AiSP

NEWSLETTER

February 2025

NEWS & UPDATE

Continued Collaboration

AiSP would like to thank National University of Singapore, Republic Polytechnic and Tenable for their continued support in developing the cybersecurity landscape:

NUS National University of Singapore

REPUBLIC POLYTECHNIC DISCOVER. TRANSFORM. ACHIEVE

tenable

News & Update

softScheck CNY celebration on 24 January

On 24 January, AiSP was invited to our Corporate Partner - softScheck APAC Chinese New Year Celebration celebrating the achievements that they have achieved for the past year. Thank you, Mr Henry Tan & Mr Victor Lim, for having AiSP in your milestone and we looked forward in working closely with softScheck in 2025.

back to top

Member Acknowledgment

Interview with AiSP EXCO Member Ms Loh Kar Wei

1. What is your vision for your contribution in AiSP? What do you think is the biggest issue in the Cybersecurity Industry?

My vision for my contribution in AiSP is a world where anyone, even someone as young as 8 years old can already start learning and educating themselves in Cybersecurity. In order to do this, we must create an effective medium that can essentially simplify and articulate what and why Cybersecurity is needed to a layman.

This ties deeply to the ever growing talent gap, where organisations struggle to find skilled professionals with technical and soft-skill know-hows. Reasons for this can be the high technical learning curve to just start somewhere and high hardware specs to even run enough Virtual Machines that not everyone, especially kids and the under-privileged will have access to. Bridging this gap has always been my mission as a Cybersecurity educator and AiSP provides opportunities to fulfill this mission on a larger scale.

2. As the EXCO member, there are times where you will be representing AiSP in events and engagements. How do you plan to uphold AiSP's reputation and values while effectively communicating its mission and objectives to external stakeholders?

AiSP's values rest on trust, integrity and collaboration. By embodying professionalism, honour, and inclusivity in all interactions while representing AiSP, I ensure that all collaboration opportunities will still reflect the organisation's commitment to advancing the Cybersecurity ecosystem in Singapore while aligning with its core values.

3. Lastly, what would you like to share and contribute your expertise with our AiSP members and the wider community?

As a Cybersecurity trainer and educator, my expertise lies in the education and talent development side for both the kids and adult sectors. There is a need for more engaging and practical learning content catered to the younger ages and learners from different

back to top

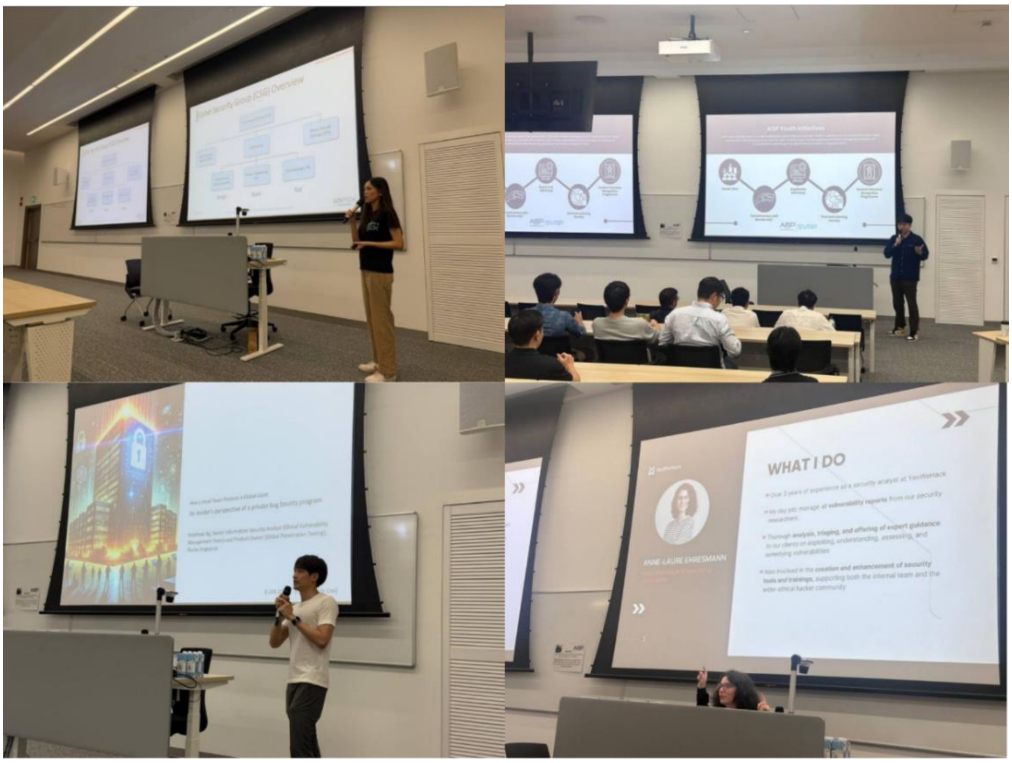
backgrounds to cultivate a culture of accessible and lifelong learning for members of AiSP and beyond. This is what I would like to share and contribute with, especially for aspiring learners with no access to the necessary hardware and direction required to get started.

Integrating my Cybersecurity technical knowledge and my skills as a hobbyist game developer, I aim to implement 2D gameplay in the way we teach and learn Cybersecurity to make learning more accessible through the browser, simplify technical content into engaging gameplay, and push this platform out to our local kids and youths to educate them in the wonders of Cybersecurity!

Student Volunteer Recognition Programme (SVRP)

AiSP Youth Meetup – Bug Bounty on 8 January

AiSP Organised our first 2025 Youth Meetup on 8 January focusing on Bug Bounty with 70 attendees. Our speakers had shared on Building Resilient Cybersecurity: Organizational Strategies, Capabilities and Career Pathways in the Public Sector, How a Small Team Protects a Global Giant and lastly, Starting Strong in Infosec: How Bug Bounty Can Bootstrap Your Career. Thank you to our Corporate Partner, GovTech Singapore and YesWeHack for supporting this event. Thank you, Ms Chai Li Xian, Mr Matthew Ng and Ms Anne-Laure Ehresmann, for speaking as well as our SVRP EXCO Lead, Mr Yu Pengfei for the sharing. Thank you to our Academic Partner, Singapore Institute of Technology for hosting us at their beautiful campus at Punggol Digital District.



back to top

Visit to RSM on 23 January

On 23 January, AiSP brought 20 students from Assumption English School to our Corporate Partner - RSM Singapore for an engaging session, where they provide an in-depth look into RSM diverse services. They gained insights from the CPA experts on audit, accounting, and work practices. Exploring in Business Consulting services that covers Internal Audit (IA) and ESG strategies. Students had the opportunity to engage with the panelists in Q&A session and ended with a Kahoot Game.

