# AiSP

**News & Update**

- SVRP
- AiSP Cyber Wellness
- Special Interest Groups
- The Cybersecurity Awards
- Ladies in Cyber
- Digital For Life
- Corporate Partner Event
- Upcoming Events

**Contributed Contents**

- AI SIG: Artificial Intelligence 101
- CISO SIG: Introduction to CISO
- CPP: OPSWAT C1D2 Certification, Vulnerabilities, and Expert Insights from OPSWAT
- SVRP 2024 Gold Winner, Jason Kek Jun Kai (NP)

Professional Development
Membership

# NEWS & UPDATE

## Continued Collaboration

AiSP would like to thank Blackpanda, Govtech and ITSec and M.Tech for their continued support in developing the cybersecurity landscape:

# News & Update

**STANDCON 2025 on 7 March**

AiSP was invited to STANDCON 2025 on 7 March and AiSP Secretary, Ms Soffenny Yap represented AiSP and received the certificate of appreciation from n0h4ts as a premier sponsor for the event.



**AiSP Annual General Meeting 2025 on 19 March**

AiSP 17th Annual General Meeting was held on 19 March at Justco @ Marina Square. AiSP would like to thank Mr Wong Onn Chee for his contributions and support for the past few years as he stepped down from the main EXCO.

AiSP would like to welcome Mr Nyan Tun Zaw to be part of our main EXCO.
The Main EXCO for 2025/2026 Term are:
President: Mr Tony Low
Vice-President: Mr Andre Shori, Ms Sherin Lee & Mr Breyvan Tan
Secretary: Ms Soffenny Yap
Assistant Secretary: Mr Huynh Thien Tam
Treasurer: Mr Boris Choo
Assistant Treasurer: Mr Samson Yeow
Committee Member: Mr Alex Lim, Mr John Lim, Mr Dennis Chan & Mr Nyan Tun Zaw
Nominated Member representing Cyber Security Agency of Singapore (CSA): Mr Wong Choon Bong
Nominated Member representing GovTech Singapore: Mr Mathew Soon
Nominated Member representing IMDA: Dr Ong Chen Hui
Nominated Member representing Singapore Computer Society: Dr Tan Mei Hui
Nominated Member representing Immediate Past President: Mr Johnny Kho

back to top

Nominated Member representing Individual:  Prof Steven Wong

We looked forward to having the Main EXCO for 2025/2026 to bring AiSP to the next level.



**Long Service Awards for 5-Year, 10-Year and 15-Year**

AiSP would like to appreciate and thank Ms Karen Ong for her 5 years as AiSP Secretariat, Mr Wally Lee for 10 years, and Mr Alex Lim for 15 years of dedicated service and contributions to AiSP.

# Student Volunteer Recognition Programme (SVRP)

**Sharing with Admiralty Secondary School on 11 March**

On 11 March, AiSP EXCO Member, Vivek Balachandran conducted a sharing for more than 35 Secondary 4-5 students from Admiralty Secondary School, where he shared about his journey in Cybersecurity and inspired students to take up Cybersecurity as a career.



back to top

Page 4 of 50
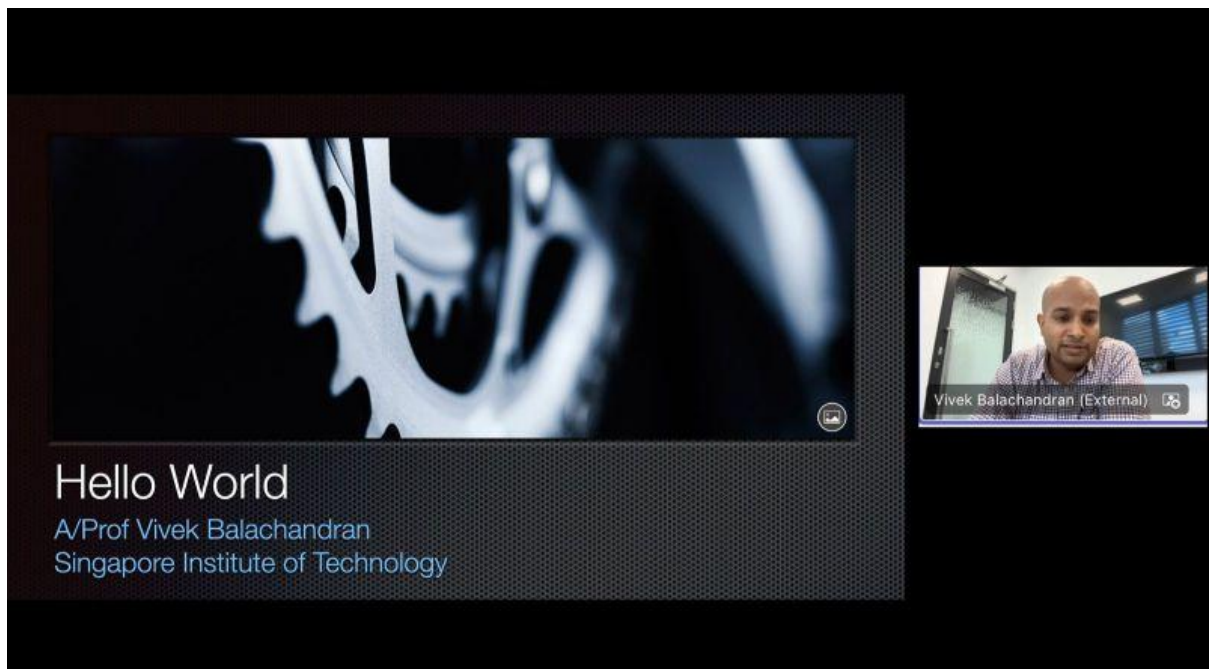
## AiSP Hackathon on 9-11 April

### AiSP Hackathon



### 🚀 Cybersecurity & AI Hackathon 2025 – Are You Ready to Hack the Future? 🚀

The inaugural **AiSP Cybersecurity & AI Hackathon** is here! If you're a **student, cybersecurity enthusiast, AI innovator, or tech professional**, this is your chance to:

- ✅ **Tackle real-world cybersecurity & AI challenges** provided by industry partners
- ✅ **Work with mentors and industry experts** to develop cutting-edge solutions
- ✅ **Gain hands-on experience** in ethical hacking, AI security, and threat intelligence
- ✅ **Compete for exciting prizes** (Over $1,500 in shopping vouchers!)
- ✅ **Earn a certificate of participation** to showcase your skills

### 🗓 Event Details

**Date:** 9 - 11 April 2025
**Time:** Day 1 & 2 (9AM – 5PM), Day 3 (2:30PM – 7PM)
**Venue:** Singapore Polytechnic
**Limited slots available – Secure your spot now!** 👉 Register Here

*Please note that the Hackathon is open for Team of 3. Participants will need to form a team of 3 members and register via the form.

### 💡 What You'll Be Working On – Possible Problem Statements

Participants will tackle real-world challenges in **Cybersecurity & AI**, which may include:

back to top

## 🔐 Cybersecurity Challenges:

- **AI-Driven Phishing Detection** – Build an **AI model** to identify and prevent phishing attacks.
- **Threat Intelligence Dashboard** – Create a **real-time** cyber threat monitoring system.
- **Security for Small Businesses** – Develop a **lightweight, AI-powered** cybersecurity solution.

