

News & Update

- SVRP
- AiSP Cyber Wellness
- Special Interest Groups
- The Cybersecurity Awards
- Upcoming Events

Contributed Contents

- AI SIG: Artificial Intelligence 101
- CISO SIG: Introduction to CISO
- Corporate Partner: Magnet Forensics
- SVRP 2024 Gold Winner, Ho Zhi Hao [RP]

Professional Development
Membership

NEWS & UPDATE

New Partners

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

New Corporate Partner



Continued Collaboration

AiSP would like to thank CSIT for their continued support in developing the cybersecurity landscape:



News & Update

Book Prize Presentation @ ITE College East Graduation Ceremony on 8 May

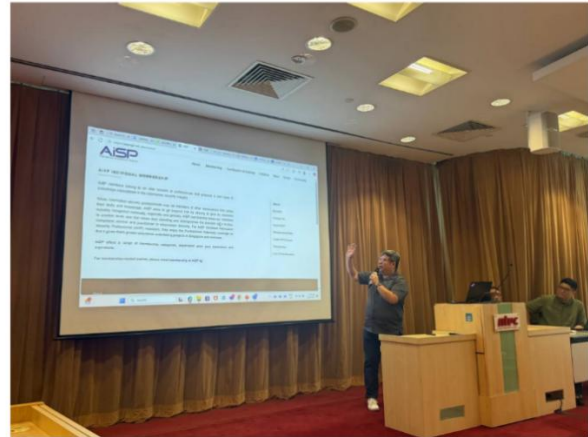
On 8 May, AiSP Director Mr Terence Siau was invited as the Guest of Honour at the ITE College East Graduation Ceremony for the School of Electronics & Info-Comm Technology (SEIT). As part of the ceremony, he presented book prizes to two outstanding students in recognition of their exceptional academic achievements.



Info Session for Design x AI x Tech (Cybersecurity) Certification Programme on 16 May

On 16 May, AiSP, National Trades Union Congress (NTUC), and Singapore University of Technology and Design (SUTD) hosted an information session at One Marina Boulevard to introduce the Design x AI x Tech (Cybersecurity) Certification Programme. This programme is tailored for non-IT professionals, PMEs, and IT practitioners who are looking to enhance their skills with up-to-date cybersecurity knowledge.

The first info session attracted 50 attendees. AiSP EXCO Member Mr Alex Lim and AiSP Director Mr Terence Siau provided insights into the Qualified Information Security Professional (QISP) certification, a key component of the programme. They also highlighted the benefits of AiSP membership and how it supports professionals in the cybersecurity community.



Punggol Digital District (PDD) Site Visit by AiSP x JTC on 26 May

On 26 May, in collaboration with ATXSG, AiSP and JTC brought a group of professionals from various companies on an exclusive tour of the Punggol Digital District (PDD) — Singapore's first smart district designed for the digital economy.

From exploring cutting-edge innovations to discovering how the Open Digital Platform and Digital Twin technology are transforming urban infrastructure, our 40 attendees had a front-row seat to what's next in smart, sustainable living and working.

AiSP Director, Mr Terence Siau, also shared how AiSP is driving cybersecurity awareness and growth, and encouraged participants to stay connected via our LinkedIn page for the latest updates, events, and opportunities.



Student Volunteer Recognition Programme (SVRP)




AiSP
Advance Connect Excel

Nomination Period:
1 Aug 2024 to 31 Jul 2025

CALL FOR NOMINATION!

STUDENT VOLUNTEER RECOGNITION PROGRAMME

Tier	Requirements
Bronze	Completion of one of three pillars or complete three of three pillars with minimum 50% attained hrs. + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Silver	Completion of two of three pillars + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Gold	Completion of all three pillars + Skills: 45 Hours or more + Events: 60 Hours or more + Leadership: 45 Hours or more



Scan the QR Code for the Nomination Form

The SVRP comprises three broad pillars where IHL students can volunteer:

- + Skills-based: E.g. Conduct cybersecurity workshops or develop related software
- + Events-based: E.g. Provide support at technology or cyber-related events
- + Leadership: E.g. Mentoring younger students and managing teams or projects

Visit www.aisp.sg/svrp.html for more details



Nomination Period:
1 Aug 2024 to 31 Jul 2025

CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

The SVRP for the secondary school and pre-university students is on merit basis and evaluation would be slightly different as cyber security is not offered as a subject nor co-curricular activities (CCA) in most schools in Singapore at the moment. The students would be given Certificate of Merit when they achieved the following (see A, B, C or D):

Example A

- + Leadership: 10 Hours
- + Skill: 10 Hours
- + Outreach: 10 Hours

Example B

- + Leadership: 0 Hour
- + Skill: 18 Hours
- + Outreach: 18 Hours

Example C

- + Leadership: 0 Hour
- + Skill: 36 Hours
- + Outreach: 0 Hour

Example D

- + Leadership: 0 Hour
- + Skill: 0 Hour
- + Outreach: 42 Hours



Scan the QR Code for
the Nomination Form

The track for Secondary School and Pre-University students comprises three broad pillars where they can volunteer:

- + Leadership refers to how the volunteer leads a team to complete the voluntary activity.
- + Skill refers to how the volunteer applies his/her cybersecurity knowledge to others
- + Outreach refers to how the volunteer is involved in outreach efforts (social media, events) to increase cybersecurity awareness for the public.