PANELLIST Q&A
EXIT
RSM
RSM x Assumption English School – Career Insights
23 January 2025
EXIT
[Career Insights] Assumption English School X RSM
2
tristan
1
gems
3
Reuben
EXIT

TP InfoTech Day 2025 on 23 January

On 23 January, AiSP SVRP EXCO Lead Mr Pengfei Yu, did a sharing on “The Present Is the Future: How AI is Changing Cybersecurity” to more than 80 Youths at TP InfoTech Day 2025. A big thank you to our Academic Partner, Temasek Polytechnic for having us.

back to top

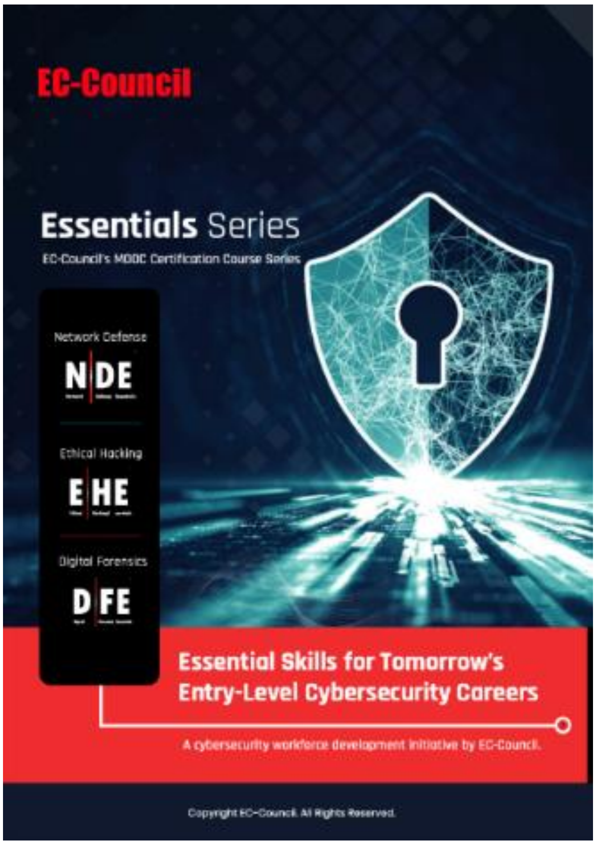
Elevating Cybersecurity Education Through Unprecedented Collaborations

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.

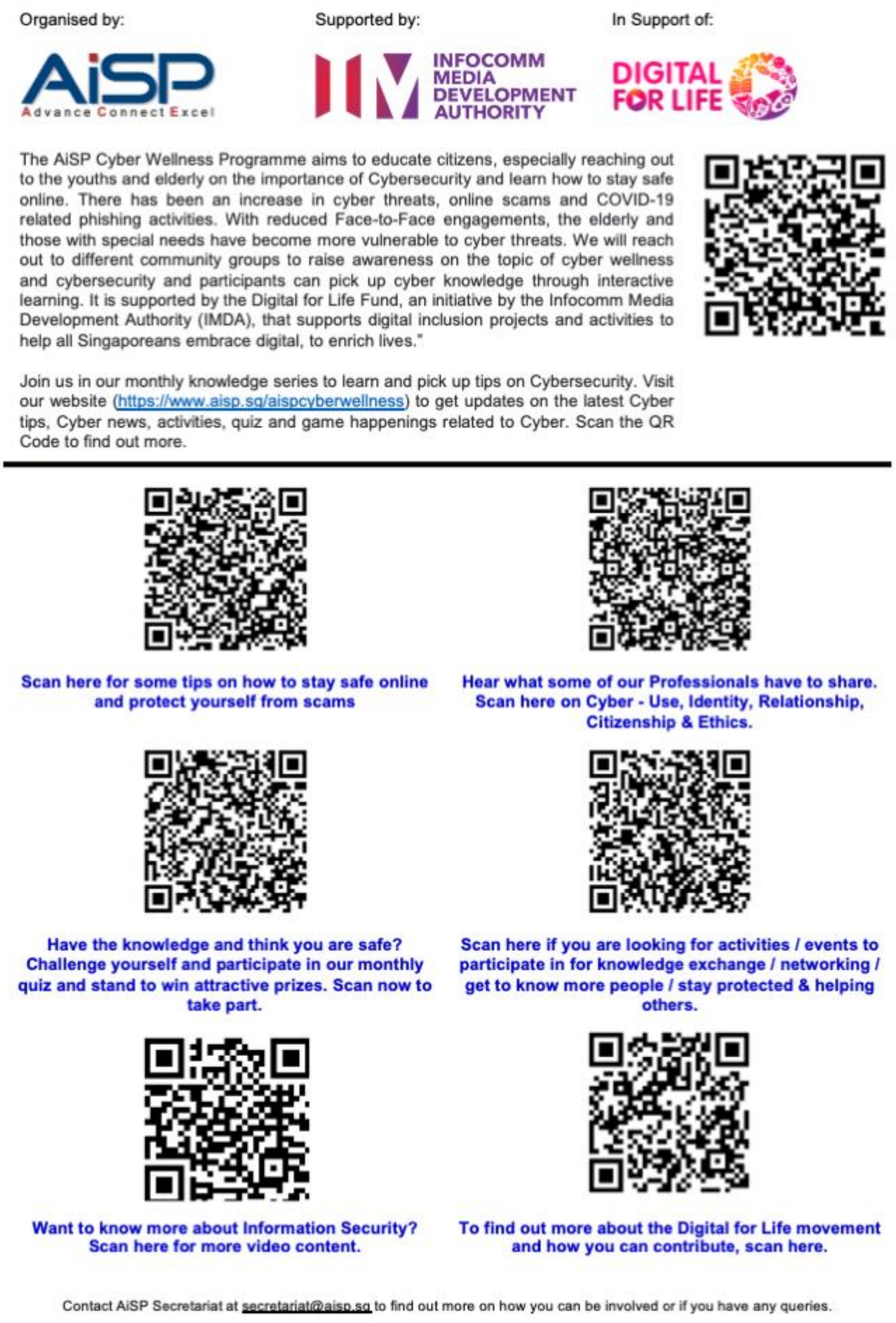
About the EC-Council Cyber Essentials Certification

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.


