AiSP NEWSLETTER
November 2024

Content Page

News & Update

Contributed Contents

News & Updates

SUSS Book Prize on 9 October

Congratulations to the two winners from Singapore University of Social Sciences (SUSS) who have won the Book Prize award sponsored by AiSP during the Convocation Ceremony on 9 October!

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES
CONVOCATION 2024
Congratulations Class of 2024!
SUSS CONVOCATION 2024
DREAM, DARE, DO.
8–9 OCTOBER

Cyber Security World Asia 2024 on 9 – 10 October

AiSP Vice President and CAAP EXCO Lead Mr Breyvan Tan spoke at the Cyber Security World on 9 October where he shared on Empowering Cyber Defenders: Innovations in Cybersecurity Awareness and Training Programs.

AiSP
EMPOWERING CYBER DEFENDERS:
Innovations in Cybersecurity Awareness and Training Programs
9 October 2024
@techweeksingapore #CSWA #CyberSecurityWorldAsia #TechWeekSingapore

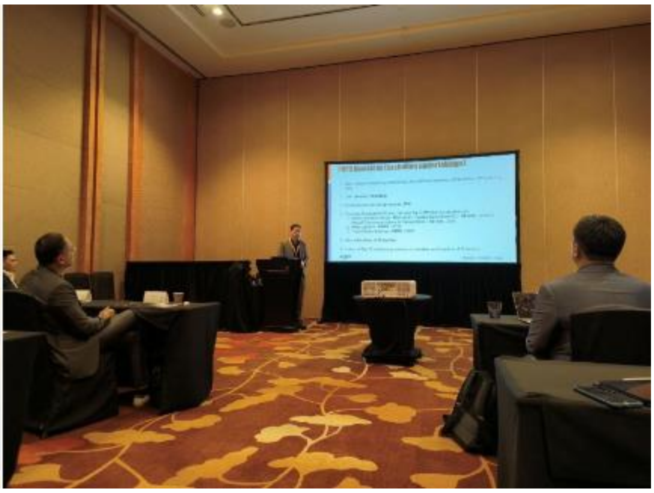
back to top

Govware on 15-17 October

AiSP had a booth at Govware from 15-17 October to share about AiSP Membership, Training and Initiatives to the attendees.

ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP
ASSOCIATION OF NATIONAL INFORMATION & COMMUNICATION TECHNOLOGY ENTREPRENEURS
CENTER FOR STRATEGIC CYBERSPACE AND INTERNATIONAL STUDIES

AiSP Data and Privacy SIG EXCO Lead Mr Wong Onn Chee shared about the Best Practices on Huawei Data Protection / Ransonware Prevention for ASEAN region held at Govware on 16 October. Thank you to our CPP - Huawei for inviting AiSP to the event.



back to top

National HealthCare Group (NHG) Cybersecurity Awareness week on 22 October

AiSP Vice-President Ms Sherin Lee together with Mr Yum Shoen Yih conducted a Cybersecurity Awareness Talk at the National HealthCare Group (NHG) Cybersecurity Awareness week on 22 October. The talk aims to share with the audience about the security requirements and what they can do for themselves and their organisation in Healthcare. Thank you NHG for inviting AiSP to be part of their Cybersecurity Awareness week.

AiSP
About us
A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem
Pillar for the Information Security Profession and Professionals in Singapore
Sustainability
Collaboration
Recognition
ADVANCE
CONNECT
EXCEL
Corporate Partners
Academic Partners
Ladies in Cyber
Members

back to top

Member Acknowledgment

Interview with AiSP EXCO Member Ms Judy Saw

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

As Lead for the Ladies in Cyber charter, my vision is to create a platform where women feel empowered and supported in their cybersecurity journeys. By driving initiatives like mentorship programs, hands-on workshops, and networking events, I aim to increase both the visibility and participation of women in the cybersecurity industry. In my role, I hope to highlight how diversity directly contributes to innovation and resilience in cybersecurity.

The biggest challenge facing the industry today is the widening gap between the growing complexity of cyber threats and the availability of skilled professionals to address them. The talent shortage, compounded by underrepresentation of women limits the industry's potential to combat evolving threats. By actively addressing these gaps through programs that encourage more women to pursue cybersecurity careers, we can enhance the overall security landscape. In addition, raising awareness about cybersecurity's critical role across industries and promoting accessible educational pathways can also help to resolve this talent crisis.

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

Upholding AiSP's reputation begins with embodying its core values—advance, connect, and excel. I plan to emphasize these values in every engagement by promoting our commitment to cybersecurity education, thought leadership, and the development of a thriving, inclusive community. One of AiSP's greatest strengths is its ability to bring together industry professionals, academia, and government bodies to work toward a common goal: building a safer and more resilient cyber environment.

When I represent AiSP at events, my approach will be to align AiSP's mission with the broader industry challenges and initiatives. This involves demonstrating how our programs and partnerships directly address key issues such as the skills gap, emerging cyber threats, and the need for greater inclusivity. I will ensure that stakeholders recognize AiSP as a driving force in shaping a future-ready cybersecurity workforce, with a strong emphasis

back to top

on developing underrepresented talent and fostering an inclusive, supportive environment for professional growth.

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

One area I'm deeply passionate about is creating opportunities for women in cybersecurity. Through initiatives like the Ladies in Cyber Symposium and the Cyber Queens Bug Bounty Challenge, I aim to create spaces where women can test their skills, learn from experts, and grow their confidence in technical and leadership roles. By actively contributing to these initiatives, I hope to bridge the gender gap in cybersecurity and give women a platform where they can thrive.

For AiSP members, I would like to share insights on how to develop strong cybersecurity careers, especially for those entering the field or looking to advance. I believe mentorship, practical hands-on experience, and continuous learning are essential. My work within AiSP is focused on building communities that provide these opportunities, especially through collaboration with industry partners, academic institutions, and government agencies. Together, we can nurture a cybersecurity workforce that is diverse, skilled, and ready to tackle tomorrow's challenges.

Student Volunteer Recognition Programme (SVRP)

Learning Journey to Grab with RP on 7 October

On 7 October, AiSP brought about 40 students from our Academic Partner, Republic Polytechnic on a learning journey to visit our Corporate Partner, Grab .

back to top

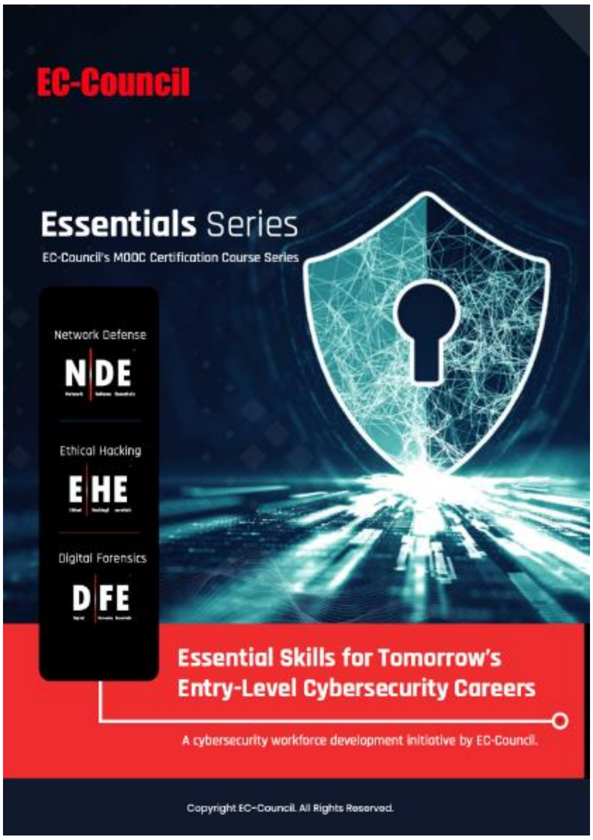
Elevating Cybersecurity Education Through Unprecedented Collaborations