## 🤖 AI & Data Privacy Issues:

- **AI for Data Breach Detection** – Detect and mitigate potential data leaks before they happen.
- **Securing AI Models** – Prevent adversarial attacks on AI-driven systems.
- **Automating Endpoint Security** – Use AI to monitor and secure connected devices.

## 🏛 Industry-Specific Problems:

- **Financial Fraud Detection** – Strengthen fraud prevention systems in banking.
- **Healthcare Data Security** – Ensure compliance while protecting sensitive medical records.
- **Fake News & Misinformation Detection** – Develop AI-powered fact-checking tools.

## 🚀 Integrated Training & Hackathon Program

This **3-day immersive experience** combines hands-on training, innovation, and competition:

### ◇ Day 1 – Training & Brainstorming

🕘 **9:00 AM – 10:30 AM:** Opening Ceremony & Keynote Address
🕥 **10:30 AM – 12:30 PM: Training 1** – Fundamentals of Ethical Hacking & Penetration Testing
🍽 **12:30 PM – 1:30 PM:** Lunch Break
🕜 **1:30 PM – 3:30 PM: Training 2** – Introduction to AI & Machine Learning for Cybersecurity
🕞 **3:30 PM – 5:00 PM:** Team Formation & Brainstorming

### ◇ Day 2 – Training & Initial Prototyping

🕘 **9:00 AM – 10:30 AM: Training 3** – Secure AI Development & Adversarial Machine Learning
🕥 **10:30 AM – 12:30 PM: Training 4** – Securing Cloud Infrastructure & Networks
🍽 **12:30 PM – 1:30 PM:** Lunch Break
🕜 **1:30 PM – 3:00 PM: Hands-on Workshop** – Rapid Prototyping with Open-Source

back to top

Security Tools

🕒 **3:00 PM – 5:00 PM:** Idea Refinement & Early Prototyping

◇ **Day 3 – Hackathon & Judging**

🕑 **2:30 PM – 4:30 PM: Final Prototyping & Testing**
🕟 **4:30 PM – 6:00 PM: Final Presentations & Judging**
🎉 **6:00 PM – 7:00 PM:** Awards, Closing Ceremony, Dinner & Networking

*Participants can work on their projects in the morning of Day 3 at their own pace and venue of choice.*

🏆 **Prizes**

🥇 **First Prize:** $900 Shopping Voucher
🥈 **Second Prize:** $600 Shopping Voucher
🥉 **Third Prize:** $300 Shopping Voucher

🎯 **Who Should Join?**

◆ **Students & Aspiring Cybersecurity Professionals** – Learn from experts and gain practical experience.
◆ **AI & Tech Enthusiasts** – Apply AI in cybersecurity to solve real-world problems.
◆ **Innovators & Problem-Solvers** – Compete in a high-stakes environment and push the boundaries of tech.

📩 **Register Now!**

👉 **Secure Your Spot** (Limited Slots Available!)

For inquiries, contact us at **secretariat@aisp.sg** or via Telegram.

**Join us in shaping the future of Cybersecurity & AI – See you at the hackathon!** 🚀

**Elevating Cybersecurity Education Through Unprecedented Collaborations**

In a pioneering initiative, EC-Council and Wissen have forged a collaboration with AiSP. This collaboration includes a sponsorship of 500 EC-Council Cyber Essentials certification vouchers. These vouchers aim to empower Polytechnic and Institute of Technical Education (ITE) students pursuing cybersecurity programs, enabling them to attain their inaugural industry certificate and commence their journey with EC-Council Essential certificates (NDE, EHE, DFE), thereby initiating their cybersecurity credentialing process.

Visit (https://wissen-intl.com/essential500/) and register to start your cybersecurity credentialing journey! Terms & Conditions apply.

**About the EC-Council Cyber Essentials Certification**
EC-Council's Essentials Series is the first MOOC certification course series covering essential skills in network defense, ethical hacking, and digital forensics. The Network Defense Essentials (N|DE), Ethical Hacking Essentials (E|HE), and Digital Forensics Essentials (D|FE) are foundational programs that help students and early career professionals choose their area of competency or select a specific interest in cybersecurity. The Essentials Series was designed to give students the foundation on which to build and develop the essential skills for tomorrow's careers in cybersecurity. These programs educate learners in a range of techniques across industry verticals, such as securing networks, mitigating cyber risks, conducting forensic investigations, and more.

# AiSP Cyber Wellness Programme

Organised by:

Supported by:

In Support of:

The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."

Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website (https://www.aisp.sg/aispcyberwellness) to get updates on the latest Cyber tips, Cyber news, activities, quiz and game happenings related to Cyber. Scan the QR Code to find out more.

**Scan here for some tips on how to stay safe online and protect yourself from scams**

**Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship & Ethics.**

**Have the knowledge and think you are safe? Challenge yourself and participate in our monthly quiz and stand to win attractive prizes. Scan now to take part.**

**Scan here if you are looking for activities / events to participate in for knowledge exchange / networking / get to know more people / stay protected & helping others.**

**Want to know more about Information Security? Scan here for more video content.**

**To find out more about the Digital for Life movement and how you can contribute, scan here.**

Contact AiSP Secretariat at secretariat@aisp.sg to find out more on how you can be involved or if you have any queries.

Click here to find out more!

back to top

# Special Interest Groups

AiSP has set up seven **Special Interest Groups (SIGs)** for active AiSP members to advance their knowledge and contribute to the ecosystem are:

- Artificial Intelligence
- CISO
- Cloud Security
- Data and Privacy
- DevSecOps
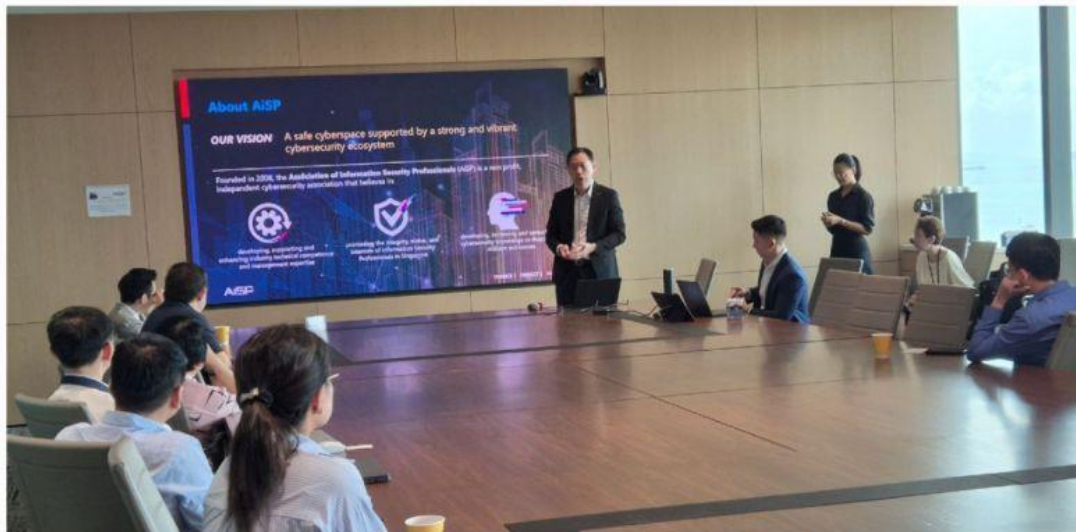- Legal Investigative Technology Experts (LITE)
- Quantum Security

We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together. If you are keen to be part of a SIG, please contact secretariat@aisp.sg

## Data & Privacy SIG Meetup on 17 March

AiSP held our Data & Privacy SIG Meetup, "Managing Third-Party Vendor Risks: Are You Prepared?" with 20 attendees at our Corporate Partner, Rajah & Tann Cybersecurity.

