

## News & Update

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

## Contributed Contents

- AI SIG: Artificial Intelligence 101
- Quantum Security SIG: Establishing a Quantum Security Special Interest Group within AiSP SG
- SVRP 2023 Gold Winner, Su Myat Naing [RP]

Professional Development Membership

## NEWS & UPDATE

### New Partners

AiSP would like to welcome Nayutal as our new Corporate Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partner



NAYUTAL PTE. LTD.

### Continued Collaboration

AiSP would like to thank Cisco and Grab for their continued support in developing the cybersecurity landscape:



# Member Acknowledgment

## Interview with AiSP EXCO Member Mr Yu Pengfei



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

The huge disconnect between academic training and practical professional demands is a major issue facing the cybersecurity sector today. My goal as a new member of the EXCO is to encourage young people and build strong foundations for future potential. I am a big supporter of creating safe spaces where students may test out new security ideas and technology before joining the job.

AiSP's SVRP initiative has already advanced this area significantly with a number of workshops and other activities. Our popular Bug Bounty Workshop series has given aspiring security researchers practical experience and taught them the fundamentals of vulnerability discovery and ethical disclosure. As SVRP look to 2025, we are stepping up these efforts with innovative new partnerships with communities like Div0-N0H4TS. We will be launching a series of workshops and meetups to explore different domains of cybersecurity. Do keep a lookout!

### **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?**

As a member of the EXCO and the SVRP Lead, I'm dedicated to serving as a powerful spokesperson for the principles and goals of AiSP and the SVRP initiatives. I hope to help AiSP establish itself as the association that backs imparting practical knowledge and building a more skillful student population that will advance into our professional talent pool. I would do my best to ensure that AiSP can maintain its position as a reliable voice in the cybersecurity community.

**Lastly, what would you like to share and contribute your expertise with our AiSP member and the wider community?**

My main contribution to the AiSP community will be to share my knowledge of purple teaming and adversary emulation to push the boundaries of cybersecurity maturity. I would like to share a few articles that deep-dives into automated adversary emulation and its critical role in creating strong detection development capabilities.

By consistently contributing to AiSP's online resources and publications, I will offer my perspectives on:

- Currently used methods for automated adversary emulation
- Case examples from the real world and insights gained from purple team operations
- Best practices and new developments in defensive capacities

My goal is to create practical, readable content that helps companies understand and implement effective security testing practices. I believe in "dumbing down" complex security concepts not to oversimplify them, but to make them more accessible and actionable. This approach will help companies and professionals make well-informed decisions about their security programs and establish meaningful metrics for measuring success.

By sharing information through written content and speaking engagements, we can all collaborate to improve cybersecurity practices in Singapore and beyond. The goal of this knowledge-sharing effort is to make complicated security concepts more understandable while also fostering a culture of continuous learning within our cybersecurity community. Through clear communication and practical guidance, we can help organizations move beyond checkbox compliance to achieve genuine security maturity.

# Student Volunteer Recognition Programme (SVRP)

## Learning Journey to Cisco on 12 November

AiSP brought 10 Students from Raffles Institution on a Learning Journey visit to our Corporate Partner, CISCO on 12 November. We hope that the students managed to capture new insights from the experience.

Thank you Cisco for hosting!



## SVRP IHL Briefing on 26 November

AiSP held our SVRP IHL Briefing on 26 November where SVRP EXCO Lead, Mr Yu Pengfei shared on the updated judging criteria on SVRP. Mr Freddy Tan and Mr Breyvan Tan also shared on QISP E-Learning and Exam.

The SVRP nomination for 2025 has started from 1 Aug 2024 - 31 Jul 2025. Feel free to reach out to [SVRP@aisp.sg](mailto:SVRP@aisp.sg) for submission.



## Learning journey to i-Sprint Innovations Pte Ltd on 29 November

On 29 November, a group of 20 students from Nanyang Polytechnic visited i-Sprint Innovations Pte Ltd for a learning journey at their office. During the visit, i-Sprint CEO, Mr Dutch Ng shared with the students on his personal experience in Cybersecurity and tips on building a Cybersecurity career path. The students also got a firsthand look at the office environment, gaining a sense of what it's like to work there. We hope this experience provided the students with valuable insights to guide them on their career paths.