EC-Council
Essentials Series
EC-Council's MOOC Certification Course Series
Network Defense
N|DE
Ethical Hacking
E|HE
Digital Forensics
D|FE
Essential Skills for Tomorrow's Entry-Level Cybersecurity Careers
A cybersecurity workforce development initiative by EC-Council.
Copyright EC-Council. All Rights Reserved.

back to top

AiSP Cyber Wellness Programme



Organised by: AiSP Advance Connect Excel

Supported by: INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In Support of: DIGITAL FOR LIFE

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:

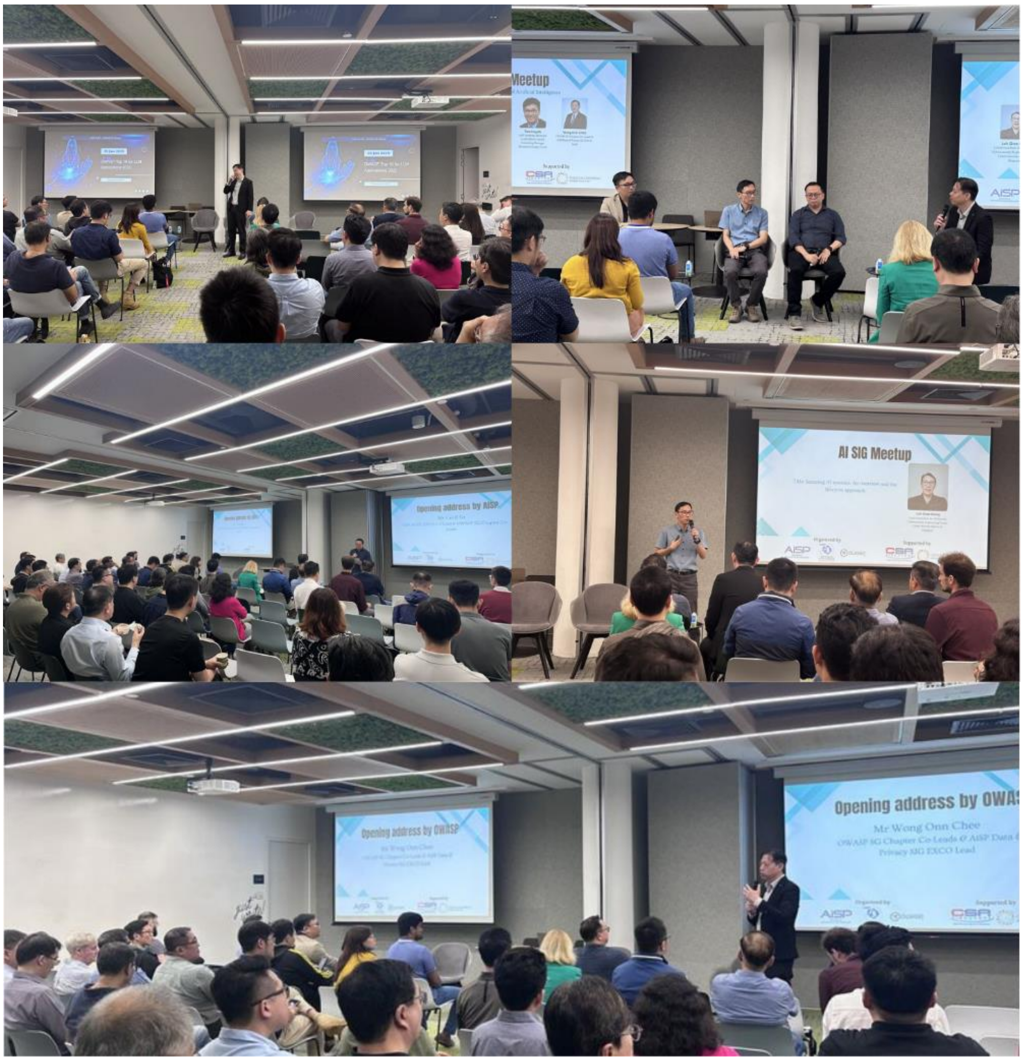
- Artificial Intelligence
- CISO
- Cloud Security
- Data and Privacy
- DevSecOps
- Legal Investigative Technology Experts (LITE)
- Quantum Security

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

back to top

AiSP AI SIG Meetup – Safeguarding the Future of Artificial Intelligence on 15 January

AiSP organised our first AI SIG meetup for 2025 on 15 January with more than 70 attendees in partnership with OWASP Singapore. Our speakers shared thought-provoking presentations, setting the stage for an intellectual journey into the heart of AI vulnerabilities and defenses. Attendees also gained insights into the latest adversarial attacks on AI models, delved into the nuances of privacy preservation in AI systems, and explored ethical considerations in AI development and deployment. Thank you, Cyber Leaders Nexus and Cyber Security Agency of Singapore (CSA), for supporting the event and thank you Mr Wong Onn Chee, Mr Cecil Su, Mr Tam Huynh and Mr Loh Chee Keong for sharing on AI at the meetup.



back to top

AiSP Quantum Security SIG Meetup – Quantum Resilience and What to Expect on 20 January

On 20 January, AiSP held our Quantum Security SIG Meetup where attendees got to engage with the speakers through panel discussion regarding the intersection of Quantum Computing and Cybersecurity that dives into the challenges and solutions surrounding secure infrastructure on Quantum. Attendees also gained insights on data protection, risk management and innovation. Thank you, Bitdefender, for supporting this event and thank you Mr Michael Lew, Mr Prasanna Ravi, Mr Niko Akatyev and Dr. Kawin Boonyapredee for speaking at the event.

back to top

AiSP DevSecOps SIG Meetup – "Learning Journey : Putting Sec[urity] in DevSecOps" on 22 January

On 22 January, AiSP DevSecOps SIG provided attendees with a learning journey where practitioners and industry professionals got to share their knowledge and engagement in communications. This event highlights the importance of having a strong security system built into software development processes where attendees also get to gain insights of the different tools and solutions to having better decision making to conclude what is suitable for their organization to understand the commitment and the support that is needed to succeed, with the support of Cyber Security Agency of Singapore (CSA), Checkmarx and Parasoft. Thank you, Mr Chuah Chin Yew, Mr Lim Yeen Fei, Mr Koh Choon Kiat, Mr Garion Kong, Mr John Lim and Mr Stanley Eu for speaking.

back to top

The Cybersecurity Awards

THE CYBERSECURITY Awards 2025

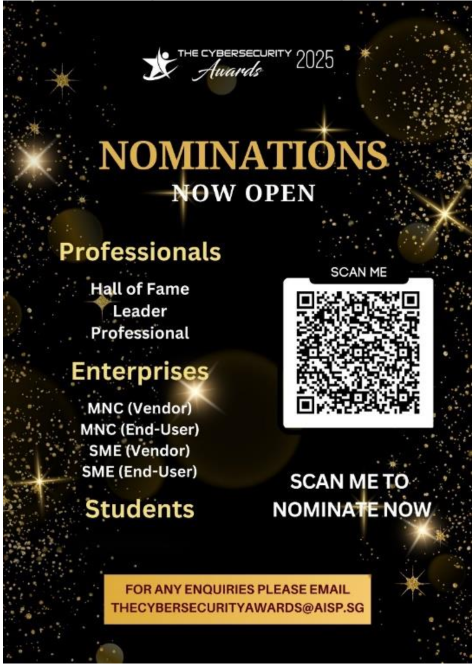
The Cybersecurity Awards 2025 nominations will start in February 2025.