Thank you Onn Chee W. and Glen Chiang for speaking at the session.

## AiSP LITE Conference 2025 on 8 April

**AiSP LITE Conference 2025**

# Digital Forensics Alchemy: Transforming Data into Evidence through the Art of Data Synthesis

Issac Newton believed in the possibility of transforming knowledge (and materials) to unlock hidden truths—an idea that mirrors the way digital forensic experts extract and synthesize evidence from various data sources to reveal hidden facts and patterns.

This presentation introduces the concept of Digital Forensics Alchemy, a process where investigators combine multiple data sources and techniques to uncover hidden truths and create a comprehensive narrative from digital evidence. In the modern world of digital forensics, relying on a single data source often leaves gaps, so a multi-source, synthesized approach is essential for accurate, complete analysis.

**Mr Church Christopher**
Senior Digital Forensic Specialist
Interpol

# Expert Panel:
# Digital Investigations in the Modern Era

**Daniel Wang**
LITE SIG EXCO Lead
AiSP
Moderator

**Pradeep Nair**
Local Principal
Baker & McKenzie.Wong & Leow
Panellist

**Sequeena Ong**
Senior Solutions
Consultant (APAC), Nuix
Panellist

**Tuan Liang Lim**
Director (Digital & Information Forensics)
Centre of Expertise
Home Team Science & Technology Agency.
Panellist

back to top

# Blockchain Tools in Legal Investigations: Enhancing Asset Tracing

Blockchain technology has become a crucial tool in legal investigations, particularly for asset tracing, fraud detection, and compliance enforcement. This presentation explores how blockchain tools aid law enforcement, legal professionals, and forensic investigators in uncovering illicit financial activities. The discussion will begin with an overview of blockchain's fundamental characteristics, such as immutability, transparency, and decentralization, and how these features support legal investigations. Real-world case studies will illustrate how these tools are used to track illicit transactions and recover stolen assets. Additionally, the presentation will address challenges such as anonymity-enhancing technologies (e.g., privacy coins, mixers), and the legal admissibility of blockchain evidence.

**Ms Lin Shumin**
Director
Drew & Napier

**Ms Arushee Bhatnagar**
Senior Associate
Drew & Napier

# Representing and Coordinating Digital Investigation in Smart City Infrastructure

Digital investigations are often fraught with complexities, particularly on modern platforms such as smart city infrastructure (SCI), where threats, cybercrime and digital evidence may need to be clearly defined. In such complex environments, the ability to share evidence and work collaboratively while consistently understanding the environment is essential for investigators. This presentation showcases the Smart City Ontological Paradigm Expression (SCOPE). SCOPE is an extended ontology from the Unified Cyber Ontology (UCO) and Cyber-investigation Analysis Standard Expression (CASE) that enables digital forensic investigators to handle future cybercrime and incidents occurring within SCI. It aims to support coordinated cyber investigations and tool interoperability for smart city cybercrime/attacks. We showcase how SCOPE could present complex data such as SCI-specific threats, cybercrime, investigation data and incident handling workflows via an incident scenario modelled after publicly reported real-world incidents attributed to Advanced Persistent Threat (APT) groups.

**Dr. Tok Yee Ching**
EXCO Member &
LITE SIG Member
AiSP

Register here: https://www.eventbrite.sg/e/aisp-lite-conference-tickets-1217349066829?aff=oddtdtcreator

# The Cybersecurity Awards

THE CYBERSECURITY *Awards* 2025

The Cybersecurity Awards 2025 nominations has been **EXTENDED to 18 April 2025**! Don't miss this last chance to nominate the company/individual that you want to recognize for their contributions!

Professionals
1. Hall of Fame
2. Leader
3. Professional

Students
4. Students

Enterprises
5. MNC (Vendor)
6. MNC (End User)
7. SME (Vendor)
8. SME (End User)

Now in its eighth year, **The Cybersecurity Awards 2025** aims to recognize and celebrate exceptional contributions by individuals and organizations to the local and regional cybersecurity ecosystems. Organized by the Association of Information Security Professionals (AiSP), the Awards are supported by the Cyber Security Agency of Singapore and several professional and industry associations under the Singapore Cyber Security Inter Association, including the Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Chapter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)² Singapore Chapter, Operational Technology Information Sharing and Analysis Center (OT-ISAC), The Law Society of Singapore, Singapore Computer Society, and SGTech.

back to top

If you know individuals or organizations that have made a significant impact on the cybersecurity industry, now is the time to ensure they receive the recognition they deserve!
Please fill up the nomination form here by **18 April 2025**!

For any enquiries, please email thecybersecurityawards@aisp.sg

Nomination will end on **18 April 2025**. All submissions must reach the secretariat by **18 April 2025.**

For more details on the awards, visit our website here!

back to top

ORGANISED BY



SUPPORTING ASSOCIATIONS



GOLD SPONSORS



Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors for The Cybersecurity Awards 2025! Limited sponsorship packages are available.

back to top

# Ladies In Cyber

**2025 International Women's Day "To-Gather: Power of Women – Bright, Brave, Bold March on 8 March**

AiSP celebrated International Women's Day with National Trades Union Congress (NTUC) U Women and Family by participating in the TO-GATHER: POWER OF WOMEN – BRIGHT, BRAVE, BOLD March from Garden by the Bay to NTUC OMB on 8 March with 1000 participants in the March.

AiSP Ladies in Cyber EXCO Lead Ms Judy Saw also join SMS Sim Ann, NTUC Sec Gen Mr Ng Chee Meng, Sister Yeo Wan Ling & MOS Rahayu Mahzam in the flag off for the march together with our Ladies in Cyber Bear Mascot.

After the walk, the participants also participated in the Friendship Circles organised by SHE Singapore and also joined in the panel discussion on Empowering Women. Participants also get to enjoy the different booth activities that were setup after the march for all to come together to celebrate International Women's Day.

**AiSP Ladies in Cyber – Capture the Flag 2025 on 9 March**

On 9 March, AiSP organised the Ladies in Cyber Capture the Flag 2025 where more than 120 attendees signed up for the session as part of the International Women Day Celebrations. Through the practical exercises, the attendees had gain essentials skills in:
1. Penetration Testing: Learn how to identify and exploit system vulnerabilities.
2. Cryptography: Gain knowledge on encrypting and decrypting sensitive data.
3. Web Application Security: Explore common web vulnerabilities like SQL injection and cross-site scripting (XSS).
4. Forensics and Threat Analysis: Practice analyzing data to detect breaches and secure systems.

Thank you Cyber Leaders Nexus for conducting the session.



back to top

## AiSP Ladies in Cyber Symposium 2025 on 9 March

AiSP Ladies in Cyber Symposium 2025 with the theme "Accelerating Action: Empowering Women's Equality in Cybersecurity" was successfully held with more than 120 attendees on 9 March in celebration of the International Women Day. During the symposium, SMS Sim Ann presented the awards to the winners for Ladies In Cyber Capture the Flag 2025 held this morning.