## SVRP Awards Ceremony on 19 November

AiSP Student Volunteer Recognition Programme (SVRP) Awards Ceremony (Sixth Edition) was held on 19 November with more than 300 students, parents and guests attended the ceremony. We received a record-breaking of 456 nominations, our highest ever for the past 5 years for this year SVRP nominations. Of the 456 nominations, 110 students were awarded the Bronze Award, 44 Students were awarded the Silver Award, 7 Students were awarded the Gold Award and for our secondary & college students, 75 Certificate of Merit award were awarded to them. The number of award recipients increased more than twofold, by over 70% from 135 winners last year to 236 winners this year.



Thank you AiSP Patron, Senior Minister of State for Ministry of Digital Development and Information, Mr Tan Kiat How for gracing the ceremony and presenting the Gold awards to the 7 students. Thank you Mr Selwyn Scharnhorst for presenting the Silver awards to the students. Thank you AiSP Secretary, Ms Soffenny Yap for giving the welcome address and presenting the Bronze Awards to the students. Also thank you to Ms Judy Saw for presenting the Certificate of Merit to the Secondary & JC students.

We would like to thank our Academic Partner, Republic Polytechnic (RP) for hosting us at their beautiful premise. Thank you to Cyber Security Agency of Singapore (CSA) and Wissen International for supporting to make the awards ceremony possible.

During the SVRP Awards Ceremony, AiSP also signed an MoU with RP to foster collaborative initiatives that enhance the learning and professional development of RP students and staff. This partnership will open doors for various programmes, including internships, Final Year Projects (FYP) and Capstone Projects, staff-led projects, and staff attachment opportunities.

Once again congratulations to all award winners and we looked forward to your participation in our Youth Activities and SVRP Programme in 2025.




## AiSP Youth Meetup – Bug Bounty on 8 January

### AiSP Youth Meetup – Bug Bounty



## Youth Meetup


### Bug Bounty



**Chai Li Xian**  
Cybersecurity Engineer  
GovTech Cyber Security Group

Organised by







Wednesday  
8 Jan 2025



Start At  
6:00PM - 8:30PM


SIT Punggol Campus



**Matthew Ng**  
Senior Information Security Analyst  
Roche Singapore

Supported by



REGISTER NOW

AiSP will be organising a Youth Meetup on 8 Jan 2025 focusing on Bug Bounty. Through this meetup, we are expecting 80 Youths and young professionals for where:

- Interaction and learning with fellow Cyber youths, Government Agency, Professionals and Industry Leaders through networking
- Understanding the Cybersecurity Landscape on the demand in talent, market trends, job demand and skillset required for the industry through talks and panel discussion.
- Providing a platform for our Youths to be engaged and feedback on what they feel that they need in Cyber and how the Association or Government can help them in it.
- Motivation from Industry Expert Leader to motivate Youth to continue their journey in Cybersecurity.

### **Building Resilient Cybersecurity: Organizational Strategies, Capabilities and Career Pathways in the Public Sector**

Speaker: Ms Chai Li Xian, Cybersecurity Engineer, GovTech Cyber Security Group

This session will provide a glimpse into GovTech's Cyber Security Group, its strategies and capabilities in tackling cyber threats against the Whole of Government IT infrastructure. It will highlight real-world projects and share insights into how these capabilities help improve our security posture. This session will also offer some advice for those looking to start a career in cybersecurity, covering essential skills, certifications, and tips for success in this field.

## **How a Small Team Protects a Global Giant**

Speaker: Mr Matthew Ng, Senior Information Security Analyst, Roche Singapore

This session offers an in-depth look at how a small team manages a vast bug bounty program across a multinational organization. We'll share our approach to triaging submissions, scaling security efforts, and dealing with the unexpected. Expect to hear stories of our biggest wins, toughest hurdles, and lessons learned on the fly.

