepreneurs in the region.

Danny is also deeply invested in educational initiatives, leading programs that inspire students in STEAM fields with hands-on learning experiences. He and his team led the first ever high school team to win the prestigious Shell XPRIZE Ocean Discovery competition. As the CEO of Quest Institute, he spearheaded various STEAM related educational programs including a unique initiative partnering with NASA and other organizations to launch student-designed experiments to the International Space Station. Danny Kim has also been a speaker and mentor at various events and programs for young entrepreneurs and innovators.

As the VP/Director AMSE and R&D, Valley Christian Schools, he leads the Applied Math Science and Engineering (AMSE) STEM program at Valley Christian Schools, contributing to future STEM growth and innovation.

Danny graduated from Cornell University with a degree in computer science and electrical engineering. He is a visionary leader and a role model who has demonstrated excellence and integrity in his work and life. He is a faith-driven entrepreneur who believes that God has a purpose for his life and business and has made significant contributions to the fields of technology, education, and space exploration.

FACILITATOR PROFILE

JEREMIAH ABRAHAM
Cybersecurity Consultant at CyberArmour

With 12 years of extensive experience in the tertiary education sector, Jeremiah is a highly skilled IT professional specializing in IT and Cyber Security, delivering large-scale & technical IT infrastructure support & solutions.

Currently, Jeremiah head the Cybersecurity Solutions business unit at Cyberarmour, a boutique cybersecurity company focused on cutting-edge threat surface reduction/removal and stealth technology for servers. His role involves leveraging his deep understanding of IT security integration, encompassing Microsoft Security, Norton, Sophos, ScanNow, Zscaler, Cisco, Fortinet, Windows Active Directory & Group Policy, to drive the development and delivery of Cyberarmour's specialized solutions.

Jeremiah also extends his expertise as a consultant to CTOs and CISOs on Enterprise IT infrastructure, including cloud services & virtualization such as Citrix, VMWare, Serverpark VDI, and SCCM. His commitment to fostering cybersecurity knowledge is further demonstrated through his active engagement with the Cyberarmour Academy. In this capacity, he contributes to teaching and learning initiatives aimed at spreading cybersecurity awareness and best practices among working adults and even school children.

FACILITATOR PROFILE

JENKO HWONG
Head of Products & Threat Research, WideField Security
(Virtual/Video Address)

Jenko Hwong is a distinguished advisor with extensive expertise in cybersecurity, threat intelligence, cloud security, product management, and technology innovation.

With a career spanning over two decades, he has been instrumental in developing cutting-edge cybersecurity solutions and leading teams across various high-tech organizations.

Jenko is currently the Products & Threat Research Lead at Widefield Security and formerly Principal Security Researcher on Netskope's Threat Research Labs, analyzing emerging cloud threats. He has over 20 years of experience in research, product management, and engineering at companies such as Cisco and TIBCO, as well as security startups in markets such as vulnerability scanning, anti-virus/anti-spam appliances, penetration-testing, threat intelligence, and Active Directory security. He has successfully founded a startup in the enterprise monitoring market and has led production deployments at enterprise customers including Walmart, Microsoft, Lucent, Chase, and European banks.

One of his passion projects was in mentoring and supporting the designing and deployment of a hardware/software platform for STEM experiments on the ISS designed by junior high students.

Jenko holds a BS in computer systems engineering from Stanford University.

TARGET AUDIENCE

- Business Leaders, Senior Management, Board Members, Chief Officers of various functions and Head of Departments.
- Any person who wish to experience the hands on learning of a cyber incident and response plan.

PROGRAMME FEE

	Aii Member	Non-Member
Early Bird Fee *(Register before: 2 June 2025)*	RM 2,160	RM 2,484
Normal Fee *(Registration closing: 2 July 2025)*	RM 2,484	RM 2,808

The above fee included SST.

ALIGNMENT TO THE FUTURE SKILLS FRAMEWORK

39 Prime Skills
13 Power Skills
Proficiency Level: Intermediate

Skills Developed by Attending this Programme

Prime Skills

Customer Experience Management	1. Customer Experience Design 2. Customer Relationship Management
Branding and Communications	3. Public Relations Management
Digital & Data Integration	4. Artificial Intelligence (AI) Management 5. Big Data Analytics 6. Data Collection and Analytics 7. Data Governance 8. Data Protection 9. Data Storytelling and Visualisation 10. Emerging Technology Synthesis 11. Enterprise Architecture 12. Infrastructure Development 13. Penetration Testing 14. Security Architecture 15. Security Monitoring 16. Threat Intelligence and Monitoring 17. Troubleshooting
Growth & Partnerships	18. Business Planning and Needs Analysis 19. Continuous Improvement and Process Re-Engineering 20. Disruption Management 21. Global Perspectives 22. Project Management 23. Scenario Planning and Analysis
People Management & Development	24. Organisational Design
Risk Management, Governance & Regulatory Compliance	25. Artificial Intelligence, Ethics and System Governance 26. Business Continuity Management 27. Business Continuity Planning 28. Crisis and Disaster Recovery Management 29. Enterprise Risk Management 30. Internal Governance 31. Operational Risk Management 32. IT Audit 33. Monitoring and Surveillance 34. Policy Implementation and Revision 35. Regulatory Compliance 36. Risk Governance 37. Risk Management 38. Risk Modelling and Validation 39. Technology Risk Management

Power Skills

Innovation & Delivery	1. Adaptability and Resiliency 2. Business Acumen 3. Change Management 4. Critical Thinking 5. Digital Fluency 6. Innovative Thinking 7. Learning Agility 8. Problem Solving
Social Intelligence	9. Collaboration 10. Communication 11. Conflict Management 12. Empathy 13. Influencing and Negotiation

REGISTER NOW!

Choose your option by scanning the QR code:
1) Group (Group 1 – Morning; Group 2 – Afternoon)
2) Industry Simulation War Room Options

Asian Institute of Insurance
197701004772 (35445-H),
Level 6, Bangunan AICB,
No. 10 Jalan Dato' Onn,
50480 Kuala Lumpur, Malaysia

For further information, please contact:
Email: sales@aiiasia.org