Thank you panellists, SMS Sim Ann, Ms Judy Saw and Ms Lata Bavisi for the insightful panel discussion. Thank you speakers Ms Lynn Phua and Mr Kelvin Wu for the insightful sharing.

Thank you facilitators, Ms Veronica Chen, Ms Syabanun Zainudin, Ms Eileen Loh, Ms Chea Le Xin Andrea, Ms Tan Ci En Anne, Ms Linda Guo, Ms Neriza S., Ms Tay Sze Ying and Ms Jackie Low for volunteering your time to facilitate the Friendship Circles.

Thank you Ms Sim Ann, Senior Minister of State for Ministry of Foreign Affairs & Ministry of National Development for gracing the event. A huge thanks to everyone for joining us and our sponsors, ST Engineering and Wissen International, our supporting partners, Cyber Security Agency of Singapore (CSA), IMDA Digital for Life Movement, ISC2 Singapore Chapter, SHE Singapore, ISACA Singapore Chapter, Yayasan MENDAKI, National Youth Council Singapore, NTUC U PME, National Trades Union Congress (NTUC) U Women & Family, Singapore Indian Development Association (SINDA) and Tech Talent AssemBly (TTAB), who have contributed to making this symposium a memorable and impactful event.



back to top

## AiSP Learning Journey to Kuala Lumpur from 24 to 27 March

As part of Singapore and Malaysia 60th years bilateral relationship, AiSP organised the Ladies in Cyber Overseas Learning Journey to Kuala Lumpur from 24 March to 27 March, supported by Cyber Security Agency of Singapore (CSA), with 35 female students and working professionals participating in the activities.



## Learning Journey to Kualar Lumpur Day 1, 24 March

On 24 March, the students visited EC-Council in KL. Thank you, EC-Council, for hosting us.



back to top

## Learning Journey to Kualar Lumpur Day 2, 25 March

On 25 March, the students first visited the CyberSecurity Malaysia. Thank you CyberSecurity Malaysia for hosting us.



For the second visit, the students went to Dell Technologies. Thank you, Dell Technologies, for hosting us.

**Learning Journey to Kualar Lumpur Day 3, 26 March**

The students visited High Commission of Singapore in Kuala Lumpur on 26 March. Thank you, High Commission of Singapore, for hosting us.



The second visit on 26 March, the students went to Asia Pacific University of Technology and Innovation (APU / APIIT) in Kuala Lumpur. Thank you APU / APIIT for hosting us.

## Learning Journey to Kualar Lumpur Day 4, 27 March

On the last day of the learning journey, the students visited Ministry of Communications. Thank you Deputy Minister Ms Teo Nie Ching for hosting us.



The second visit on the last day, the students visited Blackberry Cybersecurity Centre of Excellence. Thank you, Blackberry, for hosting us.



back to top

**Beyond Hacking: Navigating the Cybersecurity Landscape Webinar on 27 March 2025**

Our AiSP Ladies in Cyber EXCO Lead - Ms Judy Saw participated in the Beyond Hacking: Navigating the Cybersecurity Landscape Webinar on 27 March 2025 afternoon hosted by Visa to help women navigate the various career options available in Cybersecurity.

Judy shared insights and information on potential courses and learning pathways on the different courses or certifications that the participants can pursue for the different career pathways in Cyber and equip them with a learning pathway to help women who are interested in returning back to the workforce to pivot their career / reenter the tech workforce again.
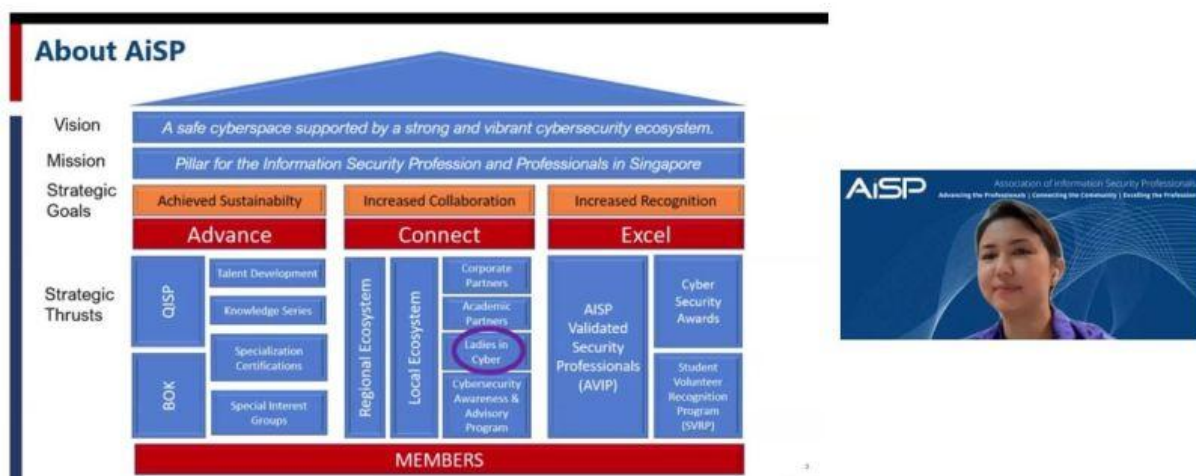
# Digital For Life

**Kampong Fiesta @ Garden Hill RN on 8 March**

AiSP & our Corporate Partner - RSM - Singapore is proud to be part of the Kampong Chai Chee Fiesta Celebration from 23 Feb 25 to 10 May 25. On 8 March, AiSP was at Kampong Fiesta @ Garden Hill RN with more than 100 participants for a day of Fun and Learning through the interactive workshops, act against scams and scam awareness talk. We also joined the residents to celebrate International Women Day together. AiSP also shared with the residents on the AI & Digital Skills for Every Generation. Thank you, AiSP Secretary & Cyberwellnees Co-Lead Ms Soffenny Yap & AiSP Patron & Grassroot Advisor, to Kampong Chai Chee - SMS Tan Kiat How for joining us.

UOB is one of the donors to the Digital for Life Fund and is a proud sponsor of Future-Ready: Mastering AI & Digital Skills for Every Generation by Association of Information Security Professionals.



**Kampong Fiesta @ Aquarius By the Park on 22 March**

AiSP & our Corporate Partner - RSM - Singapore is proud to be part of the Kampong Chai Chee Fiesta Celebration from 23 Feb 25 to 26 Apr 25. On 22 March, AiSP was at Kampong Fiesta @ Aquarius By the Park with more than 100 participants for a day of Fun and Learning through the interactive workshops, act against scams and scam awareness talk.

AiSP also shared with the residents on the AI & Digital Skills for Every Generation. Thank you, AiSP Secretary & Cyberwellnees Co-Lead Ms Soffenny Yap & AiSP Patron & Grassroot Advisor, to Kampong Chai Chee - SMS Tan Kiat How for joining us.

*back to top*

UOB is one of the donors to the Digital for Life Fund and is a proud sponsor of Future-Ready: Mastering AI & Digital Skills for Every Generation by Association of Information Security Professionals.



**PA Kampong Chai Chee Kampong Fiesta Community at Linear Green RN on 29 March**

AiSP & our DFL Partner - RSM - Singapore is proud to be part of the Kampong Chai Chee Fiesta Celebration from 23 Feb 25 to 26 Apr 25. On 29 March, AiSP was at Kampong Fiesta @ Clearwater with more than 100 participants for a day of Fun and Learning through the interactive workshops, act against scams and scam awareness talk.