Date: 8 January 2025, Wednesday

Time: 6:00PM – 8:30PM

Venue: SIT Punggol Campus

Registration: <https://forms.office.com/r/rAQm09VXmq>

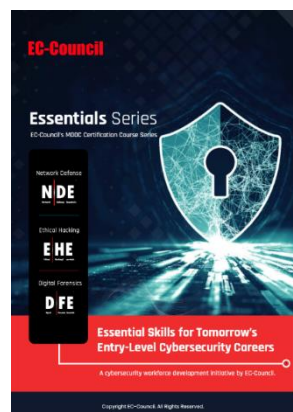
## **Elevating Cybersecurity Education Through Unprecedented Collaborations**

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](mailto: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](mailto:secretariat@aisp.sg)



## AiSP CISO SIG Meetup – The Role As a CISO on 5 November

It was an insightful evening on 5 November at the AiSP CISO SIG Meetup with more than 50 participants, where our panel delved into the critical elements of securing supply chains and ensuring robust security throughout the product lifecycle. Thank you Mr Andre Shori, Mr Bernard Tan, Mr Dennis Chan, and Ms Lee Shu Ping for sharing valuable insights on crafting a holistic security framework that addresses both cyber and product security from ideation to decommissioning. And a big thank you to Huawei for supporting the event!



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

The evening will kick off with a thought-provoking presentations by our line up of speakers, setting the stage for an intellectual journey into the heart of AI vulnerabilities and defenses. Attendees will gain insights into the latest adversarial attacks on AI models, delve into the nuances of privacy preservation in AI systems, and explore ethical considerations in AI development and deployment.

The event will culminate in an interactive Q&A session, encouraging attendees to engage directly with our speakers and fostering the collaborative spirit that both AiSP and OWASP hold dear. This open dialogue will not only address current challenges but also spark discussions on future trends and potential solutions in AI security. Join us for an evening of enlightenment, engagement, and empowerment as we collectively work towards a more secure AI-driven world. Together, we'll explore how to build unassailable fortresses in the cognitive realm, ensuring that as AI advances, our defenses evolve in tandem.

**Synopsis:**

In the rapidly evolving landscape of artificial intelligence, where Large Language Models (LLMs) and advanced AI systems are reshaping our digital world, the need for robust security measures has never been more critical. The Association of Information Security Professionals (AiSP) and the Open Web Application Security Project (OWASP) proudly present "Safeguarding the Future of Artificial Intelligence" an enlightening evening session that bridges the gap between AI innovation and cybersecurity. This event embodies the shared values of AiSP and OWASP – fostering knowledge sharing, promoting best practices, and nurturing a vibrant community of security-conscious professionals.



**Securing AI systems: An overview and the lifecycle approach**

Speaker: Mr Loh Chee Keong, Lead Consultant for AI Security, Cybersecurity Engineering Centre, Cyber Security Agency of Singapore

**OWASP Top 10 on LLMs**

Speaker: Mr Wong Onn Chee, OWASP SG Chapter Co-Leads & AiSP Data & Privacy SIG EXCO Lead

Date: 15 January 2025, Wednesday

Time: 6:30pm – 8:30pm

Venue: 6 Raffles Boulevard, JustCo, Marina Square, #03-308, Singapore 039594

Registration: <https://www.eventbrite.sg/e/aisp-ai-sig-meetup-tickets-107626552239?aff=oddtcreator>

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

AiSP DevSecOps Special Interest Group aims to provide a learning journey for students, practitioners and industry professionals with a community to share their knowledge and expertise with one another. We want to highlight the importance of having strong security built into the software development process rather than rely on external protection. While such security solutions are still required, we would also like to have software that has security 'baked in' rather than trying to patch vulnerabilities and insecurities after it is deployed.

The "Learning Journey" event is designed to provide information to developers, project managers, students, practitioners & decision-makers who are interested in making their processes more secure during the development of their applications – whether it's inhouse developed or outsourced to 3rd party development teams. In the end,

[back to top](#)



knowledge is KEY to be able to have the right conversations with the development teams.

Attendees will get to hear about how to get started with DevOps and putting Sec[urity] into DevOps to become DevSecOps. We want to promote the different tools and solutions – whether they be OpenSource or Commercial tools so that the users will have a choice to decide what fits in their organization. Also, we want to have organizations understand the Benefits & Pitfalls in transitioning to a DevSecOps setting. So that they will understand the commitment and the support that is needed in order to succeed. Finally, we will want to address the use of Artificial Intelligence and Cloud solutions to enhance and extend the ability to make their applications more secure.

During this event, we are excited to have Checkmarx, a leader in Application Security, joining us. This is a fantastic opportunity to network and learn more about the critical role of application security, and how to build an AppSec program trusted by DevSecOps teams worldwide.