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.



THE CYBERSECURITY Awards 2025

NOMINATIONS
NOW OPEN

Professionals
Hall of Fame
Leader
Professional

Enterprises
MNC (Vendor)
MNC (End-User)
SME (Vendor)
SME (End-User)

Students

SCAN ME

SCAN ME TO NOMINATE NOW

FOR ANY ENQUIRIES PLEASE EMAIL THECYBERSECURITYAWARDS@AISP.SG

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 **1 April 2025**!

For any enquiries, please email thecybersecurityawards@aisp.sg

Nomination will end on **1 April 2025**. All submissions must reach the secretariat by **1 April 2025.**

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

ORGANISED BY

AiSP
Advance Connect Excel

GOLD SPONSORS

HUAWEI

SANS | GIAC CERTIFICATIONS

SIT SINGAPORE INSTITUTE OF TECHNOLOGY

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

AiSP Ladies in Cyber Charter at St. Margaret's School (Secondary) on 10 January

AiSP Ladies in Cyber Charter started 2025 with a school talk on 10 January at St. Margaret's School (Secondary) at their annual Professional Guidance Day 2025. AiSP Exco Member Ms Loh Kar Wei shared with more than 50 female students on her journey in Cybersecurity and what certifications the students can take on to join the Cybersecurity industry. Thank you St. Margaret's School (Secondary) for having AiSP to share with the students.

back to top

SHE Singapore support Friendship Circles Kick-off and Lohei session on 17 January

AiSP Ladies in Cyber EXCO Lead - Ms Judy Saw represented AiSP to join 15 other organisations in the SHE Singapore support Friendship Circles Kick-off and Lohei session on 17 January. Judy also shared on the AiSP Friendship Circle that was done on 7 Dec 2024 with the rest of the partners. Thank you, Ms Yeo Wan Ling & National Trades Union Congress (NTUC) WAF for inviting AiSP Ladies in Cyber charter to be part of this meaningful event to reach out to more females.

Want to find out more on the Friendship Circle, join us in our next AiSP Friendship Circle on 9 March 2025 at Marina Bay Sands as part of the International Women Day celebrations. Contact the AiSP secretariat to find out more details.

back to top

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

AiSP Ladies in Cyber – Capture the Flag 2025

Ladies in Cyber
Capture the Flag 2025
SCAN HERE!
Engage in real-world cybersecurity scenarios.
9 March 2025, 9:00am - 4:30pm
Marina Bay Sands
Organized by
AiSP Association of Information Security Professionals
LADIES IN CYBER

Step into the dynamic world of cybersecurity with our Ladies' Capture the Flag (CTF) Competition, an interactive, hands-on experience designed exclusively for women. This competition offers participants the chance to engage in real-world cybersecurity scenarios, solving puzzles in areas such as cryptography, network security, and web exploitation. Through guided challenges, participants will gain practical skills, from identifying vulnerabilities to simulating attacks and defenses, providing invaluable exposure to cybersecurity tools and techniques in a supportive, collaborative environment.

This event is open to females 13 years old to 50 years old, whether you're a newcomer or have some technical background, this event is tailored to give you a firsthand, immersive introduction to cybersecurity. Join us to unlock your potential, connect with like-minded peers, and gain confidence in tackling cybersecurity challenges head-on.

Through practical exercises, participants will gain essential 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.

The event, Capture the Flag 2025 will be happening in the morning and the prize presentation will be held in the afternoon.

back to top

The prizes are:
First Prize: $500 Shopping Voucher
Second Prize: $300 Shopping Voucher
Third Prize: $200 Shopping Voucher

Requirements for device:

Component	Minimum Requirement	Recommended Requirement
Processor	Intel i5 (6th gen) or equivalent	Intel i7 (8th gen) or higher
RAM	8GB	16GB or higher
Storage	50GB free disk space	100GB free disk space
Graphics	Integrated GPU	Dedicated GPU (e.g., NVIDIA GTX 1050 or higher for AI tasks)
Network	Stable Wi-Fi, 10 Mbps or higher	Ethernet adapter (optional for stability)
Battery Life	4+ Hours	6+ Hours or access to charging stations
Display	13" screen, 1080p resolution	15" or higher, Full HD

1. Windows 10 and above (64 bit)
- Windows users should enable the Windows Subsystem for Linux (WSL)

2. macOS Ventura or later

3. Linux: Ubuntu 20.04 LTS or later
- Kali is not required

Date: 9 March 2025
Time: 9:00am – 4:30pm
Venue: Marina Bay Sands
Registration: https://forms.office.com/r/vCRWua9mKf

back to top

AiSP Ladies in Cyber Symposium 2025 on 9 March

AiSP Ladies in Cyber Symposium 2025

Ladies in Cyber
Symposium 2025 & Friendship Circle
9 March 2025, 12.30pm - 4:30pm
Marina Bay Sands
SCAN HERE!

Organized by

AiSP Association of Information Security Professionals | LADIES IN CYBER

AISP will be organising the fourth Ladies in Cyber Symposium on 09 March 2025 (Sun) at Marina Bay Sands (MBS) as part of the International Women's Day Celebration 2025 for female Youths and PMETs to know more about the importance of Cybersecurity and how women can play a role in it. We are expecting 150 Youths and professionals for the symposium. We are pleased to have with us Senior Minister of State for Ministry of Foreign Affairs & Ministry of National Development – Ms Sim Ann to be our distinguished Guest of Honour for the event.

The theme for the Ladies in Cyber Symposium 2025 is Accelerating Action: Empowering Women's Equality in Cybersecurity. In alignment with International Women's Day's call to #AccelerateAction for women's equality, the 2025 Ladies in Cyber Symposium will explore how gender diversity can propel innovation in cybersecurity. Ladies in Cyber Symposium 2025 event will feature Friendship Circles - small group discussions led by mentors that provide a supportive space for women to share experiences, seek advice, and build connections. Participants will engage in hands-on activities, workshops, and inspiring talks, focusing on overcoming barriers and driving real change to foster equality within the cybersecurity industry.