AiSP also shared with the residents on the AI & Digital Skills for Every Generation. Thank you, Cyberwellness Co-Lead Mr Dennis Chan & AiSP Patron & Grassroot Advisor, to Kampong Chai Chee - SMS Tan Kiat How for joining us.

UOB is one of the donors to the Digital for Life Fund and is a proud sponsor of Future-Ready: Mastering AI & Digital Skills for Every Generation by Association of Information Security Professionals.

# Corporate Partner Event

**AiSP x Cyber Security Agency of Singapore (CSA) x Rapid7 Security Day Singapore 2025 on 11 March**

In collaboration with our Corporate Partner, Rapid7, AiSP organised "Securing What's Next, Together - Security Day Singapore" on 11 March with more than 45 attendees.

A big thank you to Mr Rob Dooley, Mr Robin Long and Mr Jay Chow from Rapid7 for speaking at the event. As well as Ms Veronica Tan from Cyber Security Agency of Singapore (CSA) for being the keynote speaker.

## AiSP x Emereo Technology – Security-first AI powered networking from edge to cloud On 20 March

AiSP partnered with Emereo Technology, Hewlett Packard Enterprise and Microsoft where we covered on "Security-First AI Powered Networking from Edge to Cloud" with 30 attendees on 20 March.

Thank you Prof Goh Weihan, Mr Andros Chen, Mr Shi Bin Dong, Mr Margoob Chowdhury and Mr Gordon Tan for speaking at the session.

**Navigating the Digital Future: Cyber Resilience in an Era of AI, Quantum and Conflict on 14 April**

**Navigating the Digital Future: Cyber Resilience in an Era of AI, Quantum and Conflict**



In an age defined by rapid technological advancements and global uncertainties, the need for robust cyber resilience has never been more critical. As artificial intelligence (AI) and quantum computing reshape the digital landscape, new vulnerabilities and threats emerge, challenging organizations and individuals alike to safeguard their digital assets. Furthermore, the rise of cyber conflict and state-sponsored attacks highlights the importance of a resilient cyber infrastructure that can withstand and recover from disruptions.

## Global Threat Landscape 2025
Speaker: Yihao Lim, Lead Threat Intelligence Advisor (JAPAC , EMEA South), Google

This presentation will comprise of observations from global threats that we observe across Espionage, Financial Crime and Hacktivism motivated actors, and it will also comprise of some cyber threat predictions in 2025.

## 18 Years Of Cyber War And 3 Years Of Shooting War - Lessons From Estonia And Ukraine
Speaker: Luukas Ilves, Advisory to the Deputy Prime Minister of Ukraine, Former Government CIO of Estonia

18 years ago, large-scale Russian cyber attacks against Estonia in 2007 marked the beginning of cyber conflict as a tool of modern statecraft. 15 years later, Russia's

invasion of Ukraine marked the beginning of a dangerous new phase in global politics - and an escalation in the use of technology in warfare. Luukas will discuss the lessons both countries have learned from these conflicts, and what should be top of mind for all digital and cyber professionals in the coming years.

**Panel Discussion**

Moderator: Johnny Kho, AiSP Advisory Council Member & Immediate Past President
Panellists:
Justiin Ang, Government CISO, Assistant Chief Executive (Cybersecurity), GovTech
Luukas Ilves, Advisory to the Deputy Prime Minister of Ukraine, former Government CIO of Estonia
Yihao Lim, Lead Threat Intelligence Advisor (JAPAC , EMEA South), Google

## Draft Agenda

- 6:00 - 7:00 PM: Networking Dinner
- 7:00 - 7:30 PM: Global Threat Landscape 2025
- 7:30 - 8:00 PM: Keynote by Luukas Ilves
- 8:00 - 8:30 PM: Moderated Discussion

Date: 14 April 2025
Time: 6PM – 9.30PM
Venue: Village Square, MBC10 level 10
Registration: https://forms.office.com/r/ckFmSgm47x

# Upcoming Activities/Events

**Ongoing Activities**

| Date | Event | Organiser |
|---|---|---|
| Jan – Dec | Call for Female Mentors (Ladies in Cyber) | AiSP |
| Jan – Dec | Call for Volunteers (AiSP Members, Student Volunteers) | AiSP |

**Upcoming Events**

| Date | Event | Organiser |
|---|---|---|
| 1 – 4 Apr | Black Hat Asia 2025 | Partner |
| 2 Apr | Career Talk at Hougang Secondary School | AiSP & Partner |
| 3 – 5 Apr | World Skills 2025 at Marina Bay Sands | AiSP & Partner |
| 4 Apr | Career Talk at Bukit Panjang Government High School | AiSP & Partner |
| 7 Apr | Securing AI in Critical IT Systems | Partner |
| 8 Apr | Legal Investigative Technology Experts (LITE) Conference & Launch of Legal Investigative Technology Experts (LITE) Special Interest Group | AiSP |
| 9 Apr | CISO FSI Singapore | Partner |
| 9-11 Apr | AiSP Cybersecurity & AI Hackathon 2025 | AiSP & Partner |
| 13 Apr | DFL @ Yuhua CC | AiSP & Partner |
| 14 Apr | Navigating the Digital Future: Cyber Resilience in an Era of AI, Quantum and Conflict | AiSP & Partner |
| 15 Apr | ignITE Skills Challenge at ITE West | AiSP & Partner |
| 15 Apr | Govtech STACKxCybersecurity 2025 | Partner |
| 16 – 17 Apr | CS4CA APAC & APAC Cyber Summit | Partner |
| 19 Apr | PA Kampong Chai Chee Kampong Fiesta Community at Rainbow Ville RN | AiSP & Partner |
| 23 – 25 Apr | GITEX Asia | Partner |
| 26 Apr | PA Kampong Chai Chee Kampong Fiesta Community at Rainbow Bedok Reservoir View RN | AiSP & Partner |

***Please note events may be postponed or cancelled due to unforeseen circumstances*

# CONTRIBUTED CONTENTS

## Article from AI SIG

### Harnessing AI for Creative Ideation

Dr Vincent Mack is a Lecturer at Nanyang Polytechnic's School of Information Technology. His passion is in Large Language Models, Knowledge Representation, and Knowledge Management Systems. Building on his experience working as a Researcher and Policy Consultant at the S. Rajaratnam School of International Studies, Dr Vincent currently covers IT subjects across AI, analytics and software engineering for Pre-Employment Training and Specialist Diploma students. He is involved in cloud-based Gen AI and Machine Learning solutions and also conducts research at NYP.

With the rapid adoption of Generative AI (GenAI), creative ideation is undergoing a transformation. Many users employ AI to generate text, images, and code, often as a surface-level replacement for creative labour. However, this practice tends to produce shallow outputs, curated from datasets that reflect predefined notions of desirability. While we cannot escape AI's influence on the creative economy, it is imperative to understand and apply it correctly in the ideation process. By revisiting established theories of creativity, such as the Geneplore model, and leveraging AI for structured ideation, we can move beyond mere replication and harness AI as a true creative partner.