Date: 22 January 2025, Wednesday

Time: 6:30pm – 8:30pm

Venue: Lifelong Learning Institute, Paya Lebar, 11 Eunos Rd 8, Singapore 408601

Registration: <https://www.eventbrite.sg/e/aisp-devsecops-sig-meetup-tickets-1076269243279?aff=oddtcreator>

# The Cybersecurity Awards



The Cybersecurity Awards (TCA) 2024 has officially concluded on 7 November 2024. Congratulations to all The Cybersecurity Awards (TCA) 2024 winners! Thank you AiSP Patron - SMS Tan Kiat How for joining us to celebrate the achievements of the winners and present the awards to them.

AiSP would like to thank Cisco, Cyber Security Agency of Singapore (CSA), Huawei, ST Engineering, for their kind sponsorship as Platinum Sponsors, BeyondTrust, DBS Bank, Ensign InfoSecurity, Grab, SANS Institute, Singapore Institute of Technology, Trend Micro, Wissen International and wizlynx group for their kind sponsorship as Gold Sponsors for TCA 2024. Thank you for your support to make TCA24 a success. Thank you for contributing to the Cybersecurity Ecosystem.

Sponsorship for The Cybersecurity Awards 2025 is now open, contact the AiSP Secretariat at [secretariat@aisp.sg](mailto:secretariat@aisp.sg) if you are interested in it.





## Ladies In Cyber

### Visit from Cardiff University to AiSP Office on 12 November

AiSP Ladies in Cyber EXCO Lead, Ms Judy Saw met up with the representatives from Cardiff University on 12 November and shared about our Ladies in Cyber Charter Initiative. Thank you, Ms Yulia Cherdantseva and Ms Angharad Watson for visiting us.



## SHE Supports Friendship Circles: Ladies in Cybersecurity on 7 December



AiSP Ladies in Cyber is excited to present SHE Supports Friendship Circles: Ladies in Cybersecurity, in partnership with NTUC U Women and Family (U WAF) and SG Her Empowerment (SHE)!

This informal session aims to foster a supportive community for female students and professionals at all stages of their cybersecurity careers. Participants will have the opportunity to connect, share experiences, and receive guidance from women mentors and industry leaders on topics such as balancing career and personal life, navigating career transitions, and overcoming challenges.

Join us to be empowered to thrive and lead in the cybersecurity industry!

Date: 7 December 2024, Saturday

Time: 2PM – 5PM

Venue: Lifelong Learning Institute

Registration: <https://forms.office.com/r/bQw8Pf4gmu>



# Digital For Life

## Digital for Life Festival at Heartbeat@Bedok on 2-3 November

AiSP was at Digital for Life Festival at Heartbeat@Bedok on 2 and 3 November. Thank you AiSP Patron, Mr Tan Kiat How and Grassroots Advisor, Ms Ng Ling Ling for visiting our booth. Thank you, Mr Dennis Chan for hosting them.



## DFL SilverTech Carnival at Senja Hawker Centre on 23 November

AiSP was at Senja Hawker Centre for the SilverTech Carnival on 23 November. Thank you Member of Parliament, Mr Edward Chia for visiting our booth.





# Regionalisation

## UK Cardiff University visit to SIT on 11 November

UK Cardiff University visited Singapore Institute of Technology on 11 November for a time of exchange and networking.



# Corporate Partner Event

## **AiSP x wizlynx group x KnowBe4 – The Human Factor: Your Strongest Defence Against Next-Gen Cyber Threats on 14 November**

On 14 November, AiSP organised an event with our Corporate Partners, wizlynx group and KnowBe4 with about 30 attendees. Thank you Mr Leow Kim Hock for giving the opening and our speakers Mr Paul Lee and Mr Jason Tay where they shared insights on the Human Factor: Your Strongest Defence Against Next-Gen Cyber Threats. We hoped that the audience gain insights from sharing and interactive discussion.



## 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 Dec	SHE Supports Friendship Circles: Ladies in Cybersecurity	AiSP & Partner
13 Dec	RP Community Day	Partner
16-19 Dec	Learning Journey to KL for LIC	AiSP
8 January	Youth Meetup	AiSP
15 January	AI SIG Meetup	AiSP
22 January	DevSecOps Meetup	AiSP

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

# CONTRIBUTED CONTENTS

## Article from AI SIG

### Generative AI and Large Language Models

Dr Liang Nanying is a Lecturer at Nanyang Polytechnic's School of Information Technology. Dr Liang has more than 15 years of experience in Machine Learning and Artificial Intelligence, both in research and industry applications. Before joining Nanyang Polytechnic, she was a Senior Research Fellow at Subaran Jurong - Nanyang Technological University Joint Corporate Lab, focusing on applications of AI and robotics for Building Information Modelling.