Visit www.aisp.sg/svrp.html for more details

Elevating Cybersecurity Education Through Unprecedented Collaborations

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

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

About the EC-Council Cyber Essentials Certification

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



AiSP Cyber Wellness Programme

Organised by:



Supported by:



In Support of:



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



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



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



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



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



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



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



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

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

Click [here](#) to find out more!

[back to top](#)

Special Interest Groups

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

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

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



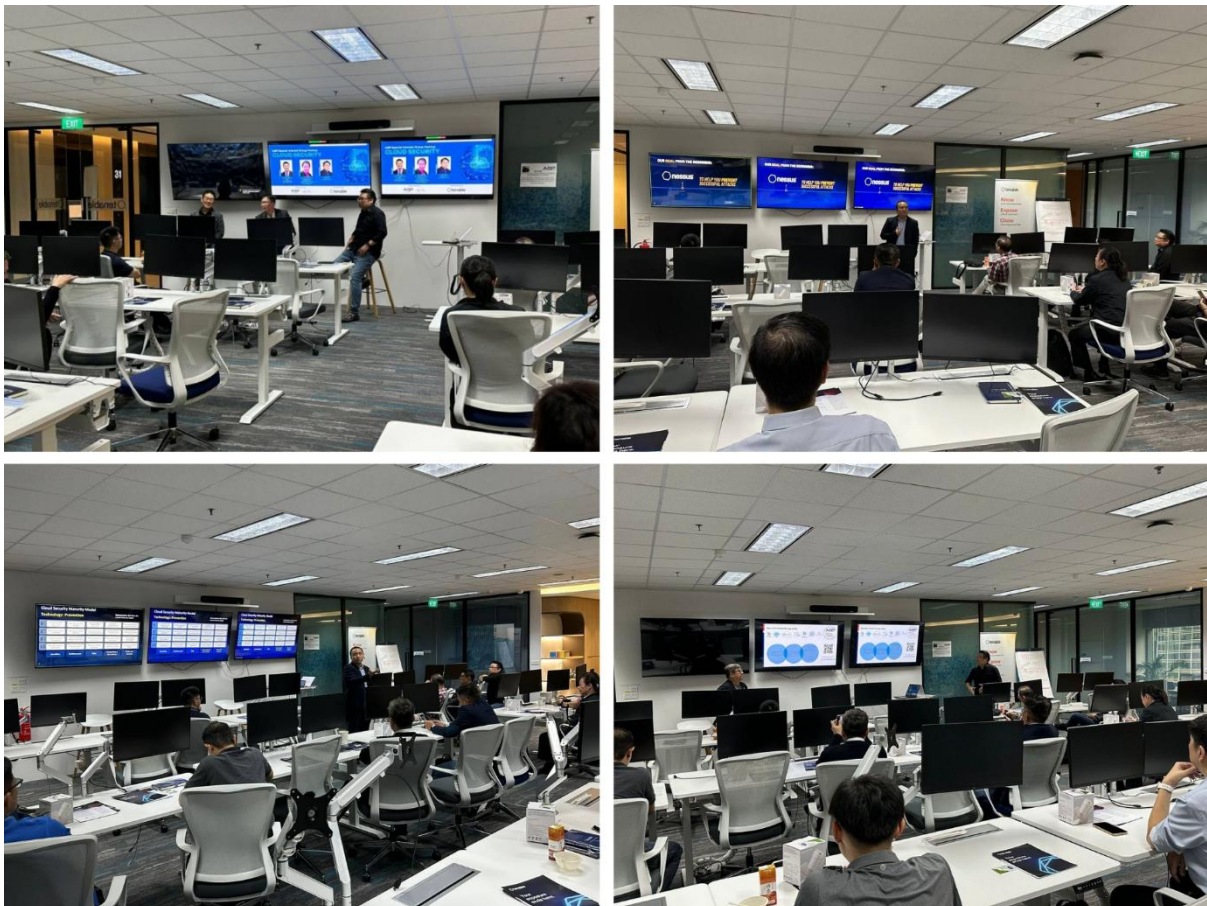
AiSP Cloud Security SIG Meetup on 13 May

We were proud to organize the AiSP Cloud Security SIG Meetup on 13 May, with special thanks to Tenable for sponsoring the event venue.

The session brought together professionals from across the cloud security landscape for an insightful evening of knowledge-sharing and collaboration. Discussions focused on securing identities, protecting sensitive data, and shaping strategic approaches to cloud security.

A heartfelt thank you to our guest speakers Mr Alvin Yeo, Mr Donald Ong, and Mr Jon Lau for their valuable insights, and to Mr Dennis Chan, AiSP Cloud Security SIG Lead, for expertly moderating the panel discussion.