### AI, Creativity, and the Search for Meaningful Innovation

The recent surge in GenAI adoption has brought both opportunities and challenges in the creative space. AI-generated content now permeates various domains, from literature and art to software development and scientific research. Despite the convenience, these AI-driven outputs often lack depth, originality, and nuance, leading to a homogenisation of creativity. This issue stems from the fact that AI models are trained on datasets comprising existing works – works that have already been deemed desirable, either through cultural biases or market forces. Consequently, the outputs are mere permutations of past ideas, reinforcing conventional thought rather than fostering genuine innovation.

A recent article in The Economist (2025) suggests that rather than leveling the playing field, AI is deepening the divide. Skilled professionals will benefit the most, while lower-skilled workers struggle to keep up. As AI takes over more creative and knowledge-based jobs, its impact seems more disruptive than helpful. This raises concerns about equitable access to creative opportunities and who ultimately reaps the harvest from AI-driven ideation.

back to top

Thus, the challenge is not in whether we should use AI, but in how we should use it. AI is already transforming creative and scientific industries, making it crucial to rethink how ideation should take place in this AI-augmented landscape. To do so, we must revisit established theories of creativity and ideation, aligning them with AI's capabilities to optimise the generative process.

**Understanding Creativity and Ideation**

Creativity has long been a contested concept in psychology and cognitive science. It defies easy definition and is often assessed through proxies such as novelty, quality, and relevance. Dean et al. (2006) propose that creativity is ultimately a function of an idea's perceived value, rather than an objective property. Practical creativity then is about balancing familiarity with the unknown – producing work that is both innovative and feasible.

The process of ideation itself has been widely studied. Two dominant perspectives emerge: ideation as a recombinatorial process and ideation as a search problem. The Geneplore model (Finke, 1996) offers a structured view of creativity as a two-phase cycle:

- **Generative Phase** – The mind produces pre-inventive structures: raw, unpolished ideas that are incomplete or abstract.

- **Exploratory Phase** – These pre-inventive structures are evaluated, modified, and refined into viable concepts.

This model aligns well with AI-driven ideation. AI systems, particularly machine learning models, excel in searching for local optima in predefined spaces. However, their efficiency is limited by how the idea space is structured. In both phases of the Geneplore model, the problem can be framed as a search task – one where AI can assist by mapping concepts onto multi-dimensional embeddings, allowing systematic exploration of idea spaces.

**AI as a Tool for Structured Ideation**

Applying machine learning to ideation requires defining how ideas – and thereby their resultant exploration space(s) – are represented. One promising approach is vector embeddings – mathematical representations of concepts in high-dimensional space. By structuring ideation as a search within this space, AI can facilitate both divergent thinking (expanding possibilities) and convergent thinking (refining ideas).

A related approach is graph-based ideation, exemplified by Don Swanson's literature-based discovery model (Smalheiser, 2017). In this framework, new knowledge emerges by identifying implicit connections between separate research domains. If A leads to B, and B leads to C, then it is conceivable that A might also lead to C – forming the basis for new hypotheses. AI can enhance this process by scanning vast scientific literatures, constructing knowledge graphs, and suggesting novel linkages that might otherwise go unnoticed.

**Overcoming AI's Limitations in Ideation**

Despite these strengths, AI struggles with one of creativity's core elements: breaking

paradigms. While AI can efficiently explore within a predefined search space, it does not easily redefine the boundaries of that space. This limitation means that human intuition, curiosity, and domain expertise remain irreplaceable.

To counterbalance AI's tendency toward conventional outputs, human users must actively introduce disruption into the AI-assisted ideation process. Techniques such as adversarial prompting, where AI-generated ideas are deliberately challenged, and cross-domain inspiration, where AI is fed inputs from unrelated fields, can push AI beyond its default creative constraints.

## Summary

As AI becomes increasingly integrated into creative and scientific workflows, the risk of superficiality grows. However, by aligning AI capabilities with established models of creativity – such as the Geneplore model and graph-based discovery frameworks – we can move beyond replication toward true ideation. AI should not replace creativity but rather augment it by acting as a structured exploration tool. To fully realise this potential, we must not only develop better algorithms but also educate users on how to wield AI as a partner in the creative process. The future of ideation lies not in AI replacing human ingenuity, but in humans and AI co-evolving towards more profound, structured, and boundary-pushing creativity.

## References

Dean, Douglas, Jillian Hender, Thomas Rodgers, and Eric Santanen. "Identifying Quality, Novel, and Creative Ideas: Constructs and Scales for Idea Evaluation." *Journal of the Association for Information Systems 7*, no. 10 (October 2006): 646–99. https://doi.org/10.17705/1jais.00106.

Finke, Ronald A. "Imagery, Creativity, and Emergent Structure." *Consciousness and Cognition* 5, no. 3 (September 1996): 381–93. https://doi.org/10.1006/ccog.1996.0024.

Smalheiser, Neil R. "Rediscovering Don Swanson: The Past, Present and Future of Literature-Based Discovery." *Journal of Data and Information Science* 2, no. 4 (December 29, 2017): 43–64. https://doi.org/10.1515/jdis-2017-0019.

The Economist. "How AI Will Divide the Best from the Rest." (February 13, 2025) Accessed February 19, 2025. https://www.economist.com/finance-and-economics/2025/02/13/how-ai-will-divide-the-best-from-the-rest.

Contact Information: Vincent Mack (Dr)
School of Information Technology
Nanyang Polytechnic
E-mail: vincent_mack@nyp.edu.sg

# Article from CISO SIG

### 1.  Introducing CISO with a deep interest in cybersecurity

I am Perry Young, a CISO and Customer Technology Advisor in the Security & Resilience practice for the world's largest Global Systems Integrator, Kyndryl where I cover the ASEAN region as a whole.

In my 27 years of experience I have largely worked in or around the Global Financial Sector in leading banks, stock exchanges and high tech vendors. Originating from the UK, I transferred to Singapore in 2017 where I met my wife and now call Singapore my home.

### 2.  What brought you to the Cybersecurity industry?

My entry point into Cybersecurity was gradual over many years and ran adjacent to various network engineering and architecture roles (including specialisms in financial markets trading technology and ultra-low latency network architectures), where I became a hybrid network and security SME, began to delve deeper into other cybersecurity realms as diverse as threat modelling, cyber risk management, security architecture and my current favourite areas of expertise (where I add industry thought leadership), threat-informed defence and security by-design.

### 3.  What were your defining moments in this industry, and factors or guidance that helped you achieve them?

There have been many industry firsts throughout my career which are too numerous to mention. The most defining moments are perhaps becoming a people leader at scale, navigating through corporate political structures and driving significant outcomes when it seems the barriers to success are everywhere. Successes are great but it is bouncing back from adversity and pushing through the roadblocks that has helped to shape my resilience and drive for growth.

### 4.  What is it that you love most about your role?

I recently decided to pivot back from Enterprise into the sell side and I really like the energy and the diversity of exploring the different challenging scenarios across organisations in different markets, cultures and industry sectors. I really liked what Kyndryl stands for, its focus on Cyber Resilience as well as Defence and the ability to help build and expand our ASEAN Security & Resilience practice. The potential feels boundless.

### 5.  What are some of the trends you have seen in the market lately, and what do you think will emerge in the future?

The days of spending on security technologies without alignment to specific measurable security outcomes are gone. A threat aligned approach to implementing security

countermeasures to measurably reduce residual risks as part of a continuous lifecycle is the best chance we have of moving the needle in protecting organisations.