In recent years, Generative Artificial Intelligence (AI) has revolutionized various fields by enabling machines to create and simulate human-like content. From text and code generation, realistic images and video creation to 3D scene reconstruction<sup>1</sup>, 3D protein structure prediction<sup>2</sup>, generative AI has the potential to reshape industries and redefine the way we interact with technology. At the core of many modern generative AI

<sup>1</sup> Avetisyan et al.(2024), "SceneScript."

<sup>2</sup> Abramson et al.(2024), "Accurate Structure Prediction of Biomolecular Interactions with AlphaFold 3."

systems is the backbone of Large Language Models (LLMs), which are capable of understanding and generating human language.

In this article, we will introduce generative AI and its applications, then transition to LLMs, focusing on autoregressive language models. We will explain how they work by examining their autoregressive and attention mechanisms. Lastly, we will discuss adopting LLMs in application development, emphasizing aspects of application content, the data and the model.

### What is Generative AI?

Unlike traditional AI models that focus on recognizing patterns or making predictions based on input data, generative AI models learn the underlying distribution of the training data and use it to produce output. These output can take various forms, including text, images, video, music, audio, and even complex data structures like software code, scene scripts and protein structure descriptions.

Through training with a plethora of data and extensive computing time, generative AI models understand the statistical properties and patterns within the training data to produce realistic and coherent output. And with instruction fine-tuning, generative AI can follow human instructions and intentions to create new content and even collaborate with designers and artists in co-creating architectural layouts, paintings, and music compositions.

There are a few types of generative AI models commonly found: Autoregressive Models, Diffusion Models, Generative Adversarial Networks (GANs), and Variational Autoencoders (VAEs).

### Common Types of Generative AI Models

**Autoregressive Models:** These models generate data one step at a time, with each step conditioned by the previous output. They model the probability distribution of a sequence by breaking it down into a product of conditional probabilities.

Autoregressive models have shown impressive results in human-like language generation, and examples include OpenAI's Generative Pre-trained Transformer (GPTs) and Recurrent Neural Networks (RNNs).

**Diffusion Models:** Diffusion models are used for high-quality images and video synthesis from text prompts. These models learn to generate data by reversing a gradual noising process. During training, noise is incrementally added to the data, and the model learns to reconstruct the original data from the noisy versions. At generation time, the model starts from random noise and iteratively denoises it to produce new data samples. Diffusion models have shown remarkable results in image and audio generation. Examples include SORA, DALL-E 2/3 and Stable Diffusion.

**Generative Adversarial Networks (GANs):** Consist of two neural networks—the generator and the discriminator—that are trained simultaneously through adversarial processes.

The generator creates fake data, while the discriminator evaluates it against real data, pushing the generator to produce increasingly realistic outputs.

Variational Autoencoders (VAEs): Encode input data into a latent space and then decode it to reconstruct the data. VAEs can generate new samples by sampling from the latent space.

### Applications of Generative AI

Depending on its output format, generative AI has applications across different domains, mainly including natural language processing, computer vision, and audio synthesis. Here are a few examples:

- Natural Language Processing (NLP): Large language models, such as GPTs, Llama and Qwen, are used to generate human-like text, making them suitable in applications like chatbots, content creation, and translation services.
- Code Generation: Generative AI can write code, assist in software development, and create scripts for various tasks, significantly reducing the workload for programmers.
- Image and Video Generation: AI models like DALL-E 2/3 and SORA can generate realistic images and videos, which are useful in design, entertainment, and marketing.
- Creative Arts: From music composition to visual art, generative AI is used by artists and creators to push the boundaries of creativity.

Notably, the newly launched OpenAI o1, a new series of LLMs trained with reinforcement learning, generates a detailed internal chain of thought before arriving at an answer. OpenAI o1 demonstrates an IQ score of 120, placing it in the top 15% of human intelligence, and can answer graduate-level scientific questions, which pushes LLMs to unprecedented heights of capability in reasoning.

### Application Development Using LLMs:

Successful adoption of LLMs requires careful consideration of three critical aspects: application content, data, and the model.