We're grateful to all who attended and contributed to shaping the SIG's 2025–2026 workplan. Together, we're building a stronger and more secure cloud ecosystem.



Upcoming Event: AiSP Quantum Security SIG Meetup on 2 July**AiSP Quantum Security SIG Meetup**

Join us for an engaging session at the upcoming AiSP Quantum Security Special Interest Group (SIG) Meetup, where experts, innovators, and enthusiasts from the quantum security community gather to explore the evolving threat landscape and future-ready solutions.

The meetup will begin with registration and networking over refreshments, offering attendees a chance to connect with fellow professionals before the official programme kicks off.

The session will open with welcome remarks by Mr Michael Lew, AiSP Quantum Security SIG Lead, alongside representatives from CSA Singapore, setting the tone for an insightful afternoon.

We are pleased to welcome distinguished speakers who will share vital perspectives on quantum security strategies and innovations:

Dr Kawin Boonyapreddee

Chief Strategy Officer & APAC CEO, Applied Quantum

Topic: Primer: The Quantum Threat Landscape

Gain a foundational understanding of the “harvest-now-decrypt-later” threat model and the urgency of transitioning to post-quantum cryptography (PQC).

Mr Cyril Tan

Quantum Security Architect, SpeQtral

Topic: Spotlight: Quantum Tech in Singapore

Discover real-world use cases of quantum key distribution (QKD) and satellite-based secure communications developed by local pioneers.

Dr Prasanna Ravi

CEO, PQStation

Topic: Demo: PQC Scanning in Action

Watch a live demonstration of advanced tools for scanning and identifying PQC vulnerabilities, with actionable insights for seamless adoption.

[back to top](#)

A panel discussion will follow, featuring all speakers as they delve deeper into technical challenges and engage the audience in an interactive Q&A session. The event will close with final remarks and key takeaways from Mr Michael Lew and CSA Singapore. Whether you are already navigating the quantum frontier or just beginning your journey, this meetup offers an excellent platform to stay informed, collaborate, and contribute to the future of quantum-secure ecosystems.

Date: 2 July 2025 (Wednesday)

Time: 3:30PM – 6PM (Registration starts at 3.30pm)

Venue: Ministry of Digital Development and Information

140 Hill Street #01-01A, Old Hill Street Police Station, Singapore 179369

Register [here](#)

Upcoming Event: AiSP AI Security Summit on 26 August – CALL FOR SPONSORS



Launched in 2024 and organized by the Association of Information Security Professionals (AiSP) AI Special Interest Group (SIG), the AiSP AI Security Summit is a unique annual event that explores the critical intersection of artificial intelligence and cybersecurity. This year's summit delves into the emerging paradigm of Agentic AI—systems that can plan, act, and adapt with minimal human oversight—and the complex security challenges they introduce across the public, private, and academic sectors.

From threat amplification and loss of control to data integrity and trust, the event addresses the risks inherent in these powerful technologies.

By bringing together thought leaders and practitioners, the summit aims to chart a path toward the resilient, responsible deployment of Agentic AI—unlocking its promise while safeguarding our digital future.

For interested sponsors, please email:
secretariat@aisp.sg

The Cybersecurity Awards



The Cybersecurity Awards 2025 nominations has ended on **18 April 2025**! Thank you all for your nominations!

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)

For more details on the awards, visit our website [here](#)!



ORGANISED BY



SUPPORTING ASSOCIATIONS



GOLD SPONSORS



SILVER SPONSOR



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](#)

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
28 June	I am Digitally Ready @ South West Hong Kah North Community Club	Partner
1 July	CISO SIG Meetup	AiSP
1-3 July	CYDES 2025	Partner
2 July	Quantum Security SIG Meetup and Roundtable	AiSP
4 July	Learning Journey to I-Sprint for NYP	Partner
17 July	AI & DevSecOps SIG Meetup	AiSP
22 July	Learning Journey to Grab for TP	AiSP & Partner
26 August	AiSP AI Security Summit 2025	AiSP
21-23 October	GovWare 2025	Partner
19-21 November	Digitech ASEAN Thailand	Partner

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

CONTRIBUTED CONTENTS

Article from AI SIG

Using Amazon Bedrock to Run OpenAI-Compatible Applications

Mr Woon Tong Wing is a Senior Lecturer at Nanyang Polytechnic's School of Information Technology (SIT), where he leads the development of cloud computing curricula. As Chief Coach for the WorldSkills cloud computing trade, he trains NYP competitors for the WorldSkills competition, leading them to medal wins. He is also a member of the Information Technology Standards Committee (ITSC) for Cloud Computing and holds multiple industry certifications in cloud technology, cybersecurity and AI.

Introduction

OpenAI is a leading artificial intelligence research and deployment company. Founded in December 2015, it is known for creating advanced AI models, such as the GPT (Generative Pre-trained Transformer) series, and developing safe, useful, and widely accessible AI technologies. The OpenAI API allows developers to integrate powerful AI models—like GPT-4 for natural language understanding, DALL·E for image generation, and Whisper for speech recognition—into their own applications, websites or services, enabling a wide range of innovative and intelligent solutions.