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

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

About the EC-Council Cyber Essentials Certification

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



EC-Council

Essentials Series

EC-Council's MOOC Certification Course Series

Network Defense
N|DE

Ethical Hacking
E|HE

Digital Forensics
D|FE

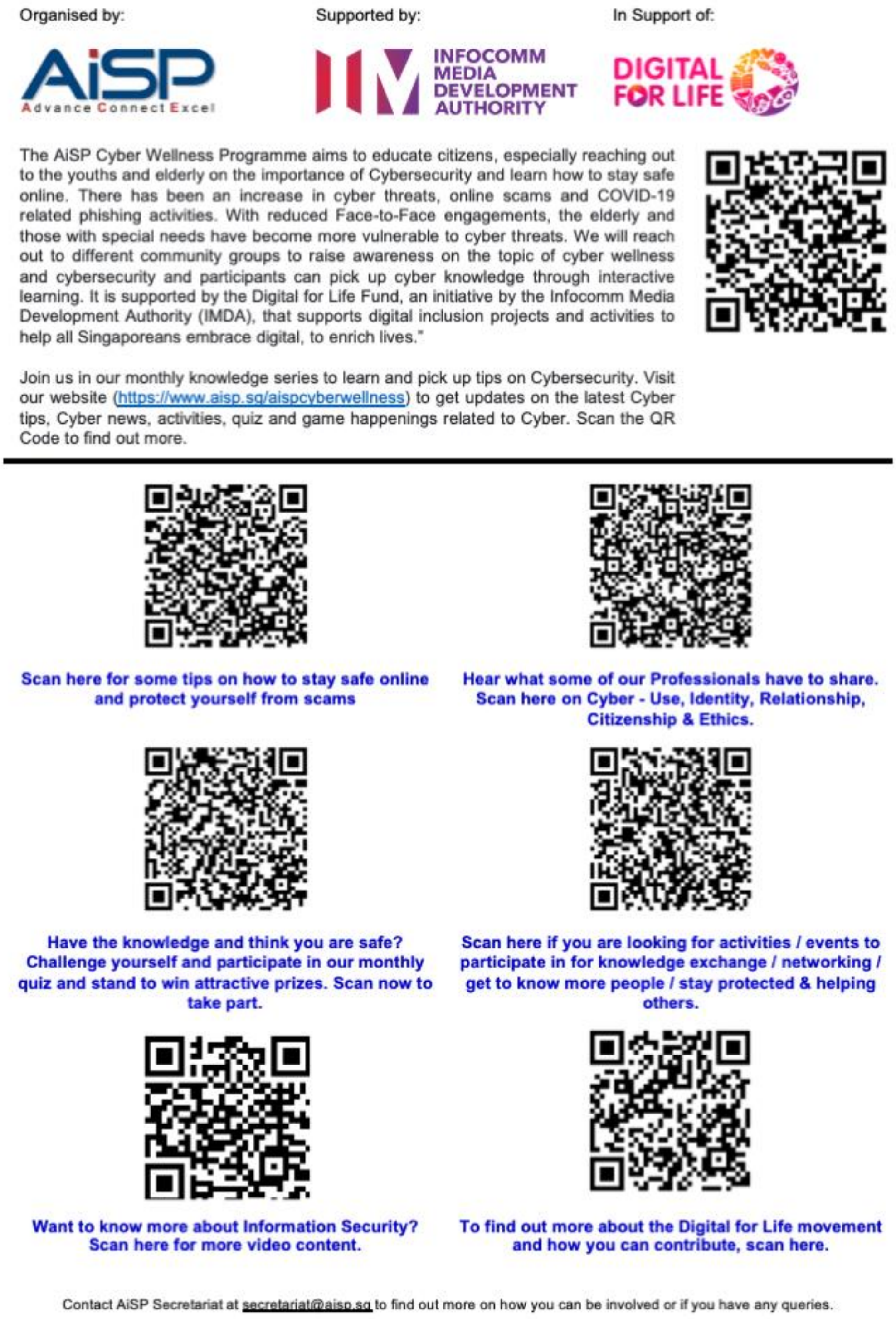
Essential Skills for Tomorrow's Entry-Level Cybersecurity Careers

A cybersecurity workforce development initiative by EC-Council.

Copyright EC-Council. All Rights Reserved.

back to top

AiSP Cyber Wellness Programme



Organised by: Supported by: In Support of:

Advance Connect Excel
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
DIGITAL FOR LIFE

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

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

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

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

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

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

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

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

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

Click here to find out more!

back to top

Special Interest Groups

AiSP has set up six **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)

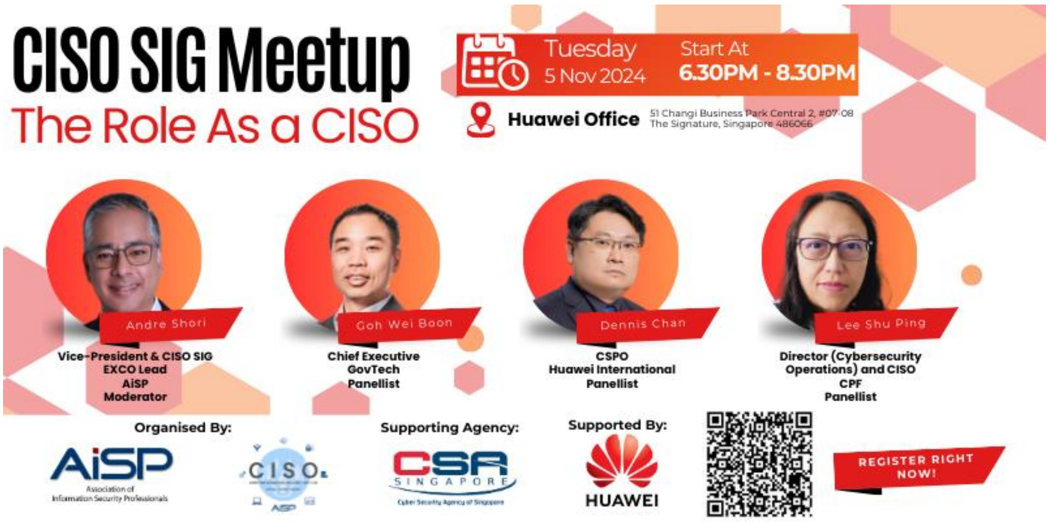
We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together. If you are keen to be part of a SIG, please contact secretariat@aisp.sg

back to top

AiSP LITE SIG Meetup - Inside the Lab: A Day in the Life of a Digital Forensic/e-Discovery Specialist on 3 October

AiSP held our first LITE SIG Meetup on 3 October with more than 60 guests attended the meetup. Thank you Daniel Wang for giving the opening address and Chua De Hui, Jacky Ang, Mohamad Ridzuan and Shirley Liew for being in the panel.