Understanding the content of your application is fundamental. It helps in defining problem statements and constructing the solution pipeline. By examining the solution pipeline and refining it in response to application requirements and available advanced techniques, you can identify which components or modules are suitable for adopting machine learning methods or generative AI models such as LLMs.

The next critical aspect to consider is data. This includes not only access to data but also evaluating its quantity, quality and diversity. LLMs accept tokens as its inputs.

Leveraging the capabilities of these models involves encoding different input formats into tokens. Natural languages can be tokenized, images can be converted to tokens, and even complex sequences like amino acids can be represented as tokens, as demonstrated by AlphaFold 2 and 3, which has been recognized in this year's Nobel



Prize in Chemistry. Different types of data require different tokenization strategies, from simple to complex ones.

Once the content and data are fully understood, it is important to evaluate which components in the application's solution pipeline are suitable for adopting LLMs techniques. Selecting appropriate model architecture is crucial. This may involve using pure LLM architecture, combined vision-language models (VLMs), or other multi-modal models depending on the type of input data and the intended outputs.

There are several constraints to consider when deploying applications using LLMs, including model size, hallucination, and data privacy. Firstly, the size of large language models ranges from a few million parameters to several trillion. Selecting the appropriate model size requires balancing computational resources with desired performance. Secondly, one of the challenges when using LLMs is their potential to generate hallucinations—incorrect or fabricated information. Existing methods, such as retrieval-augmented generation (RAG) and graph-based LLMs, can mitigate hallucinations to some extent. However, for critical applications, it is essential to have subject matter experts involved in the application loop to validate LLM outputs. Thirdly, if data privacy is a primary concern, it may be advisable to use open-source LLMs instead of closed-source models. Open-source models provide greater transparency and control over data handling, reducing the risks associated with data privacy.

Generative AI presents incredibly promising opportunities for application development across various domains, including industry, healthcare, legal and even accelerating scientific research. Successful integration of generative AI and LLMs requires careful consideration and understanding of application content, data and models. For real-world applications, concerns like hallucination and data privacy need to be carefully addressed. By thoroughly understanding these aspects, we can harness the full potential of generative AI and LLMs to create powerful, transformative solutions, push boundaries in AI and accelerate innovation.

## References:

- Abramson, J., Adler, J., Dunger, J., Evans, R., Green, T., Pritzel, A., ... & Jumper, J. M. (2024). Accurate structure prediction of biomolecular interactions with AlphaFold 3. *Nature*, 1-3.
- Avetisyan, A., Xie, C., Howard-Jenkins, H., Yang, T. Y., Aroudj, S., Patra, S., ... & Balntas, V. (2024). SceneScript: Reconstructing Scenes With An Autoregressive Structured Language Model. *arXiv preprint arXiv:2403.13064*.
- Dubey, A., Jauhri, A., Pandey, A., Kadian, A., Al-Dahle, A., Letman, A., ... & Ganapathy, R. (2024). The llama 3 herd of models. *arXiv preprint arXiv:2407.21783*.

Contact Information: Liang Nanying (Dr)  
School of Information Technology  
Nanyang Polytechnic  
E-mail: [liang\\_nanying@nyp.edu.sg](mailto:liang_nanying@nyp.edu.sg)

# Article from Quantum Security SIG

## Establishing a Quantum Security Special Interest Group within AiSP SG

### Overview

AiSP is establishing a Special Interest Group (SIG) - **Quantum Security** with the following objectives:

1. Create awareness on the impact of Quantum Security, including both opportunities and threats.
2. Engage with various agencies to promote Quantum-Safe initiatives in the local industry.
3. Facilitate discussions and knowledge sharing among members to enhance preparedness for quantum-based security challenges.
4. To collaborate with industry experts to develop best practices.

This SIG aims to help members navigate the evolving landscape of quantum technologies in information security and beyond.

### Charter

1. **Thought Leadership:** Working with thought leaders to create awareness and develop best practices and white papers related to Quantum Security.
2. **Community Building:** To build a cohesive community of like-minded information security professionals who wish to collaborate and create a better and more robust quantum security environment.
3. **Engagement with Stakeholders:** Given that Quantum-Safe initiatives have a nationwide implication, it is crucial to engage with stakeholders such as CSA, IMDA and NQSN (National Quantum-Safe Network).
4. **Skills Development:** Organise seminars, workshops and bespoke training to bridge the skills gap of information security professionals to be better prepared for quantum-based security challenges.