OpenAI offers a variety of powerful APIs that allow developers to harness advanced AI capabilities in their applications. Among these are the **Responses API**, which provides straightforward text completions; the **Chat Completions API**, designed for more interactive and conversational experiences; and the **Realtime API**, which enables faster, low-latency interactions ideal for live applications. Additionally, the **Assistants API** allows for the creation of goal-oriented AI agents that can handle complex tasks, while the **Batch API** supports the processing of large volumes of requests efficiently. Together, these APIs provide flexible and scalable tools to integrate cutting-edge AI into a wide range of digital products and services.

A typical OpenAI-powered application works by sending structured JSON payloads to a set of standardised API endpoints provided by OpenAI. These endpoints correspond to specific services—such as text generation, conversation handling or image creation—and are designed to receive input data, process it using advanced AI models, and return relevant responses (Figure 1).

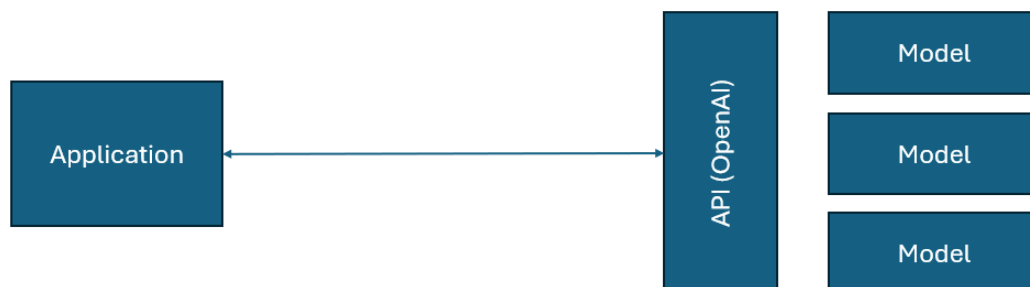


Figure 1

Due to the popularity of OpenAI's API, other providers have begun offering compatible APIs, such as:

- Google (Gemini): <https://ai.google.dev/gemini-api/docs/openai>

[back to top](#)

- Anthropic (Claude): <https://docs.anthropic.com/en/api/openai-sdk>
- xAI (Grok): <https://docs.x.ai/docs/overview>

Bedrock Access Gateway

Amazon Bedrock is a fully managed service by Amazon Web Services (AWS) that allows developers to build generative AI applications using a variety of foundation models—including those from Anthropic, Meta, Mistral, Cohere, and Amazon—without the complication of managing infrastructure.

However, Amazon Bedrock does not natively support OpenAI-compatible API endpoints. To bridge this gap, AWS provides a community-supported project: **Bedrock Access Gateway** [1]. This project acts as a middleware layer to emulate OpenAI API endpoints and forward requests to Bedrock models (Figure 2)



Figure 2

Setup

There are three main deployment options available for setting up the Bedrock Access Gateway: (1) using AWS CloudFormation with Lambda, (2) using CloudFormation with Fargate, or (3) running the gateway locally. The first option—CloudFormation with Lambda—offers a straightforward setup process and is generally more cost-effective. Once the deployment is complete, the system architecture will resemble what is shown in Figure 3.

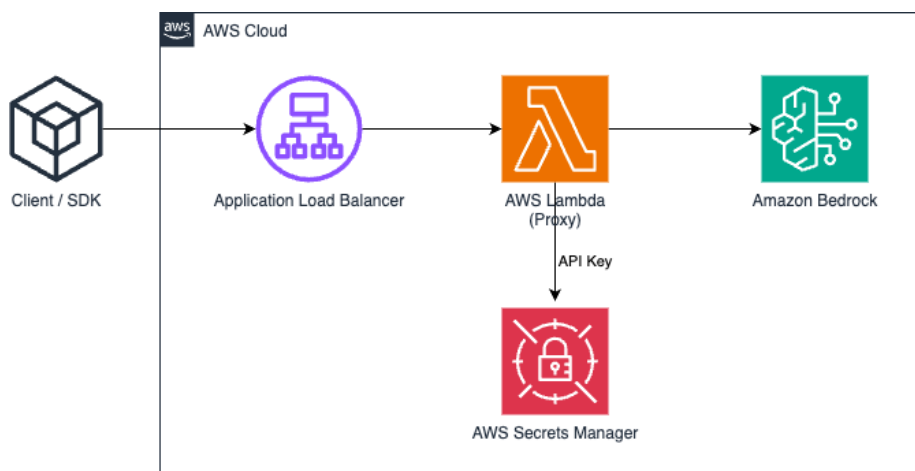


Figure 3

The general steps for setting up the Bedrock Access Gateway using AWS CloudFormation with Lambda, are: Start by selecting a region that supports Amazon Bedrock, such as us-east-1. Then, create an API key in AWS Secrets Manager and store it securely. Next, request access to the models needed through the Amazon Bedrock Console, and deploy the CloudFormation stack using the link in the Bedrock Access Gateway [<https://github.com/aws-samples/bedrock-access-gateway>]. Finally, once the deployment is complete, retrieve the API endpoint from the CloudFormation stack for use in your applications.