Threat-Modelling which focuses on assets, systems and attacks to identify exploitable weaknesses and the implementation of Minimum Viable Countermeasures (MVC) to focus cyber mitigation efforts is the key.

I align defences to the MITRE ATT&CK framework to determine defensive coverage as well as gaps and validate controls efficacy using adversary emulation testing and Purple teaming methodology. As new threats emerge or technologies change, it becomes a continuous iterative process to review risk posture.

Cyber Resilience from the perspective of being able to Anticipate, Withstand, Respond and Recover in the context of the inevitable assumed breach is an essential consideration. I like to explore what is an organisations Cyber RTO nd how will this be accomplished.

I am also active in various industry working groups and contribute to thought leadership in Zero Trust Architectures, AI Security methodology and more.

## 6. What do you think is the role of CISO?

This is influenced by the company type and the CISO's reporting line. I for one am more of the Field CISO type, which is different from a more GRC focused enterprise CISO or other types. I heard from one CISO who reported to his firms Chief Legal Officer, which when you think about it has some merits.

## 7. What can we do to encourage more people to join the cybersecurity sector?

It is a hugely diverse field of expertise these days. There is something in it for many types of individuals, not just STEM graduates. I do think that for serious Cybersecurity technical roles, it is better to elevate from another discipline such as networks, software engineering or another technology field. You cannot secure a thing if you do not understand the mechanics of the thing you are securing.

## 8. What do you want to achieve or contribute to the Cybersecurity Ecosystem?

I am beginning to make my mark driving Threat-Informed Defence approaches focused on the technology and I want to expand this discipline across Asia, to really move the needle on effective cyber defence across industry verticals.

## 9. Any advice for the Cybersecurity Professionals?

Continuous learning, don't fall at the first hurdle as there will be 1000 more hurdles. Ask questions, stretch beyond your comfort zone and set yourself stretch goals.

back to top

# Article from CPP, OPSWAT

**C1D2 Certification, Vulnerabilities, and Expert Insights from OPSWAT**

Welcome to the OPSWAT Update – your source for news and information on Critical Infrastructure Protection (CIP) and OPSWAT products and services. If you haven't already, be sure to follow OPSWAT on **LinkedIn**, **Facebook**, **X**, and **Instagram** for real-time updates.

## OPSWAT in the News

**OPSWAT's MetaDefender Optical Diode Achieves C1D2 Certification, Enhancing Safety and Cybersecurity in Hazardous Environments**
The MetaDefender Optical Diode has achieved a C1D2 certification, ensuring its safe and reliable operation in hazardous environments such as oil, gas, and chemical industries, while enhancing both physical safety and cybersecurity.
**Learn More**

**Alessandro Porro, VP of Global Channels, Awarded 2025 CRN Channel Chief for Third Consecutive Year**
Alessandro Porro has been named on the 2025 CRN Channel Chiefs list for the third consecutive year in recognition of his leadership and success in driving the company's growth through its channel strategy.
**Learn More**

**Protecting Apps from Hackers: OPSWAT Discovers Remote Execution Vulnerability in Mongoose, a Developer Library for MongoDB**
Discover how an OPSWAT Cybersecurity Fellowship Program Researcher uncovered the vulnerability and worked closely with Mongoose developers to quickly fix it, not just once, but twice.

**Learn More**

**Cybersecurity Trends Shaping Critical Infrastructure in 2025 with Benny Czarny**
Benny Czarny, CEO and Founder of OPSWAT, was featured on the Risk Management Show to discuss 2025 trends with a heavy focus on Content Disarm and Reconstruction (CDR).

**Watch Now**

back to top

Check out our recent global and media coverage highlights at **OPSWAT in the News** and **Press Releases** to see how we are continuing our commitment to protect the world's critical infrastructure.

## Critical Infrastructure Resources

### The Network: The Cybersecurity Intelligence War You Never See

From defending the Pentagon to pioneering next-gen security solutions, this documentary explores the relentless fight against cyberthreats, the evolution of network detection and response, and how the merger of OPSWAT and InQuest is building the ultimate defense against modern cyber warfare.

Watch Now

### Detonator - The Endless Quest for the Perfect Sandbox

Detonator is the untold journey of Jan Miller and how his relentless pursuit of innovation transformed sandboxing technology from a security tool into a global standard. Together with OPSWAT's early belief in his vision for the future of sandboxing, discover how he took a niche technology and turned it into an industry-defining solution that protects critical infrastructure worldwide.

Watch Now

### Whitepaper: A New Day, A New Dawn for File Security

Download our newest resource for expert strategies in protecting files, enabling secure collaboration, meeting compliance standards, and future-proofing your file security against emerging threats.

**Download Now**

### Customer Story: Abdi Ibrahim Secures Pharma Data with OPSWAT MetaDefender Kiosk™

Türkiye's largest pharmaceutical company safeguards sensitive intellectual property and ensures compliance using OPSWAT technology to scan and sanitize 18,000+ files per day with no downtime, eliminating malware risks from peripheral media.

**Learn More**

## Product Spotlight

### MetaDefender Sandbox™

AI-driven analysis that quickly detects even the most evasive malware. With multi-layered, lightning-fast detection and adaptive threat analysis, it provides the deep insights needed to protect critical assets from zero-day attacks.

Learn More

## OPSWAT Channel

*back to top*

As a leader in critical infrastructure protection, OPSWAT brings innovative technologies and products to your existing security portfolio. Our solutions are available through our exclusive community of distributors and resellers across the globe. To locate a distributor or reseller in your region please visit our **reseller locator**.

# Article from SVRP 2024 Gold Winner, Jason Kek Jun Kai [NP]



**How SVRP has directly impacted your cybersecurity journey?**
SVRP has given me numerous opportunities to participate in industry-relevant events and skills training. By engaging in various volunteer activities such as assisting in events like BlackHat Singapore and SINCON, I have been able to network with professionals and hone my skills. Furthermore, through leadership roles in initiatives like organizing the ISC2 Youth Wing activities, I've been able to refine my event planning and management capabilities. The structured support from SVRP has also encouraged me to continuously learn and grow within the cybersecurity field.

**How SVRP has inspired them to contribute to the cybersecurity field?**
SVRP has highlighted the importance of giving back to the community. Through the recognition program, I've seen firsthand how volunteers can shape the next generation of cybersecurity professionals. By being a leader and mentor, I can contribute by sharing my knowledge and organizing educational activities. These efforts not only help foster a stronger cybersecurity community but also create awareness and interest among youths who may be considering careers in cybersecurity.

**What motivates you to be a student volunteer?**

What motivates me the most is the opportunity to give back and make a difference. Volunteering allows me to share my knowledge and experiences while learning from others. It's rewarding to see how my efforts in organizing workshops, such as the ones I led for NullSec, have helped other students gain confidence in their skills. Additionally, the camaraderie and teamwork in volunteering activities inspire me to keep pushing the boundaries of my abilities.

**How would you want to encourage your peers to be interested in cyber security?**

I would encourage my peers by showing them how exciting and impactful cybersecurity can be. I'd share my experiences of competing in CTFs and participating in bug bounty programs, emphasizing the practical skills you gain and the real-world applications of what we learn. I would also introduce them to the vibrant cybersecurity community through volunteer opportunities, where they can network and grow professionally. I believe peer-led workshops and hands-on sessions are great ways to get more students involved.

back to top

# PROFESSIONAL DEVELOPMENT

## Qualified Information Security Professional (QISP®)

**Register for QISP Preparatory Course conducted by RP on 14-16 April**

# QISP Exam Preparation Crash Course by Deloitte

**Online QISP Exam Preparatory Course**



The QISP examination enables the professionals in Singapore to attest their knowledge in AiSP's Information Security Body of Knowledge domains. Candidates must achieve a minimum of 50-64% passing rate to attain the Qualified Information Security Associate (QISA) credential and 65% and above to achieve the Qualified Information Security Professional (QISP) credential.