The ideal target audience are experienced information security professionals, academics, developers and forward-thinking individuals who would like to start early and potentially play an integral role in future proofing the evolving landscape of quantum technologies.

## Activities

**Thought Leadership:** Working with thought leaders and industry experts to create awareness and develop white papers on quantum-based security. This includes the production of articles, informative charts, diagrams, short videos and others.

**Seminars / Webinars and Panel Discussions:** Invite industry experts (both local and international) to share on latest developments and best practices on quantum technologies and to organise panel discussions with local agencies and stakeholders to support national Quantum-Safe initiatives.

**Workgroup Meetings:** Organise in person workgroup meetings to keep interested members engaged and to learn from one another in the emerging area of quantum-based security.

## Membership

Membership in the Quantum Security SIG will be open to all AiSP members with an interest in quantum technologies, including but not limited to security professionals, academics and developers. Non-members interested in Quantum Security may also participate in SIG activities as guests.

**Leadership:** The SIG will be led by a steering committee comprising of experienced professionals from the Quantum Security and Quantum-Safe community in Singapore. The committee will be responsible for setting strategic direction, planning activities and ensuring effective running and growth of the SIG.

## Process

As a start, I manage to obtain high level support from a few local and international domain experts in quantum technologies and a core team / steering committee of senior AiSP members including the support from the top leadership of Horangi (a Bitdefender Company) as a potential sponsor and steward to carry out our initial activities.

Of course, we will continue to engage with more linked minded AiSP members / companies as soon we get the SIG started with build some positive traction. Concurrently, we will immediately commence our engagement with the following stakeholders:

1. **CSA** – Cyber Security Agency Singapore
2. **IMDA** – Infocomm Media Development Authority
3. **NQSN** - National Quantum-Safe Network
4. **SIT** – Singapore Institute of Technology
5. **Other related Institutions and Universities**

## Conclusion

The establishment of a Quantum Security Special Interest Group within AiSP Singapore will provide a platform for information security professionals, academics, and industry experts to collaborate, learn, and address the challenges and opportunities in quantum

technologies. By promoting Quantum-Safe practices and preparing for the future of quantum-based security the SIG will play a key role in safeguarding Singapore's digital landscape. We look forward to your support in making this initiative a success.

## Article from SVRP 2023 Gold Winner, Su Myat Naing [RP]



### **How do you think SVRP has directly impacted your cybersecurity journey?**

Svrp has been such a huge impact on my journey, allowing me to volunteer whilst gaining further knowledge/interest in this industry.

### **How has SVRP inspired you to contribute to the cybersecurity field?**

I found it really inspiring to see student volunteers being shown recognition through the svrp award in the cybersecurity sector in Singapore. This motivated me so much more knowing that wow, what I enjoy doing is appreciated & recognised in the cyber security industry.

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

I am motivated to be a student volunteer for cybersecurity in Singapore as I believe in the importance of securing our digital landscape. By volunteering, I can actively contribute to the cybersecurity industry that I am so interested in & possibly make even the slightest bit of impacts in this industry. Not only this, I find it fulfilling to possibly get others to gain interest in this field to possibly pursue in the future & actively continue this lifecycle like possible volunteering as I have been doing currently.

### **How would you want to encourage your peers to be interested in cybersecurity?**

In order to encourage my peers to develop an interest in cybersecurity in Singapore, I would employ a multifaceted approach. Firstly, I would emphasize the critical importance of cybersecurity by highlighting its role in safeguarding personal data,

[back to top](#)

businesses, and national security. I would then use real-world examples, such as recent cyberattacks and their consequences, to illustrate the immediate relevance of cybersecurity in our lives. To make it more tangible, I'd suggest various learning resources, like online courses and tutorials, to help them get started. Additionally, I believe in the power of hands-on experience. I would organize workshops, talks, and even ethical hacking demonstrations to provide practical insights and engage their curiosity. Encouraging participation in Capture The Flag (CTF) competitions can add an element of competition and fun to the learning process. To foster a sense of community, I would suggest forming a cybersecurity club or group where peers can collaborate, share knowledge, and support each other's learning journey. Bringing in guest speakers who are professionals in the field would further expose them to real-world experiences and career opportunities. Next, I'd stress the promising career prospects in cybersecurity and the high demand for professionals in Singapore, motivating them with the potential for a fulfilling and lucrative career. Staying updated on the latest cybersecurity trends and threats would also keep their interest alive. Lastly, I would share my personal experiences in this sector that I have experienced so far being a Student. All in all, I believe this holistic approach would effectively encourage my peers to pursue an interest in cybersecurity.