Pros and Cons of Using Bedrock Access Gateway

The main advantage of using the Bedrock Access Gateway include consolidated billing, which allows centralised tracking of costs within AWS, and the ability to leverage AWS credits - particularly beneficial for startups in the AWS Activate programme. Additionally, users can access a wider variety of models that may not be available through OpenAI, along with the added benefits of AWS services such as IAM-based security, CloudWatch logs and VPC networking, all of which enhance security and monitoring.

However, there are some drawbacks to consider. The setup introduces increased complexity by adding an extra layer of translation and infrastructure management. There may also be slight latency in request and response times, and not all OpenAI endpoints may be fully compatible with the system. Lastly, while the hosting costs are minimal, they still add another component to maintain within the infrastructure.

Summary

For teams already building AI applications using the OpenAI API format, the Bedrock Access Gateway provides a bridge to AWS's secure and flexible ecosystem. It allows developers to take advantage of AWS-native benefits—such as consolidated billing, enterprise governance, and broader model access—without rewriting existing codebases. While it introduces some overhead, the trade-off may be worth it, especially in enterprise or multi-cloud contexts where control, compliance, and cost tracking matter.

Contact Information: Woon Tong Wing
School of Information Technology
Nanyang Polytechnic
E-mail: woon_tong_wing@nyp.edu.sg

References

1. <https://github.com/aws-samples/bedrock-access-gateway>

Article from CISO SIG

Introducing CISO with a deep interest in cybersecurity

Eugene Teo is the Chief Security Advisor at Microsoft ASEAN. As a seasoned CISO, he provides strategic guidance and thought leadership, serving as a trusted advisor to CXOs and Board directors on cybersecurity governance and strategy, data protection and digital resilience. He also serves as the Data Protection Officer (DPO) for Microsoft Singapore.

Eugene brings more than two decades of experience in digital and cybersecurity, having dedicated much of his career helping US companies establish and grow their Asia Pacific cybersecurity capabilities in Singapore. Before joining Microsoft, Eugene was Vice President of Security and Deputy Chief Security Officer at UKG (formerly Ultimate Software) and also served as a Subsidiary Board Director for its Singapore entity. His earlier roles include security leadership positions at Symantec Security Response and Red Hat Product Security.

Beyond his professional role, Eugene serves as the Co-Chair of the Singapore Chapter at the FAIR Institute and is a Co-opted Committee Member of the Cybersecurity Chapter at the Singapore Computer Society (SCS). His involvement in the security community began in the early 2000s as a founding executive committee member of SIG^2 (Special Interest Group in Security and Information InteGrity).

Eugene is an Accredited Director with the Singapore Institute of Directors (SID) and a Boardroom Certified Qualified Technology Expert (QTE). Eugene holds bachelor's and master's degrees in computing from the National University of Singapore (NUS), along with industry-recognized certifications including CISM, CRISC, CIPM, CIPP/E and Open FAIR 2 Foundation. He is featured in the book *Tribe of Hackers Security Leaders: Tribal Knowledge from the Best in Cybersecurity Leadership*. Eugene has spoken at security conferences including DEF CON's AI Village and Black Hat Asia's AI Summit, served on advisory and review boards, and regularly advises technology startups.

What brought you to the Cybersecurity industry?

My early exposure to Unix during my pre-university days ignited a strong passion for Linux and open source development. I often found myself more immersed in exploring system internals and contributing to the open source community than focusing on my coursework. Thankfully, I still performed well academically, and this passion led to opportunities with several startups during the dot-com days, where I was able to apply and further hone my technical skills.

My first significant encounter with a computer security incident came during the ILOVEYOU virus outbreak. It was a VBScript-based worm that propagated itself through emails and caused widespread disruption at the startup I was working with. That

[back to top](#)

experience was a pivotal moment when I realised I could combine my Unix/Linux background with a deeper understanding of computer security to carve out a distinctive and valuable niche in the field.

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

Let me share another defining moment that shaped my career.

I had a fulfilling career at Red Hat, where I led the global Cloud Business Unit's product security team. I also earned a place on the upstream Linux kernel security team, becoming the only member from Asia at the time. I'm proud of the work we did to strengthen the security of numerous prominent open source projects, particularly the Linux kernel.

Over time, however, I began to feel that my expertise was becoming too narrowly focused. I wanted to broaden my perspective and gain experience across other domains of cybersecurity. Seeking new challenges, I took a leap of faith and joined Symantec. They took a chance on me, bringing me in as the founding leader to help build and lead a new team supporting both global security response efforts and regional initiatives. I made my fair share of mistakes along the way, but each one taught me valuable lessons and shaped me into a more well-rounded leader with a deeper understanding of business alignment and execution.