Date: 9 March 2025
Time: 12.30pm – 4:30pm
Venue: Marina Bay Sands
Registration: https://forms.office.com/r/vCRWua9mKf

back to top

Corporate Partner Event

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

RAPID7 | AiSP Advance Connect Excel
RAPID7 SECURITY DAY SINGAPORE
SECURING WHAT'S NEXT, TOGETHER
SECURITY DAY 2025
SINGAPORE
11 March Tuesday | 2:30pm - 6:00pm | NTUC Centre, One Marina Boulevard

Join us at the AiSP x Cyber Security Agency of Singapore (CSA) x Rapid7 Security Day Singapore on Tuesday, 11th March 2025, to gain an in-depth understanding of how the cyber threat landscape will evolve in 2025.

Special Guest Speaker
Hear from Veronica Tan, Director of the Safer Cyberspace Division at the Cyber Security Agency of Singapore (CSA). Her keynote, "From Risk to Resilience - Cybersecurity as Your Competitive Advantage," will explore strategies for leveraging cybersecurity to drive business resilience and success.

2025 Threat Predictions
Rapid7's CTO will reveal emerging threats and evolving attack vectors, offering actionable prevention tactics to help you stay ahead of cybercriminals and prepare for the challenges of tomorrow.

Spotlight on Emerging Fields
Discover the latest advancements in Continuous Red-Teaming (CTEM), Cyber Asset Attack Surface Management (CAASM), and Attack Surface Management (ASM) on the Rapid7 Platform. See how these cutting-edge approaches are simplifying risk and compliance management through practical, real-world use cases.

Register here

back to top

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
7 Feb	Bug Bounty Insights and Intro to Mobile App Pentesting	AiSP & Partner
10-14 Feb	Magnet Virtual Summit 2025	Partner
12-14 Feb	XCION 12th 2025	Partner
21 February	Youth Meetup at TIG Centre	AiSP
9 Mar	Ladies In Cyber Capture the Flag Competition	AiSP
9 Mar	Ladies in Cyber Symposium	AiSP
11 Mar	AiSP x Cyber Security Agency of Singapore (CSA) x Rapid7 Security Day Singapore	AiSP & Partner
20 Mar	Event with Emerotech	AiSP & Partner
24 – 27 Mar	Learning Journey to KL	AiSP

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

CONTRIBUTED CONTENTS

Article from CISO SIG

1. Introducing CISO with a deep interest in cybersecurity

Nyan Tun Zaw, CISSP, is serving dual roles as Chief Information Security Officer (CISO) as well as Senior Vice President at Athena Dynamics Pte Ltd, which is a subsidiary of BH Global Corporation Ltd, an SGX mainboard listed company. He is also currently serving as in the executive committee of ISC2 Singapore Chapter as Membership Director. With a wide range of background in cyber security operations, software development, web development, networking as well as business development, Zaw specializes in evaluating and analysing radically differentiated advanced cybersecurity technologies and has played critical roles in bringing technologies like high-speed DFIR or military grade file sanitisation technologies like content disarm & reconstruction to Singapore. During the early days as technical lead and head of good hackers alliance (gha), he

back to top

was also involved in various project implementations with Athena Dynamics in several highly confidential government and critical infrastructure projects in Singapore and the region.
Nyan Tun Zaw holds a Master of Business Administration from Quantic School of Business and Technology as well as Bachelor of Business Management, with double majors in Finance and Information Systems, from Singapore Management University. He is also a holder of CEH, ECSA and CISSP.

2. What brought you to the Cybersecurity industry?

It was an unexpected journey. I started as a web and C++ developer – creating and maintaining corporate websites and internal accounting system for BH Global (the parent company of Athena Dynamics) under the IT team. They were doing a large scale digital transformation at that time to sort out the IT and security of the group, brought in a Group CIO, and while doing do, they have stumbled upon really great cyber protection technologies that they feel will benefit Singapore's cybersecurity industry so ultimately decided to spin off the IT department as a cybersecurity company, serving both internal and external.

Naturally as part of the transformation, our Group CIO took on a dual role as CEO of this new spin-off that would become Athena Dynamics and I took up the role as a solution support / implementation engineer role. This was the start of my cybersecurity journey. The learning curve at the start was incredibly steep because I didn't have any background in cyber but now looking back, I'm glad I went through that because that provided me with accelerated hands-on learning opportunity for various aspects of cyber, having to work on a large number of highly sophisticated projects.

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

I would say winning the awards from NTUC MayDay Awards, Tech Talent Assembly and being nominated as a finalist in the "professional" category for The Cybersecurity Award by AiSP have given me the confidence and encouragement needed to keep pushing myself to contribute more to this profession and industry and I am very grateful to have been able to receive guidance from various veterans in the industry as well as the strong support and mentorship from my company's CEO.

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

I am blessed to be in a unique situation where I get the opportunity to deal with both internal and external cybersecurity challenges so everyday I am learning new things and constantly have to challenge myself to improve, which is something I love the most because I am a firm believer of lifelong learning. Especially in industries like cyber, there are new threats and attack methods coming out everyday so the moment we stop learning, our knowledge could become obsolete very quickly.

back to top

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

There are two distinct trends that I have seen in the market so far: Cyber for AI and protection against Quantum based threats

On cyber for AI, with the massive popularity of GenAI / LLM these days, everyone is using for almost every purpose that we could possibly think of and there are growing trends of attacks and techniques in this such as prompt injection, attack on the APIs, and poisoning the LLM itself. All these have huge impact on our day-to-day life and more people need to be aware of because LLM providers might not be fully equipped to have strong protections against these with the technology still being in rapidly evolving stage.

As for quantum based threats, its becoming more of a reality than theory that can fundamentally change a lot of encryption based security measures that we have in place today and we have seen technologies like quantum key distribution to counter against these attacks so its interesting to see how the industry will evolve going forward.

Alongside, I have also been seeing many innovations such as automated GRC tools enhanced by GenAI, high speed digital forensics technologies as well as even technologies that can make an organization undiscoverable (or in other words – invisible from the internet) and all these make our jobs as cybersecurity professionals much more interesting.

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

People say that an organization is often the reflection of its leader. Similarly, I believe that CISO, as the head of the security team, is an important senior management figure that plays a key part in how mature or protected an organization is against cyber threats. CISOs need to make sure that they are constantly updated with information about the latest threats, attack methods as well as how to protect against them so that they can set the right policies, start the right initiatives and lead the team effectively to ensure that the organization is well-prepared to defend against rising cyber threats because today cyber threats are not just a computer or technical problem. They have real business impact that can effect an organization in a critical way or in some cases, even in terms of people's safety (especially in OT sector).