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



As the digital landscape evolves rapidly, ensuring the security of our supply chain has become paramount. Vulnerabilities within these chains can lead to devastating consequences, including data breaches, financial losses for companies and disruptions both for industry and critical infrastructure. Join us for a panel discussion on the critical aspects of securing the supply chain and ensuring a secure product life cycle. This panel discussion will delve into the idea of building a comprehensive security framework involving cyber and product security, at each step, from ideation to decommissioning.

back to top

Experts from leading organizations will also discuss the importance of implementing strategies to help create a collective cybersecurity ecosystem of trust.

Panel Discussion
Moderator: Mr Andre Shori, Vice-President & CISO SIG EXCO Lead, AiSP
Panellists:

1. Mr Goh Wei Boon, Chief Executive, GovTech
2. Mr Dennis Chan, CSPO, Huawei International
3. Ms Lee Shu Ping, Director (Cybersecurity Operations) and CISO, CPF

Date: 5 November 2024, Tuesday
Time: 6.30PM – 8.30PM
Venue: Huawei Office
Registration: https://forms.office.com/r/BNYmVM610X

The Cybersecurity Awards

THE CYBERSECURITY Awards 2024

Thank you for your support! The Cybersecurity Awards 2024 nominations has ended and the awards ceremony will be on 7 November 2024.

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)

back to top

THE CYBERSECURITY *Awards* 2024

ORGANISED BY

AiSP
Advance Connect Excel

SUPPORTED BY

CSA SINGAPORE
Cyber Security Agency of Singapore

SUPPORTING ASSOCIATIONS

CSA cloud security alliance SINGAPORE CHAPTER

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

ISACA Singapore Chapter

ISC2 CHAPTER SINGAPORE

OT-ISAC

SCS Singapore Computer Society

SGTECH WHERE TECH MEETS

THE LAW SOCIETY OF SINGAPORE

PLATINUM SPONSORS

CISCO

HUAWEI

ST Engineering

GOLD SPONSORS

BeyondTrust

DBS

ENSIGN INFOSECURITY

Grab

SANS

SIT SINGAPORE INSTITUTE OF TECHNOLOGY

TREND MICRO

WISSEN Cyber Security Competency Development

wizlynx group

back to top

Regionalisation

AJCCA Conference on 17 October

The ASEAN-Japan Cybersecurity Community Alliance (AJCCA) Conference was held on 17 October at Suntec Singapore with insightful panel discussions and sharing from our speakers on various topics to strengthen our cybersecurity ties across the region.

AJCCA and South East Asia Cybersecurity Consortium (SEACC) have pledged through an MoU exchange to collaborate and enhance the Cybersecurity capabilities, information sharing and mutual support among its member nations to address the evolving challenges in the digital landscape.

Thank you MOS Rahayu Mahzam for gracing the event and witnessing the MOU exchange between AJCCA & SEACC. Also a big thank you to our sponsors, Veracity Trust Network, Gemini Data Inc., Magnet Forensics, CyberSafe, EC-Council ASEAN, GMO Cybersecurity, NTT, SailPoint who contributed to making this event a success!

back to top

AiSP Advisory Council Member and Immediate Past President, Mr Johnny Kho conferred as the Co-Founder of AJCCA Award on 17 October

Congratulations to AiSP Advisory Council Member and Immediate Past President of AiSP, Mr Johnny Kho who was conferred as the Co-Founder of AJCCA Award at the inaugural AJCCA Cyber Resilience Awards (ACRA) Ceremony at AJCCA Conference 2024 held at Suntec Convention Centre on 17 October.

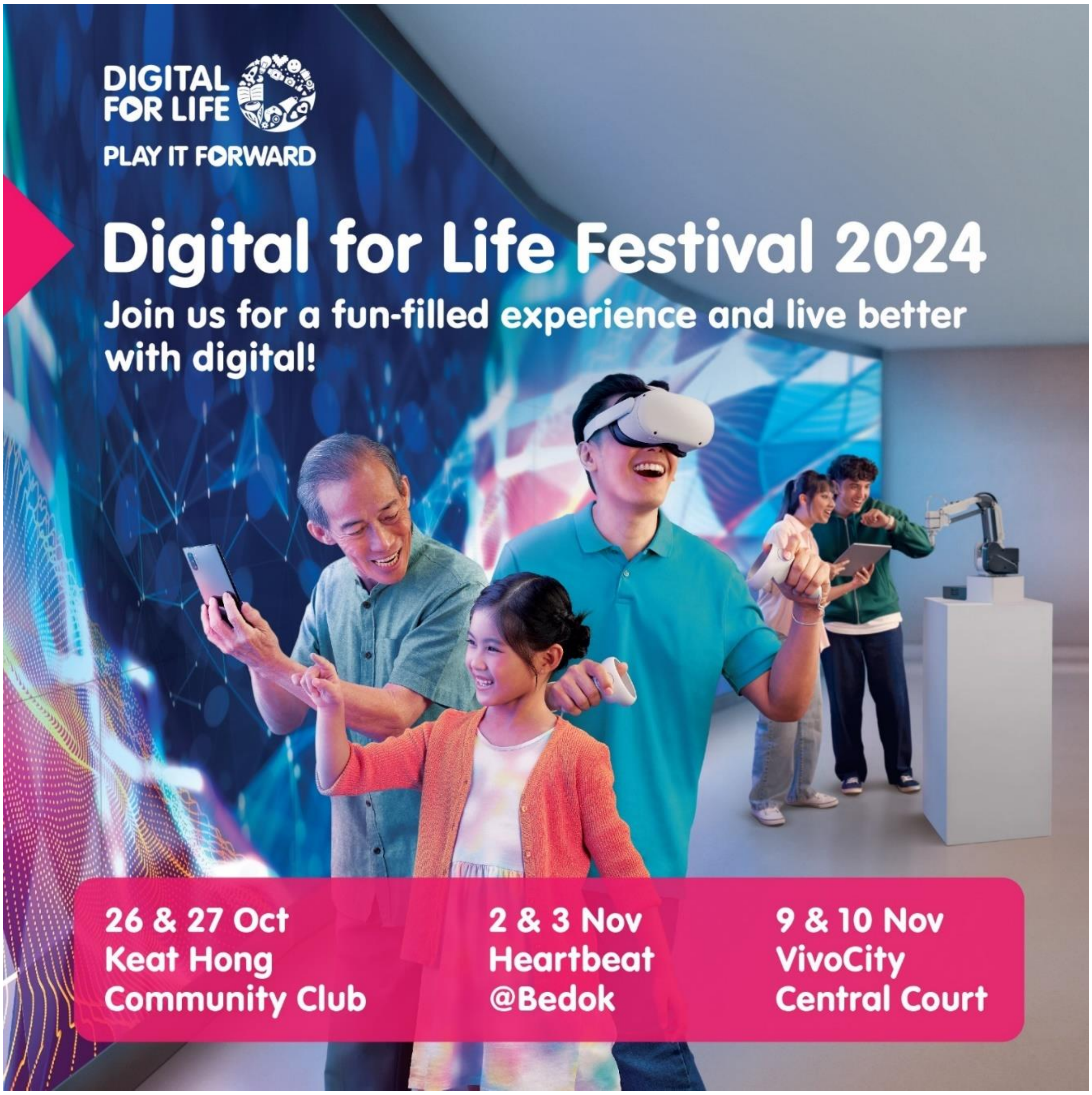
MOU signing with rawSEC and AiSP on 17 October