That role opened the door to my next opportunity at Ultimate Software (prior to its acquisition, merger, and rebranding as UKG), where I was tasked with establishing the company's first international office in Singapore. My initial mission was to build a Security Operations Centre (SOC) capable of monitoring, detecting, and responding to cybersecurity threats and payment frauds. It was a true startup experience backed by a well-established, publicly listed company in the States. On my first day, we had to find a serviced office just so I had a place to work. When I hired my second employee, a Korean, I even had to pay for his Employment Pass (EP) application with my personal credit card. We did not have group insurance policies until our team reached a certain size. Those early days were my happiest and incredibly formative.

As the office grew, so did my responsibilities. I worked closely with legal, compliance, finance, HR, and other key stakeholders, not only on local operational matters, but also to align our global security programme around protecting our company's most critical business activities. When Ultimate Software was acquired by a private equity firm, I gained valuable exposure to portfolio-level CISOs and board members. This gave me a much deeper appreciation for cybersecurity governance from the boardroom's perspective, and what it takes to mature a security programme at scale.

Looking back, had I not taken the leap from Red Hat to Symantec, I might never have gained the experience of building a regional team from the ground up, or later stepping into a global cybersecurity executive role.

[back to top](#)

What is it that you love most about your role?

At Microsoft, I have the privilege of working alongside some of the brightest minds in the industry. I joined the company at a pivotal time when we were, and continue to be, focused on rebuilding customer trust following a couple of high-profile nation-state intrusions.

Witnessing firsthand how our CEO sets the tone at the top by prioritising security above all else, and making it clear that it is everyone's responsibility, was impactful. This is inspiring because not many CISOs have the privilege of seeing cybersecurity championed so strongly at the highest level of leadership.

I have seen how transformational changes were implemented across the company to strengthen our defences, reduce our attack surface, and minimise the likelihood of future incidents. Many of the lessons and best practices we have developed internally have become valuable insights that I have had the opportunity to learn from, share with our customers, and hopefully apply should I return to a CISO role in the future.

In my current role, I work closely with CISOs and CIOs across diverse industries, from highly regulated sectors and critical information infrastructure providers to industries like real estate where security programmes tend to be less mature and more IT-driven. Drawing on my background as a former CISO, I help these leaders strengthen their cybersecurity strategies and programmes. It is also a great opportunity to grow my local and regional network and stay connected to the evolving priorities across the cybersecurity landscape.

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

There has been growing discussion around digital resilience, looking beyond just cybersecurity risks. How can organisations strengthen business continuity and ensure resilience against both cyber and non-cyber disruptions? How can organisations build resilience into the critical services and workloads their business depends on? And importantly, how should companies prepare for scenarios where access to commercial services is disrupted due to geopolitical events beyond their control?

Another top of mind topic is Agentic AI. How can organisations harness AI to automate business processes and enhance employee productivity? At the same time, how can they strike the right balance between driving innovation through AI and managing the costs required to implement it effectively across the business?

There is a growing interest in learning to quantify cybersecurity risks using frameworks like Open FAIR (Factor Analysis of Information Risk). How can we explain cybersecurity in a language that resonates with senior stakeholders? Should we continue to rely on 5x5 risk matrices, or is it time to express cybersecurity risks in terms of probable loss exposure in

financial terms based on specific cybersecurity risk scenarios that are relevant to the business context?

What do you think is the role of CISO?

The CISO role has evolved from a purely technical position to that of a strategic business leader, with a mandate that extends well beyond IT. Today's CISO is not a gatekeeper who tells the business what it can or cannot do, but a partner who understands the business landscape. The CISO is there to support the business to conform with legal and regulatory requirements, meet strategic objectives and performance, and unlock new opportunities. The CISO's mission is to protect critical business activities by implementing the necessary controls that are proportionate to the risks and aligned with the value they safeguard.

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

There is no shortage of people looking to enter the cybersecurity field. It is important to join for the right reasons. You need to have the passion, the relentless drive to keep learning, and the adaptability and resilience to face evolving threats and challenges head-on. Cybersecurity is dynamic and demanding, and for those who are truly invested, it can be very rewarding.

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

Boards have a timely opportunity to transform and strengthen how they govern digital and cybersecurity risks. Cybersecurity is now recognized as a critical business risk, amplified by the increasing number of high-profile cyber incidents reported in mainstream media. Directors must go beyond surface-level awareness by asking the right questions, thoughtfully assessing and challenging the responses, and providing meaningful oversight. The Cyber Resilience Guide for Boards in Singapore, published by SID, is a step towards the right direction.

As an aspiring independent non-executive director (INED), I am seeking board opportunities with organisations that are open to adding directors with digital and cybersecurity expertise. I am also keen to contribute by writing thought leadership articles and participating in discussions and sharing sessions to help directors strengthen their oversight of cybersecurity risks. At the same time, I continue to learn and broaden my knowledge by exploring topics beyond cybersecurity, including ESG (Environmental, Social, and Governance).

Any advice for the Cybersecurity Professionals?

Build a strong technical foundation early in your career is essential. As you gain experience on the job, it is equally important to develop your soft skills, such as communication, presentation and critical thinking skills. Do not shy away from difficult or unfamiliar projects as growth often comes from stepping outside your comfort zone.