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

Its encouraging to see that more people are taking cybersecurity seriously and we have been seeing more fresh graduates entering the workforce as well as mid-career changers coming into cyber. Based on my experience, having more industry initiatives to share more about what does a cyber security professional do day-to-day and even

back to top

fun initiatives like mass training and CTF events has inspired more people to join the cybersecurity sector because it helps people to understand what its like to be in cyber and what is needed. On the other hand, I am also seeing various tertiary institutions are starting to offer more cybersecurity focused diplomas or degrees so hopefully this could become more mainstream and help to attract more people to take up this career path.

Another thing is that cybersecurity certifications or trainings can typically be quite costly so if there are more programs or initiatives that can help to alleviate some of these concerns either via subsidies or even low-cost high-quality training sessions from the industry itself, this could potentially encourage more people to enter cybersecurity sector.

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

One thing that I love about this industry is that most people are willing to do knowledge sharing with each other. Everyone faced different situations and I believe that there are many things we can learn from each other's experiences so I'm glad to have been a part of such communities and would love to contribute more to facilitate these information flow. Also, through various industry thought leadership sharing be it at conferences / events or even like what we are doing now in this article, I hope to be able to inspire more people to join in the profession.

9. Any advice for the Cybersecurity Professionals?

As cybersecurity professionals, it is not an easy task to keep up with all the latest trends and technologies so its my belief that being active in communities like AiSP would be a great way to stay up to date and I would encourage everyone to share more, talk to each other more and learn more together because cyber is never an individual game but more of a collective team effort.

Article from AI SIG

Using Agents to Extend Capabilities of Large Language Models

Dr Leong Siang Huei is a Senior Lecturer at Nanyang Polytechnic's School of Information Technology. Prior to academia, he did R&D at both Government and private organisations, working on Artificial Intelligence, Machine Learning, Medical Robotics, Instrumentation, Building Automation and IoT. He has authored/co-authored more than 40 research papers in peer reviewed journals and 14 granted US Patents.

The power of Large Language Models (LLMs) today lies in their ability to process vast amounts of data and generate human-like text, enabling them to perform a wide range of tasks not limited to language translation, text generation and information retrieval. These models can understand context, generate coherent responses, and even perform reasoning tasks to some extent.

back to top

Limitation of Large Language Models

Today, LLMs on their own, powerful as they are, face challenges due to their limited ability to interact with the outside world. Some key limitations include:

- Real-World Interaction - LLMs may lack the ability to directly perceive and influence the real world. They are confined to processing information based on their training data and cannot interact with external systems or data.

- Static Knowledge - LLMs are like libraries with fixed training data. They may not be able to continuously acquire new information, which can lead to outdated or incomplete responses as real-world knowledge evolves.

- Reason and Act - LLMs can generate text but may struggle with reasoning and decision-making in complex scenarios. They lack the ability to select the right tools or take actions based on external inputs.

- Dynamic Data Access - LLMs may not access dynamic or real-time information, limiting their ability to provide up-to-date responses or perform tasks that require current data.

- Dependency on Training Data - LLMs are limited by what they have learned during training. They may not adapt well to new situations or tasks that go beyond their initial training data.

One approach to overcome the limitation of LLMs is to use Agents.

Extend LLM with Agents

Agents can play a crucial role in enhancing LLMs. For example, tools such as Data Stores, Extensions, and Functions may interact with LLM Models and provide agents with access to real-time information, external systems, and specialised capabilities, thereby enhancing the performance and reliability of LLMs[1].

The following describes the concept of agents, and extensions and their roles:

Agents

- are applications that observe the environment, act upon it, and can achieve goals independently. They can reason, plan, and execute tasks based on the tools available to them.
- can be proactive in reaching their goals and can make decisions based on the information they have.
- can manage session history, allowing for multi-turn interactions with users. They can use cognitive architectures like ReAct[2], Chain-of-Thought[3], or Tree-of-Thoughts to guide their reasoning and decision-making processes.

back to top

- may improve their performance over time through feedback and experience.

Extensions

- can bridge the gap between an agent and external APIs in a standardised way. They allow agents to seamlessly execute APIs regardless of their underlying implementation.
- may provide examples and parameters to teach agents how to use API endpoints effectively. They enable agents to dynamically select the most appropriate extension for a given task based on the provided examples.
- enhance the agent's ability to interact with external systems and access real-time information, expanding the range of tasks they can perform.

Thus a “LLM Powered Agent” can consist of an LLM serving as the agent’s brain, as well as key components for planning, memory and tool use[4]. In more complex systems, multi-agent architectures may also be considered.

Realising Agentic Behaviour

To realise agentic behaviour, popular LLM frameworks such as LangChain[5] or LlamaIndex[6] can be used. Some practical use cases that can deliver immediate value include Agentic RAG, report generation, customer support and SQL Agents.

Cybersecurity Implications

The integration of LLM agents in cybersecurity presents as a double-edged sword, offering powerful tools for both attackers and defenders. On the one hand, LLM agents can support automated threat detection and response in the context of threat identification, alert prioritisation, context-driven response generation, security policy enforcement, and threat handling[7]. On the other hand, LLM agents may also pose threats to cybersecurity. For example, teams of LLM agents can be used to exploit real-world, zero-day vulnerabilities.[8]

[1] Google whitepaper written by **Julia Wiesinger, Patrick Marlow and Vladimir Vuskovic,** https://www.kaggle.com/whitepaper-agents

[2] Yao, S. et al., 2023, ‘ReAct: Synergizing Reasoning and Acting in Large Language Models’, https://doi.org/10.48550/arXiv.2210.03629

[3] Wei, J. et al., 2023, ‘Chain-of-Thought Prompting Elicits Reasoning in Large Language Models’, https://doi.org/10.48550/arXiv.2201.11903

[4] Introduction to LLM Agents, https://developer.nvidia.com/blog/introduction-to-llm-agents/

[5] LangChain. https://python.langchain.com/v0.1/docs/modules/agents/

[6] LLamaIndex. https://docs.llamaindex.ai/en/stable/use_cases/agents/

[7] Molleti, R. et al., 2024, ‘Automated threat detection and response using LLM agents’, https://doi.org/10.30574/wjarr.2024.24.2.3329

[8] Fang R. et al., 2024, ‘Teams of LLM Agents can Exploit Zero-Day Vulnerabilities’. Available at: https://arxiv.org/pdf/2406.01637

back to top

Summary

By integrating reasoning, logic, and access to external information, LLM agents can make better decisions, engage with external systems, and produce responses or actions based on real-time data. This allows agents to manage complex tasks autonomously, extend the capabilities of language models, and deliver to users more accurate and reliable results.