We are pleased to share that rawSEC and AiSP signed an MoU on 17 October at the AJCCA Conference 2024 to deepen collaboration between Singapore and Malaysia witnessed by AJCCA Chairman Pak Rudi & Dato' Dr Amirudin Abdul Wahab' for learning and sharing which include overseas learning journey for students. As such, AiSP will also be bringing 34 female students for an overseas Ladies in Cyber Learning Journey to KL in December 2024 and visit to Cyber Security Malaysia, EC-Council (Wissen International) and High Commission Singapore in KL.

back to top

Digital For Life

Digital for Life Festival on 2-3 November



back to top

Corporate Partner Event

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

AiSP x wizlynx group x KnowBe4 – The Human Factor: Your Strongest Defence Against Next-Gen Cyber Threats

AISP X WIZLYNX GROUP

The Human Factor: Your Strongest Defence Against Next-Gen Cyber Threats

Cultivate and leverage strong security culture within your organisation to combat next generation cyber threats, such as Generative AI and Deepfakes.

Register Now!

14 Nov 2024 | 2.30PM - 6PM

Justco @ Marina Square

Organised by:

Gartner reports that 93% of organisations are using or considering Generative AI (GenAI) at work. While beneficial, this technology also presents new cybersecurity challenges.

Cyber adversaries are using GenAI to create sophisticated social engineering attacks, including convincing phishing emails and deepfakes. Verizon's 2023 Data Breach Investigations Report reveals that 74% of data breaches stem from social engineering and human error.

To combat these next-generation threats, organisations must build a strong security culture. This involves implementing robust technical defences and empowering employees to be the first line of defence against cyber-attacks.

On 14 November, join wizlynx group and KnowBe4 to learn how you can cultivate a resilient security culture in your organisation. Learn strategies to educate and empower your workforce, enabling them to make smarter security decisions and protect your organisation from evolving cyber threats.

Enhancing Your Organisation's Cybersecurity and Security Awareness Training with Wizlynx
Speaker: wizlynx group

Did you know that the human factor is a major contributor to data breaches? In fact, according to Verizon's 2022 Data Breach Investigations Report, 82% of data breaches have been linked to human-

back to top

related security weaknesses. This often involves employees succumbing to phishing attacks, other forms of social engineering tactics, and unauthorized use of employee credentials.

Join us to learn more about wizlynx's Managed Cyber Security Services and KnowBe4's latest artificial intelligence-driven phishing to secure your organisation's assets in the cyberspace.

The Art & Science of Deception: How Our Thoughts and Actions Can Be Hacked and Hijacked
Speaker: KnowBe4

Cybersecurity isn't just about technology — it's about people. This presentation explores how social engineering exploits human behaviour and why a strong security culture is our best defence against sophisticated attacks like Generative AI and Deepfakes.

The session covers:

- Deceptions in successful security breaches
- Building a human firewall through security culture
- Strategies for organisation-wide security awareness

Who should attend?
CISOs, Cyber Security Managers, IT Managers, HR Practitioners, Compliance Managers
Kindly RSVP by 4th November 2024. We look forward to welcoming you in person.

Date: 14 November 2024, Thursday
Time: 2.30PM – 6PM
Venue: JustCo @ Marina Square
Registration: https://forms.office.com/r/16f7kvfRpU

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
2-3 Nov	Digital for life Festival by IMDA	Partner
5 Nov	CISO Meetup – What is the role of a CISO	AiSP & Partner
6-7 Nov	STACK 2024 Developer Conference	Partner
6-8 Nov	Singapore FinTech Festival (SFF) 2024	Partner
7 Nov	TCA24 Gala Dinner	AiSP
11-14 Nov	Cisco Live 2024 Melbourne	Partner
12 Nov	Learning Journey to Cisco for Raffles Institution	AiSP & Partner
14 Nov	CPP Event with Wizlynx	AiSP & Partner
14 Nov	CISO Canberra 2024	Partner
19 Nov	SVRP Awards Ceremony	AiSP
19-20 Nov	CISO New Zealand 2024	Partner
23 Nov	DFL SilverTech Carnival	Partner
26-28 Nov	Australian Cyber Conference Melbourne 2024	Partner
27-28 Nov	CDIC Conference 2024 Bangkok	Partner
29 Nov	Learning Journey to I-Sprint for NYP	AiSP & Partner
7 Dec	Ladies in Cyber Career Sharing for PME	AiSP & Partner
13 Dec	RP Community Day	Partner
16-19 Dec	Learning Journey to KL for LIC	AiSP

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

back to top

CONTRIBUTED CONTENTS

Article from CISO SIG

Ee Lin is the Deputy Director of CISO & Governance at HTX, where she leads cybersecurity strategies and governance for Singapore's Home Team Departments. With over 15 years of experience across both public and private sectors, Ee Lin is recognised for her expertise in strategic cybersecurity and risk management, and is dedicated to fostering the next generation of cybersecurity professionals.

1. Introducing a CISO with a Deep Interest in Cybersecurity
As a CISO, my passion for cybersecurity goes beyond just a profession—it's a mission to protect the infrastructure and public assets vital to Singapore's safety and economy. With a natural curiosity about how things work and a desire to solve complex problems, cybersecurity became an ideal path for me to apply that passion in a meaningful and impactful way.

I didn't enter the field of cybersecurity with the specific goal of becoming a CISO. My journey began with a focus on understanding the challenges within the digital landscape and using that knowledge to protect vital systems. As I became more deeply involved in solving complex cybersecurity challenges, I realised the potential to make a real-world impact in safeguarding both systems and people. Over time, the opportunities I encountered, along with my growing understanding of the industry, led me naturally into this leadership role. Today, I align cybersecurity efforts with business strategy, ensuring that security is not just an operational function but a strategic enabler for organisational resilience.

2. What Brought You to the Cybersecurity Industry?
I began my career in the defence sector, where I developed a strong sense of mission to protect vital systems that impact our nation. Defence work instilled in me a mindset focused on protection and security. As the digital landscape evolved, it became clear that these challenges were no longer confined to defence but had expanded into the business, public, and private sectors. Cybersecurity became a natural and necessary pivot for me.