Article from Corporate Partner, Magnet Forensics

Modernizing forensic workflows with Magnet Automate

Cybersecurity threats are increasing in frequency and complexity. Improving the speed and scale that enterprise digital forensics and incident response (DFIR) teams investigate and respond to incidents is vital to keep pace with threats.

In this guide, discover how Magnet Automate enables rapid response to threats by harnessing the power of automation to transform DFIR workflows—specifically by unlocking lab capacity, empowering your experts, and ultimately finishing digital investigations faster.

Key takeaways:

1. The benefits of automation in DFIR and how the powerful capabilities of Magnet Automate such as orchestration, remote collection, parallel processing, and more, can be utilized.
2. How Magnet Automate increases the efficiency of three common workflows: data loss prevention (DLP), malware, and inter-department handoffs.
3. Additional ways you can leverage automation to transform and enhance your workflows

Start responding to security incidents faster by automating the tasks and tools in your DFIR workflows to reduce the number of manual touchpoints and keep pace with threats.

Download the White Paper Now

CTA: https://www.magnetforensics.com/resources/modernizing-forensic-workflows-with-magnet-automate-enterprise/?utm_source=AiSP&utm_medium=SponsoredEmail&utm_campaign=UTMC-0000142

Article from SVRP 2024 Gold Winner, Ho Zhi Hao [RP]



How SVRP has directly impacted your cybersecurity journey?

SVRP has impacted my cybersecurity journey in many ways such as academics, educational and career path. SVRP has impacted my academics in a way which motivates me to perform better. SVRP allows me to have the opportunities to conduct workshops for my peers and therefore it allows us recap the learning resources and materials from our school. This better prepares for our examinations and therefore increases our chances of scoring well. At the same time, it improves our skills and knowledges for cybersecurity. SVRP has impacted my cybersecurity journey in educational purposes allowing me to learn from peers from other polytechnics be it skill wise or knowledges. Through SVRP, I have made many new connections with peers and this allows me to learn from them. At the same time, SVRP has provided me a series of opportunities which allowed me to learn from companies in the same industry skillsets that I have never learnt before. SVRP has also impacted directly on my career path as it allowed me to better understand what I want to do in the future and it opens a series of career opportunities for me.

How SVRP has inspired them to contribute to the cybersecurity field?

SVRP has inspired me to contribute to the cybersecurity field in many ways such as the different learning opportunities and leadership opportunities. SVRP has provided me with different learning opportunities to learn from peers and to learn from companies. My peers allowed me to learn from them the skillsets that I did not have and therefore we will exchange knowledge with one another. The company opportunity opens up knowledges and skills that is not included in our school syllabus. For instance, Trend Micro has allowed me to learn more about Cloud Security, Endpoint Security and

Mobile Security. SVRP has provided me leadership opportunities that helped me to lead and guide peers to conduct a safe and conducive series of workshops that are run in school. With these opportunities that are provided, SVRP has inspired me to contribute more to the cybersecurity field because it made me realize the experiences that I have opened up a potential in me to lead, guide and spread awareness and knowledge to others. Therefore, SVRP inspired me to contribute into the cybersecurity field.

What motivates you to be a student volunteer?

A student volunteer to me is not just about volunteering. It allows us to see what it truly means by volunteering as when we are volunteering in cybersecurity events, it allows us to learn from the event or others who have higher experiences than us. At the same time, we are also able to make others in the community to learn too. This allows and motivates me to be a student volunteer. I strongly believe that being a student volunteer allows us to have the opportunity to contribute and spread awareness and knowledge to others in the community, making the community an inclusive one. Having an inclusive community is important because cybersecurity is for everyone. Everyone that is connected to the Internet is required to have basic knowledge of how to protect themselves. Therefore by having an inclusive community, it will allow everyone to learn and protect themselves. I am motivated to be a student volunteer because it allows me to inspire my juniors to be the same as me. As when I have obtained this award last year, multiple juniors and peers were inspired. This means that I should continue to be a learning role model. I hope that I can inspire many of my other peers and juniors such that they can continue to spread the inclusivity so that more netizens are able to learn.

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

I would encourage my peers to be interested in cybersecurity not just because of all these awards and opportunities. I would encourage my peers to be interested and be passionate because cybersecurity is everywhere and has become part of our daily lives. It is important for them to understand the importance of cybersecurity and to stay safe online. I would encourage them by making a series of engaging events to allow them to learn about the different cybersecurity concepts. The engaging events aim to help and motivate them to keep learning about cybersecurity as cybersecurity is an ongoing learning journey. Each day we have to learn about new different attacks and potential vulnerabilities in order to stay safe. By engaging my peers in a series of events, this will ensure them to have not just the interest and passion but also the discipline to keep up with learning.

PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®)

QISP Preparatory Course by RP from 11-13 June



Qualified Information Security Professional (QISP) Preparatory Course

(SkillsFuture Funded)

About the Course

Designed for entry to mid-level professionals, this course covers key domains from the AiSP Information Security Body of Knowledge 2.0 (IS-BOK 2.0), including Governance & Management, Physical Security, Security Architecture, and Cyber Defence. It prepares learners for the QISP examination.