Used ethically, LLM agents can bring much benefit. When developed and deployed responsibly, they have the potential to revolutionise various fields and improve our lives in countless ways, including and not limited to areas of Education, Healthcare, Environmental Science, and Social Good.

Contact Information: Leong Siang Huei (Dr)
School of Information Technology
Nanyang Polytechnic
E-mail: Leong_Siang_Huei@nyp.edu.sg

Article from SVRP 2024 Gold Winner, Rayden Leau Tian En [NYP]

Organised by
AiSP Association of Information Security Professionals
CSA SINGAPORE
EC-COUNCIL
REPUBLIC POLYTECHNIC
STUDENT VOLUNTEER RECOGNITION PROGRAMME
2024 AWARDS

How SVRP has directly impacted your cybersecurity journey?
SVRP has given me motivation and a form of recognition for my contributions to cybersecurity which has improved my standing within the community.

back to top

How SVRP has inspired them to contribute to the cybersecurity field?
I wouldn't say SVRP has directly inspired me to contribute to the cyber field. I've always wanted to contribute to cyber, SVRP is just a happy side effect.

What motivates you to be a student volunteer?
To see other people succeed and be able to learn from each other.
How would you want to encourage your peers to be interested in cyber security?
Hold more CTFs, workshops to give practical experience. I feel that practical experience is the best motivator and interest maker for cyber.

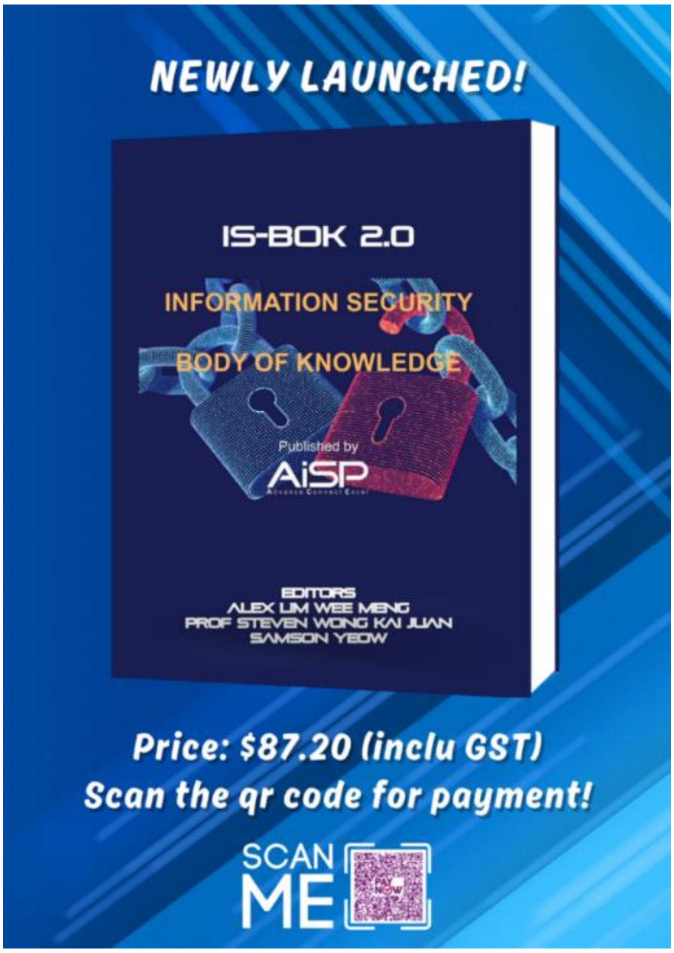
back to top

PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®)

Body of Knowledge Book (Limited Edition)

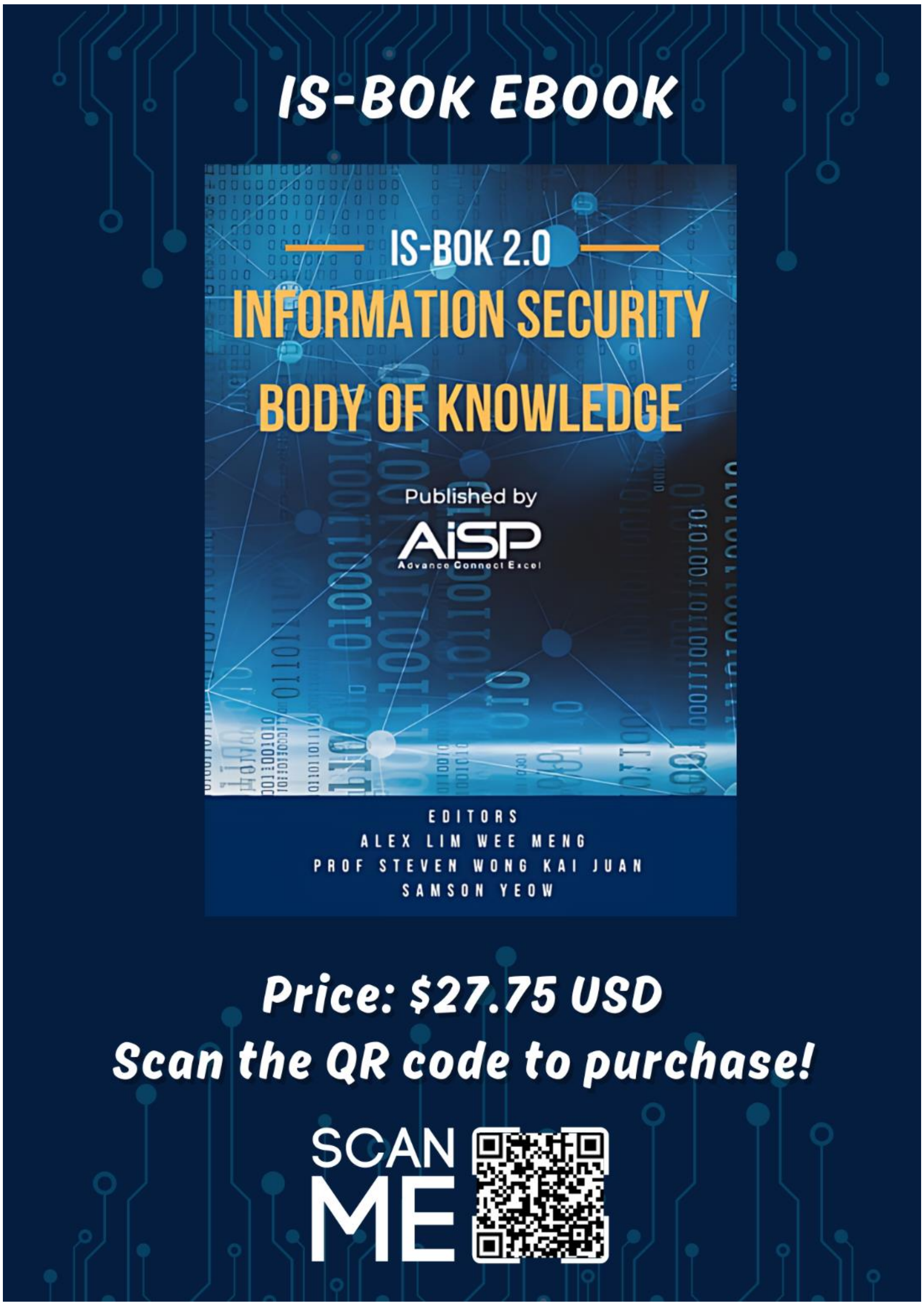
Get our **Limited Edition** Information Security Body of Knowledge (BOK) Physical Book at **$87.20 (inclusive of GST)**.