Our highly responsive e-learning platform will allow you to learn anytime, anywhere with modular courses, interactive learning and quizzes. Complete the course in a month or up to 12 months! Enjoy lean-forward learning moments with our QISP/QISA preparatory e-learning course. Receive a certificate of completion upon completion of the e-learning course. Fees do not include QISP examination voucher. Register your interest here!

## Body of Knowledge Book (Limited Edition)

Get our **Limited Edition** Information Security Body of Knowledge (BOK) Physical Book at **$87.20 (inclusive of GST)**.
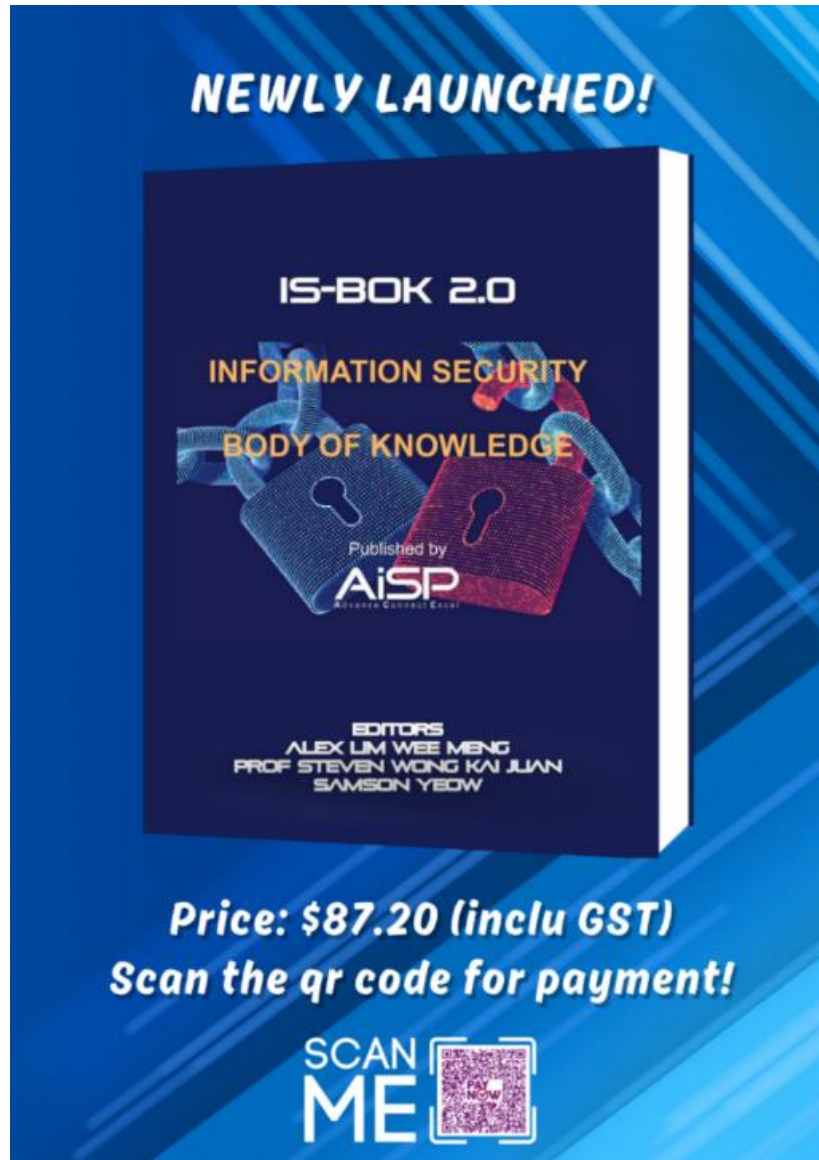


Please scan the QR Code in the poster to make the payment of **$87.20 (inclusive of GST)** and email secretariat@aisp.sg with your screenshot payment and we will follow up with the collection details for the BOK book. **Last 30 books for sale!**

back to top

## Body of Knowledge E Book

# MEMBERSHIP

## AiSP Membership

**Complimentary Affiliate Membership for Full-time Students in APP Organisations**

If you are currently a full-time student in the IHLs that are onboard of our **Academic Partnership Programme (APP)**, AiSP is giving you complimentary Affiliate Membership during your course of study. Please click **here** for the application form and indicate your student email address, expected graduation date and name of your institution in the form.

**Complimentary Affiliate Membership for NTUC Members**

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2025) from 1 Jan 2025 to 31 Dec 2025. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. This does not include Plus! card holder (black-coloured card), please clarify with NTUC on your eligibility.

On **membership application**, please do not email your personal data to us via email if your information or attachment is not password-protected. Please send us your password via **Telegram** (@AiSP_SG).

Once we receive confirmation from NTUC on the validity of your NTUC membership, AiSP would activate your one-year complimentary AiSP Affiliate membership.

**CPP Membership**



For any enquiries, please contact secretariat@aisp.sg

**AVIP Membership**

AiSP Validated Information Security Professionals (**AVIP**) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development, and career progression for our professionals.

**Membership Renewal**

**Individual membership expires on 31 December each year.** Members can renew and pay directly with one of the options listed here. We have GIRO (auto - deduction) option for annual auto-renewal. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.

**Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!**

**Please check out our website on Job Advertisements by our partners.** For more updates or details about the memberships, please visit www.aisp.sg/membership.html

# AiSP Corporate Partners

Acronis

AZ ASIA-PACIFIC

BeyondTrust

BLACKPANDA

CISCO

CLIXER

CSA SINGAPORE

CSIT Centre for Strategic Infocomm Technologies

CYBERSAFE YOUR SECURITY, OUR PRIORITY

DBS

Eclypsium

ENSIGN INFOSECURITY

FORTINET

Genesis NETWORKS

GOVTECH SINGAPORE

Grab

HORANGI CYBER SECURITY

HTX

HUAWEI

illumio

image engine

back to top

Visit https://www.aisp.sg/corporate_members.html to know more about what our Corporate Partners (CPP) can offer for the Cybersecurity Ecosystem.

# AiSP Academic Partners

# Our Story…

We are an independent cybersecurity association that believes in developing, supporting as well as enhancing industry technical competence and management expertise to promote the integrity, status and interests of Information Security Professionals in Singapore.

We believe that through promoting the development, increase and spread of cybersecurity knowledge, and any related subject, we help shape more resilient economies.

**Our Vision**
A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem.

**Our Mission**
AiSP aims to be the pillar for Information Security Professionals and the overall Information Security Profession through:

▪ promoting the integrity, status and interests of Information Security Professionals in Singapore.
▪ enhancing technical competency and management expertise in cybersecurity.
▪ bolstering the development, increase and spread of information security knowledge and its related subjects.

🌐 www.AiSP.sg
✉ secretariat@aisp.sg
📞 +65 8878 5686 (Office Hours from 9am to 5pm)
*Please email us for any enquiries.*