Key Learning Outcomes

- Align security goals with business strategies.
- Implement governance, risk management, and compliance measures.
- Design and manage secure architectures.
- Ensure physical security and business continuity.
- Enhance software security and cyber defence.
- Conduct security audits and assessments.

Who Should Attend?

IT professionals, security analysts, system administrators, and anyone looking to validate their cybersecurity expertise with the QISP certification.

Date of Course:
11-13 June 2025

REGISTER INTEREST



QISP Exam Preparation Crash Course by Deloitte

Deloitte.

AiSP
Advance Connect Excel

QISP® EXAM PREPARATION CRASH COURSE

Are you ready to boost your cybersecurity career with the QISP® certification? Join Deloitte's intensive crash course and get exam-ready in just 3 days!

- **Taught by our experts with several years of industry experience**
- **Intensive fast-tracked learning**
- **Practical exercises for real-world application**
- **Flexible batch timings**



The QISP® training is based on AiSP's Information Security Body of Knowledge (IS BOK) 2.0. Candidates must achieve a minimum of 50-64% (Qualified Information Security Associate), 65% and above (Qualified Information Security Professional) to pass.

Domains covered on the QISP® exam:

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

New batch is starting soon, register your interest now by scanning the QR code!

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

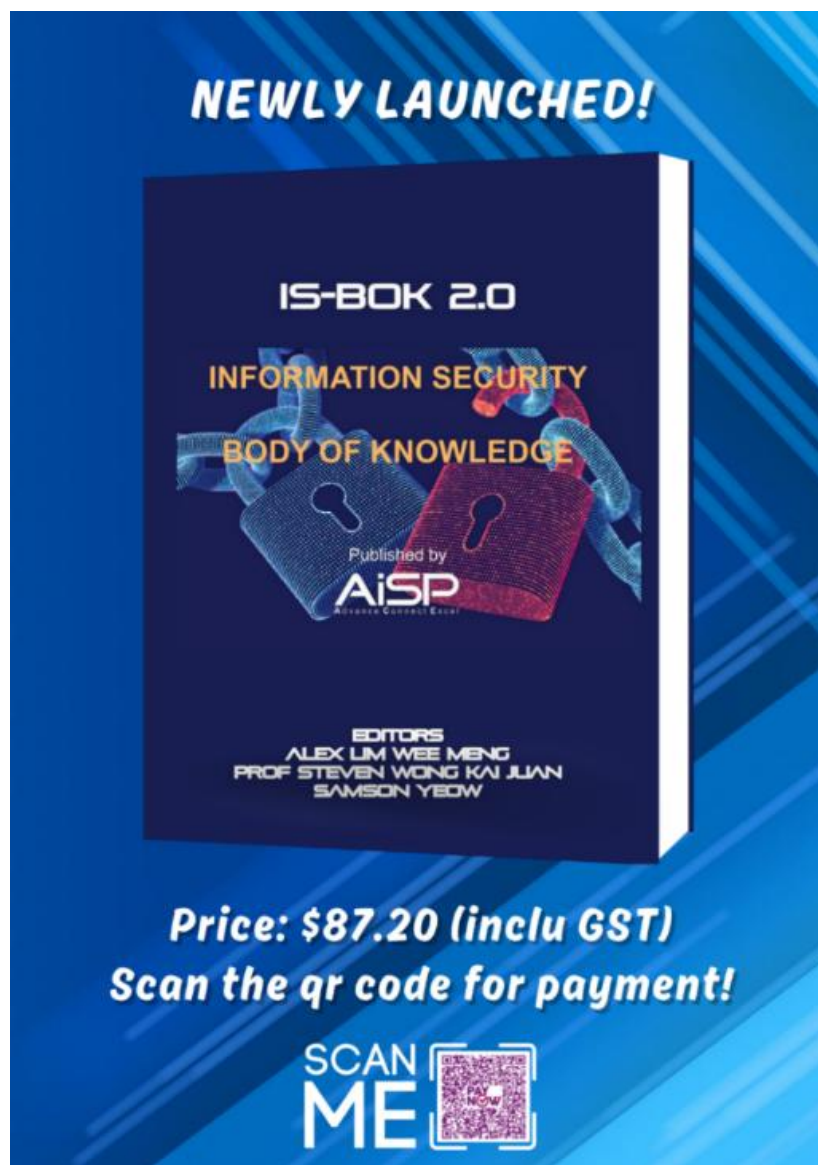
WISSEN Cyber Security Competency Development enquiry@wissen-intl.com | www.wissen-intl.com

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](#)!

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!**

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



MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

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

Complimentary Affiliate Membership for NTUC Members

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

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

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

CPP Membership



For any enquiries, please contact secretariat@aisp.sg

[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





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

AiSP Academic Partners



Our Story...

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

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

Our Vision

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

Our Mission

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

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



www.AiSP.sg

secretariat@aisp.sg

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

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