Cybersecurity provides the satisfaction of tackling complex and ever-evolving challenges. Each day brings new and unpredictable problems, from advanced persistent threats to zero-day vulnerabilities, ensuring that no two days are ever the same. This constant stream of challenges has kept me engaged and provided opportunities to innovate and continuously improve security practices. This continuous evolution is what ultimately drew me deeper into the field.

back to top

3. What Were Your Defining Moments in This Industry, and What Helped You Achieve Them?

Several defining moments have shaped my journey, but mentorship—both being mentored and mentoring others—has been at the heart of my growth. Early in my career, having the right mentors made a significant impact on how I approached cybersecurity. They helped me see that it wasn't just about technical challenges but about thinking strategically and aligning cybersecurity with broader business objectives. These mentors encouraged me to embrace difficult challenges and broaden my perspective beyond technical expertise.

As I progressed, I became equally passionate about mentoring others. Passing on the guidance I received and helping others navigate the complexities of the industry is one of the most rewarding aspects of my role. I am deeply committed to developing the next wave of cybersecurity leaders.

Another defining moment was my involvement in the global cybersecurity community. Contributing to discussions at international forums, writing thought leadership pieces, and learning from others in the field has kept me at the cutting edge of industry developments. These connections have broadened my understanding and reinforced the importance of collaboration and diversity of thought in solving today's security challenges.

4. What Do You Love Most About Your Role?

What I love most about being a CISO is the dynamic and unpredictable nature of the role. Cybersecurity is constantly evolving, and each day brings new challenges that require innovative solutions. This constant learning curve keeps me on my toes, and while it can be stressful, the satisfaction of overcoming difficult challenges with a trusted team is incredibly fulfilling.

Seeing the tangible impact of my work is another aspect I greatly value. The security of vital infrastructure directly affects millions of people, and knowing that my efforts help protect essential services and make a real difference in the lives of Singaporeans gives me a deep sense of purpose. Securing systems that so many people rely on every day makes the hard work worthwhile.

Additionally, the opportunity to influence organisational strategy and guide security efforts at both operational and strategic levels allows me to contribute to business success while safeguarding against risks. Helping teams and organisations become more resilient in the face of cyber threats is one of the most rewarding aspects of the role.

5. What Are Some of the Trends in the Market Lately, and What Will Emerge in the Future?

One of the most significant trends today is the integration of AI with existing infrastructure to bolster security. AI and machine learning (ML) have become essential for automating threat detection, streamlining responses, and identifying vulnerabilities. This not only

back to top

improves security posture but also enables organisations to scale their defences more effectively against sophisticated threats. AI's role in cybersecurity will continue to grow, particularly as AI-driven solutions integrate more into cloud environments.

AI-driven solutions are also transforming proactive threat detection by analysing vast datasets to identify anomalies that human analysts might miss. In the near future, we can expect AI-automated incident response systems to become more common, enabling teams to focus on high-priority issues while AI handles repetitive tasks. However, adversaries are also leveraging AI for attacks, making it essential for security teams to continue innovating.

Beyond AI and cloud, we're seeing a growing focus on securing operational technology (OT) and supply chains. As more critical infrastructure becomes digitised, OT security becomes vital in ensuring that essential services aren't disrupted by cyber incidents. Additionally, ensuring the security of supply chains—especially those involving third-party vendors—is becoming a key concern for organisations worldwide.

Looking ahead, cyber resilience will take centre stage. It's not just about preventing attacks but ensuring rapid recovery and continued operation when they occur. AI-driven automation and self-healing systems will be key components in achieving this. As threats evolve, organisations must focus on both prevention and recovery, maintaining business continuity in an increasingly complex threat landscape.

6. What Do You Think Is the Role of CISO?

The CISO role is fundamentally about risk management. It's not just about the technical aspects of cybersecurity but about communicating risk in business terms that resonate with stakeholders at every level—from the boardroom to operational teams. Managing relationships and aligning the concerns of diverse groups within the organisation is essential to ensuring cybersecurity is understood as a strategic enabler of business success rather than a barrier to progress.

Being a CISO also involves deep engagement in strategic discussions. We're not simply approving or "rubber-stamping" decisions but challenging them when necessary to ensure cybersecurity risks are thoroughly evaluated and mitigated. While regulatory compliance is crucial, the focus needs to go beyond compliance to build a proactive and resilient security posture that anticipates future risks.

Fostering a culture of security is also key. A CISO must ensure that cybersecurity is not seen as an isolated function but as a shared responsibility across the organisation. Strong leadership and the ability to influence teams to prioritise security in their daily activities are crucial for long-term success.

back to top

7. What Can We Do to Encourage More People to Join the Cybersecurity Sector?

To bring more talent into the sector, we must start by demystifying cybersecurity. It's often seen as highly technical, which can deter those without a technical background. We need to show that cybersecurity involves much more—it's about strategy, communication, and risk management, alongside technical skills. Highlighting the variety of roles available will help attract a broader range of talent.

We also need to emphasise the societal impact of cybersecurity. Many people are motivated by the opportunity to make a difference, and cybersecurity offers the chance to protect vital infrastructure and secure individuals and businesses from threats. By positioning it as a career with purpose, we can inspire more people to join.
Fostering diversity and inclusion is also essential. Cybersecurity benefits from diverse perspectives, and creating a supportive and inclusive environment will help break down barriers. Mentorship programmes, scholarships, and outreach initiatives will be critical in bringing more talent into the industry.

Finally, raising awareness early is crucial. By introducing cybersecurity concepts in schools and universities and providing hands-on opportunities like hackathons and internships, we can spark interest from a young age, showing students that it's a dynamic and rewarding career path.

8. What Do You Want to Achieve or Contribute to the Cybersecurity Ecosystem?

I believe that making an impact starts within my organisation. My goal is to foster a culture where cybersecurity is integrated into every operation. This builds trust, collaboration, and innovation, creating an environment where security is a core part of everything we do.

Once this culture is well-established, I aim to expand that influence outward to the broader cybersecurity ecosystem. I want to contribute to building a resilient and inclusive ecosystem by mentoring the next generation of cybersecurity professionals. By providing leadership and guidance, I hope to help develop future leaders who will drive the industry forward.

Promoting diversity and inclusion is central to my vision. Diverse teams are better equipped to solve complex problems, and I want to create an environment where everyone feels safe, valued, and empowered to contribute. Cybersecurity is a collective responsibility, and together we can achieve far more.

9. Any Advice for Cybersecurity Professionals?

My advice for cybersecurity professionals is to remain curious and adaptable. The field is constantly evolving, and staying ahead requires a commitment to continuous learning—whether through formal training or by staying up to date with the latest trends. Cybersecurity is not static, and neither should your skills be.

back to top

It’s also important to remember that cybersecurity is a team effort. Build strong relationships and collaborate with your peers—trust and communication are key. Don’t hesitate to ask for help, share insights, or mentor others. Collaboration is essential in solving complex cybersecurity challenges.