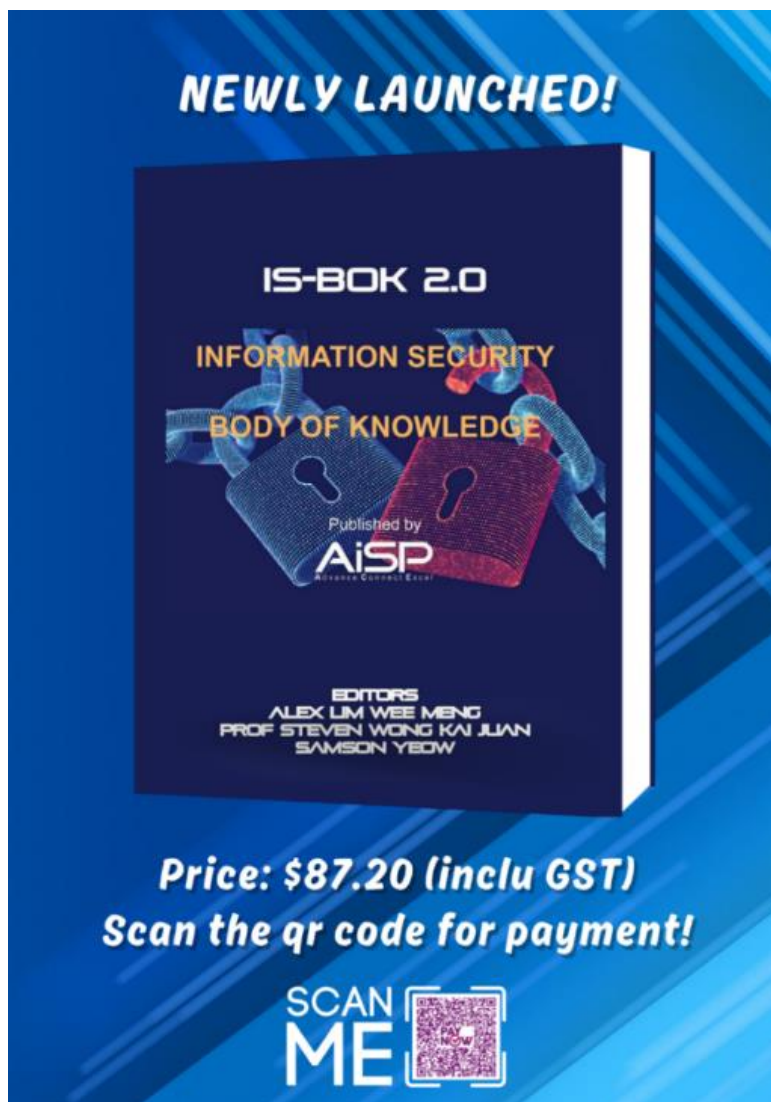


# PROFESSIONAL DEVELOPMENT

## 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](mailto: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**



**Online Course launched on 1 March 2024!**

## 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!](#)

# 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](mailto:secretariat@aisp.sg)

For any enquiries, please contact [secretariat@aisp.sg](mailto: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](mailto: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](http://www.aisp.sg/membership.html)

## AiSP Corporate Partners

Acronis

athena  
dynamics



[back to top](#)



**xcellink.pte.ltd.**  
completing your technology chain

**YesWeHack**

Visit [https://www.aisp.sg/corporate\\_members.html](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.

## AiSP Secretariat Team



Terence Siau  
Director



Vincent Toh  
Associate Director



Elle Ng  
Senior Executive



Karen Ong  
Executive



[www.AiSP.sg](http://www.AiSP.sg)



[secretariat@aisp.sg](mailto:secretariat@aisp.sg)



+65 8878 5686 (Office Hours from 9am to 5pm)



6 Raffles Boulevard, JustCo, Marina Square, #03-308,  
Singapore 039594

Please [email](#) us for any enquiries.