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



IS-BOK EBOOK

IS-BOK 2.0

INFORMATION SECURITY BODY OF KNOWLEDGE

Published by AiSP Advance Connect Excel

EDITORS

ALEX LIM WEE MENG

PROF STEVEN WONG KAI JUAN

SAMSON YEOW

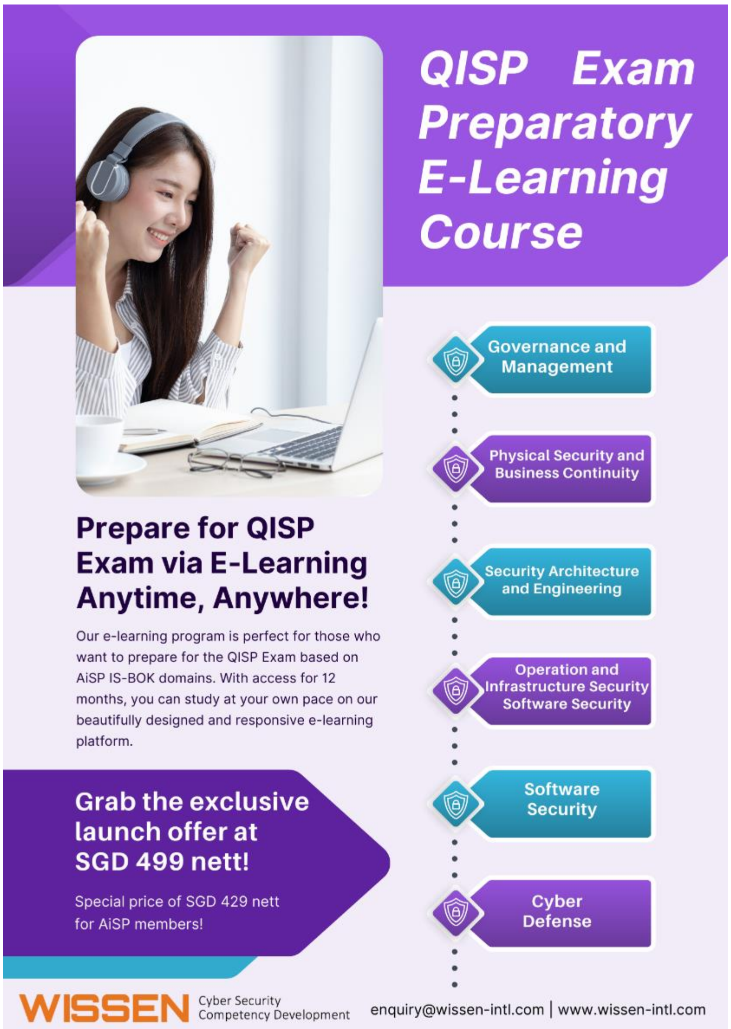
Price: $27.75 USD

Scan the QR code to purchase!

SCAN ME

back to top

Online QISP Exam Preparatory Course



QISP Exam Preparatory E-Learning Course

Prepare for QISP Exam via E-Learning Anytime, Anywhere!

Our e-learning program is perfect for those who want to prepare for the QISP Exam based on AiSP IS-BOK domains. With access for 12 months, you can study at your own pace on our beautifully designed and responsive e-learning platform.

Grab the exclusive launch offer at SGD 499 nett!

Special price of SGD 429 nett for AiSP members!

- Governance and Management
- Physical Security and Business Continuity
- Security Architecture and Engineering
- Operation and Infrastructure Security Software Security
- Software Security
- Cyber Defense

WISSEN Cyber Security Competency Development enquiry@wissen-intl.com | www.wissen-intl.com

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!

back to top

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

Join our Corporate Partner Programme for exclusive benefits and partnership with AiSP

Contact AiSP Secretariat for the benefits and corporate pricing at secretariat@aisp.sg

For any enquiries, please contact secretariat@aisp.sg

back to top

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
athena dynamics
AZ ASIA-PACIFIC
BD
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

back to top

HORANGI CYBER SECURITY

HTX

HUAWEI

illumio

image engine

INTfinity

ITSEC ASIA

KnowBe4 Human error. Conquered.

MAGNET FORENSICS®

M.TECH Your Preferred i-Security Partner

NAYUTAL PTE. LTD.

ONESECURE®

opentext™

OPSWAT.

proofpoint.

RAJAH & TANN CYBERSECURITY

RAPID7

RSM

SailPoint.

SCANTIST

Schneider Electric

Security Scorecard

Singtel

softScheck We Build Trust

ST Engineering

TEMASEK

tenable

TREND MICRO™

Veracity Trust Network

VOTIRO

WISSEN Cyber Security Competency Development

wizlynx group

YesWeHack

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

back to top

AiSP Academic Partners

ITE Institute of Technical Education

NYP NANYANG THE INNOVATIVE POLYTECHNIC

NGEE ANN POLYTECHNIC

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

NUS National University of Singapore

REPUBLIC POLYTECHNIC DISCOVER. TRANSFORM. ACHIEVE

SiT SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek POLYTECHNIC

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.

back to top

AiSP Secretariat Team

Terence Siau
Director

Vincent Toh
Associate Director

Elle Ng
Senior Executive

Karen Ong
Executive

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

back to top