Resilience is another crucial aspect. There will be breaches and setbacks, but how you respond is what truly matters. Learn from challenges and turn them into opportunities for growth. Resilience will help you navigate tough situations and keep moving forward. Lastly, always prioritise time for family and friends. They provide invaluable emotional support, especially during overwhelming moments. Balancing your professional life with personal relationships is key to maintaining your emotional health. Know your limits, and engage in activities that help you unwind—whether it’s a hobby or travelling. Taking time for yourself is essential to staying grounded and resilient in this demanding field.

Article from AI SIG

Ensuring Responsible, Fair and Ethical AI: The Critical Role of AI Governance

Dr Koh Noi Sian is a Senior Lecturer at Nanyang Polytechnic’s School of Information Technology, with over 10 years of experience teaching Machine Learning and Artificial Intelligence. Noi Sian has presented at multiple international conferences, and her research papers have been widely cited by academics and the media. She was also the recipient of the prestigious President’s Award for Teachers in 2019.

As AI technologies become more embedded in our daily lives, the impact of their errors is becoming increasingly apparent. AI systems now make decisions that affect hiring, lending, policing and even healthcare, but these systems are not infallible. Just as cybercriminals adapt to new technologies, the risks associated with unchecked AI require a proactive and responsible governance framework to ensure that AI is ethical, transparent and accountable.

When AI Goes Wrong: The Consequences of Poor Governance

Poorly governed AI systems have demonstrated negative real-world impact. For example, a study by Buolamwini & Gebru (2018) revealed that facial recognition algorithms from major tech companies were significantly less accurate at identifying women and people of colour compared to white males. Such bias in AI can have severe consequences, as seen in an article titled “*Wrongfully Accused by an Algorithm*,” published by *The New York Times* on June 24, 2020, where police wrongfully arrested an individual based on biased AI facial recognition matches. This underscores the need for transparency and fairness in AI systems.

back to top

From biased recruitment algorithms[1] to discriminatory credit scoring systems[2], AI has the potential to amplify societal biases and cause harm when not governed effectively. These incidents highlight the critical need for AI governance frameworks to prevent unintended consequences and ensure that AI is used ethically.

Learning from Responsible AI Principles

To prevent such errors, organizations must adhere to **responsible AI principles—**a set of guidelines designed to ensure that AI technologies are fair, transparent, and accountable. These principles[3] provide the foundation for building trustworthy AI systems:

- **Fairness**: AI systems must be free from bias and discrimination. Ensuring fairness requires organizations to actively detect and mitigate biases in the data and algorithms used in AI systems.
- **Transparency and Explainability**: Users and stakeholders must be able to understand how AI decisions are made. This means making AI systems explainable and transparent, so that their outcomes can be scrutinized and understood by non-experts.
- **Accountability**: Clear accountability structures must be in place to ensure that organizations take responsibility for the actions and decisions of their AI systems. This includes establishing mechanisms for remediation when things go wrong.
- **Privacy and Security**: AI systems must safeguard personal data and comply with data protection regulations. Organizations must ensure that their AI models protect user privacy and are resilient to cyber threats.
- **Human Centricity**: AI systems should be designed with the goal of benefitting people and operating safely, minimizing risks and preventing harm, whether directly or indirectly.

Leveraging AI Governance Frameworks to Build Trustworthy Systems

Governance frameworks offer organizations a structured approach to embedding responsible AI principles into the design, development and deployment of AI systems. Just as businesses adopt cybersecurity frameworks to protect against phishing attacks, AI governance frameworks[4] provide essential safeguards against AI failures. Here are some ways on how organizations can leverage these frameworks to build trustworthy AI systems:

1. **Establish Clear Internal Governance Structures**: Organizations must create dedicated teams or committees responsible for overseeing AI ethics and

[1] Jeffrey Dastin, "Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women," *Reuters*, October 11, 2018.
[2] Edmund L. Andrews, "How Flawed Data Aggravates Inequality in Credit," *Stanford University*, August 6, 2021.
[3] Infocomm Media Development Authority (IMDA), *Model AI Governance Framework*, 2019, published on Artificial Intelligence | SG Digital | IMDA
[4] Singapore Computer Society. (n.d.). AI ethics body of knowledge (BoK). Retrieved from https://www.scs.org.sg/ai-ethics-bok

back to top

governance. These structures help ensure accountability and provide a platform for addressing ethical concerns during the AI development process.

2. **Conduct Regular Audits for Bias and Fairness**: Governance frameworks should include regular audits of AI systems to detect and mitigate biases. By using fairness metrics and testing AI models on diverse datasets, organizations can reduce the risk of discriminatory outcomes.
3. **Ensure Transparency and Explainability in AI Models**: Governance frameworks should mandate that AI systems be transparent and interpretable. Organizations can use tools like explainable AI to help users understand how AI arrives at its decisions, making the system more accountable and trustworthy.
4. **Implement Robust Risk Management and Impact Assessments**: Just as organizations use risk assessments in cybersecurity, AI systems should undergo impact assessments to identify potential ethical risks. These assessments help organizations anticipate and mitigate issues such as bias, discrimination or safety hazards.
5. **Engage with Stakeholders and Affected Communities**: A strong governance framework emphasizes stakeholder engagement, allowing organizations to gather feedback and address concerns from those impacted by AI systems. This helps ensure that AI technologies align with societal values and meet the needs of diverse groups.

Avoiding AI Pitfalls: The Role of Governance

As AI becomes more pervasive, the demand for responsible AI will only continue to grow. Without the guardrails of a governance framework, AI systems can easily go astray. Failure to account for biases, a lack of transparency, or inadequate risk management can lead to incidents that erode public trust and cause real harm. By implementing governance frameworks, organizations can avoid these pitfalls and ensure that their AI technologies are ethical, fair and transparent.

Responsible AI is not just a matter of ethical obligation—it is a strategic imperative for building trustworthy, reliable and fair AI systems that can thrive in today's rapidly evolving digital landscape. By leveraging AI governance frameworks, organizations can ensure their AI systems deliver positive outcomes and prevent the harm that can result from poorly governed AI.

References:

Hill, K. (2020, June 24). *Wrongfully accused by an algorithm*. The New York Times. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77-91).

back to top

Contact Information:Koh Noi Sian (Dr)
School of Information Technology
Nanyang Polytechnic
E-mail: koh_noi_sian@nyp.edu.sg

Article from AJCCA Sponsor - Wissen

A New Era in Cybersecurity: Announcing C|EH v13

The cybersecurity industry is in the midst of a pressing and all too critical challenge: a massive skills shortage at all levels of the profession. In fact, according to the U.S. Bureau of Labor Statistics, there are currently as many as 700,000 open cybersecurity positions, with that number set to grow.

That is why we are thrilled to announce today a major leap forward in our mission: the launch of **Certified Ethical Hacker CEH v13**, the world's first ethical hacking program that fully integrates artificial intelligence learning and skills. This groundbreaking certification program marks a new era in cybersecurity education, where AI takes center stage.

The Stakes Have Changed:
The cybersecurity industry is at a crossroads. We're no longer just talking about data breaches – we're facing a new breed of AI-powered threats that are faster, smarter, and more sophisticated than ever before. This isn't just a challenge; it's a fundamental shift in the cybersecurity landscape.

EC-Council Leads the Charge:
For over two decades, EC-Council has been at the forefront of cybersecurity training, setting the global standard with our Certified Ethical Hacker (CEH) program. Today, we're proud to announce a groundbreaking evolution: **CEH v13**, the world's first ethical hacking program fully integrating AI learning and skills.

Why This is a Game-Changer:

- **Industry First:** C|EH v13 isn't just an update; it's a paradigm shift. We're the first to fully integrate AI into ethical hacking training, equipping professionals with the skills to combat the threats of tomorrow, today.
- **Closing the Skills Gap:** The cybersecurity industry is facing a critical shortage of skilled professionals, and the rise of AI only exacerbates this challenge. C|EH v13 directly addresses this gap, creating a new generation of AI-savvy cybersecurity experts.
- **Raising the Bar:** By integrating AI into our flagship program, we're not just keeping pace with the industry; we're setting a new standard for excellence in cybersecurity training.

back to top

Benefits for Your Organization:

- **Future-Proof Your Security:** Don't wait for AI-powered attacks to happen; be prepared. CEH v13 empowers your team to proactively identify and mitigate these emerging threats.
- **Gain a Competitive Advantage:** In today's rapidly evolving threat landscape, organizations with AI-powered cybersecurity capabilities have a distinct advantage. Invest in CEH v13 and position your organization as a leader in cybersecurity.
- **Attract and Retain Top Talent:** Demonstrate your commitment to innovation and employee development by offering the most advanced cybersecurity training available.

The Future of Cybersecurity is Here:
C|EH v13 is more than just a certification; it's a commitment to staying ahead of the curve and empowering cybersecurity professionals with the skills they need to build a safer digital world.
We believe that empowering ethical hackers with the right skills is crucial to building a safer digital world, closing the massive cybersecurity skills gap, and providing individuals around the globe with a pathway into highly valuable and rewarding careers. CEH v13 is a testament to our commitment to staying ahead of the curve and providing the most relevant and advanced cybersecurity training available, and we are proud of all of those who have contributed towards making this new version the very best in the industry.

Join us in shaping the future of cybersecurity.
Learn more about CEH v13 powered with AI today! Email enquiry@wissen-intl.com for more information.

Article from AJCCA Sponsor - Sailpoint

SailPoint unveils third-annual Horizons of Identity Security report

Organizations with advanced identity security experience "bending of the curve," see accelerated value from reduced cyber risk to increased workforce productivity

Key findings:

- 83% of organizations reported fewer identity-related security issues due to their security investments in 2023
- Organizations with mature identity security reported seeing disproportionately higher returns, "bending" the identity security-to-value curve
- Organizations with more mature identity security practices are, on average, seeing about 1.7 times higher adoption of AI-powered identity security solutions

back to top

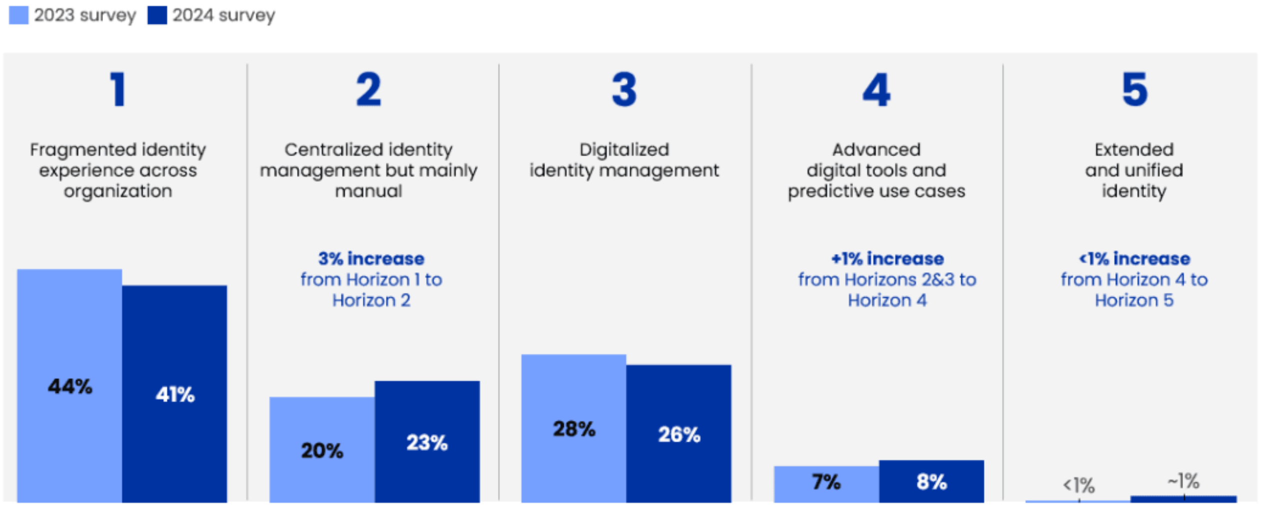
- Machine identities are expected to increase about 30% in the next 3-5 years, growing faster than all other identity types, making coverage of these identities increasingly important for organizations of all maturity levels

AUSTIN, Texas – Oct. 8, 2024– SailPoint Technologies, Inc., a leader in enterprise identity security, today released the findings from the 2024-2025 edition of its annual research report, 'The Horizons of Identity Security.'This year's report reveals that while most organizations are still in the early horizons of their identity security journey, those who achieve maturity are seeing disproportionately higher returns for every dollar spent.

The value of identity security remains largely untapped today. Of the organizations surveyed, roughly 41%remain at the very beginning of their identity security journey with only 10% progressing to the more advanced stages; this large gap highlights the significant opportunities for organizations to realize the full potential of identity security. Our research suggests that organizations that mature their identity security practice can "bend" the identity security-to-value curve, delivering disproportionate economic impact.These disproportionately higher returns are observed through three key factors: reduced cyber risk, increased business value, and improved productivity. More mature organizations gain disproportionate reductions in risk, higher topline business value, and increased workforce productivity.

With 41% of organizations still in Horizon 1, significant opportunity exists to unlock the "full potential" of identity security

Distribution of enterprises across the 5 customer identity journey horizons



Note: Horizon 1 is updated to include the unpenetrated IAM market (who are screened out of later sections of the survey)

"Achieving identity security maturity does not have to be an arduous undertaking. With the right strategy, operating model, technology, and expertise, organizations can get there, seeing disproportionately higher returns and bending the identity security-to-value curve for their organization," said Matt Mills, President, SailPoint. "Typically, we see spending on cybersecurity delivering linear returns, yet organizations around the world and across industries have already begun to prove advanced identity security can reap compounding benefits."

back to top

The 2024 Horizons of Identity Security report outlines several areas where mature identity security programs have progressed and unlocked new value pools, such as:

- Stronger coverage of machine identities, the fastest growing identity class: Organizations with mature identity security have 87% more coverage of non-human or machine identities, such as bots, compared to 28% for organizations in the early stages of their identity journey. This is significant because survey results also indicate that machine identities are highly fragmented with organizations and likely to grow faster than any other identity class. According to past survey results, machine identities represent more than 40% of total identities within a given organization, and one-third of respondents expect machine identities to increase by 30% in the next year.
- Higher coverage of third-party identities: Organizations with mature identity security have up to 50% higher coverage of third-party identities compared to those in the early stages of their identity journey.Third-party identities are an increasingly important identity class as more and more businesses are turning to third-party providers for critical services, therefore increasing the attack surface.
- Leveraging identity data intelligence:Organizations with mature identity security are two times more likely to leverage identity data to create actionable intelligence and power new use cases such as intelligent guidance for user access, context-aware security policies, and intelligent access reviews. This is significant because it can enable more accurate and timely access decisions, a key to reducing security risk.
- Higher adoption of AI and willingness to invest in GenAI: Organizations with mature identity security have nearly two times higher adoption of AI-powered identity solutions, which has proven to create scalable solutions and enhance productivity.Organizations with mature identity security have the foundations to invest in scalable GenAI-powered use cases, prioritizing tools for workflow creation, user entitlements, role descriptions, and natural language search. Alternatively, most early-stage organizations remain focused on automating basic help desk tasks.
- Lower cyber insurance premiums: 92% of survey respondents report that insurers assess their cyber capabilities before setting premiums. Interestingly, more than 7 in 10 identity security decision makers view identity security as one of the three most impactful security capabilities determining cyber insurance premiums.

Over the last three years, our research and experiences have confirmed that the future of identity security will be shaped by integrated identity programs across diverse technology environments. This integration includes unified access controls providing visibility across all identity types, integration with security operations, and support for machine identity management and actionable intelligence.Additionally, with advanced next-generation identity security, access decisions are increasingly driven by AI-powered analytics, which use context-aware policies to enhance security through anomaly detection, identity pattern recognition, and behavior analysis. Organizations can utilize these next-generation capabilities to set the north-star vision to reach the future of identity security.

back to top

A SailPoint customer, RWE reached identity security maturity in just six months. RWE's identity security transformation included moving from on-premises manual identity management to a cloud, AI-driven solution enabling identity security at scale. The company was able to implement more comprehensive coverage, scaling its identity security from 2.5K to roughly 30K user accounts. Notably, it reduced onboarding time from 25 days to less than 3 hours on average, improving productivity. And—key to maturing an identity security program—RWE implemented a unified approach to identity, moving from zero to 30 business units sharing an identity strategy. These findings underscore that committed investments in identity security help organizations safeguard their assets and gain competitive advantages in the digital age.

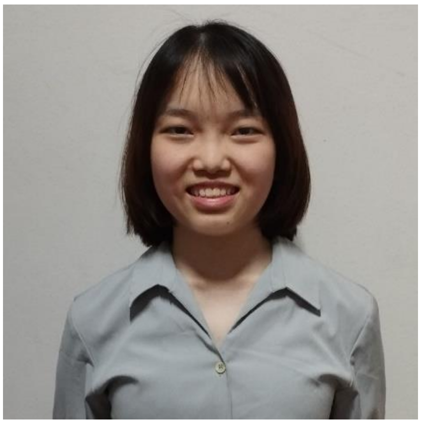
Learn more about Horizons at SailPoint's flagship "Navigate: Identity Security Transformed" conference kicking off in Orlando and followed by a series of global events in São Paulo, Singapore, Sydney, and London. To register, visit the Navigate website.
Download a copy of the 2024-2025 Horizons of Identity Security report and take the maturity assessment.

About the research and methodology
'The Horizons of Identity Security' surveyed identity and access management decision-makers across the globe to assess their capabilities across identity security horizons and define the future of identity. This year's report is based on insights from 350 global cybersecurity senior leaders in information technology, cybersecurity, and risk. Of those surveyed, more than half work for organizations with more than 10,000 employees. Unless otherwise indicated, all data points in this press release relate to the findings of this survey.

About SailPoint
SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.
# # #
Media Relations for SailPoint
Samantha Person
Senior Manager, PR & Corporate Communications
512-923-4053
Samantha.Person@SailPoint.com

back to top

Article from SVRP 2023 Gold Winner, Ho Xin Ying [NYP]



How do you think SVRP has directly impacted your cybersecurity journey?
I was previously awarded the bronze award in 2022 and SVRP has affirmed my contribution towards the cybersecurity community. I think that the award is also useful to prove that my contribution towards the community has been verified by a reputable company.

How has SVRP inspired you to contribute to the cybersecurity field?
Personally i find it quite enjoyable to be able to make an impact on the cybersecurity field. I think that svrp encouraged me to contribute in a more holistic manner as i usually focus more on events and skills rather than leadership.

What motivates you to be a student volunteer?
I enjoy being able to help others and using my knowledge and abilities to help them. I like to volunteer for not just cybersecurity field but also community events in general.

How would you want to encourage your peers to be interested in cybersecurity?
With the growth of IT cyber security is an indispensable part of our everyday lifes and i would like to help them recognise the importance of cyber security. even if they are not interested in IT, i think that it is an important skill to have to keep ourselves cybersafe online.

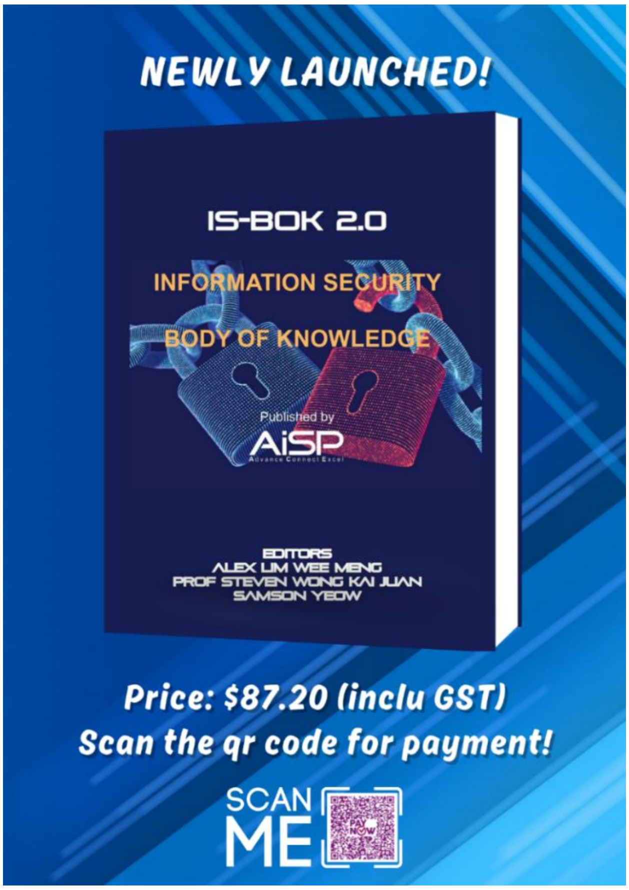
back to top

PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®)

Body of Knowledge Book (Limited Edition)

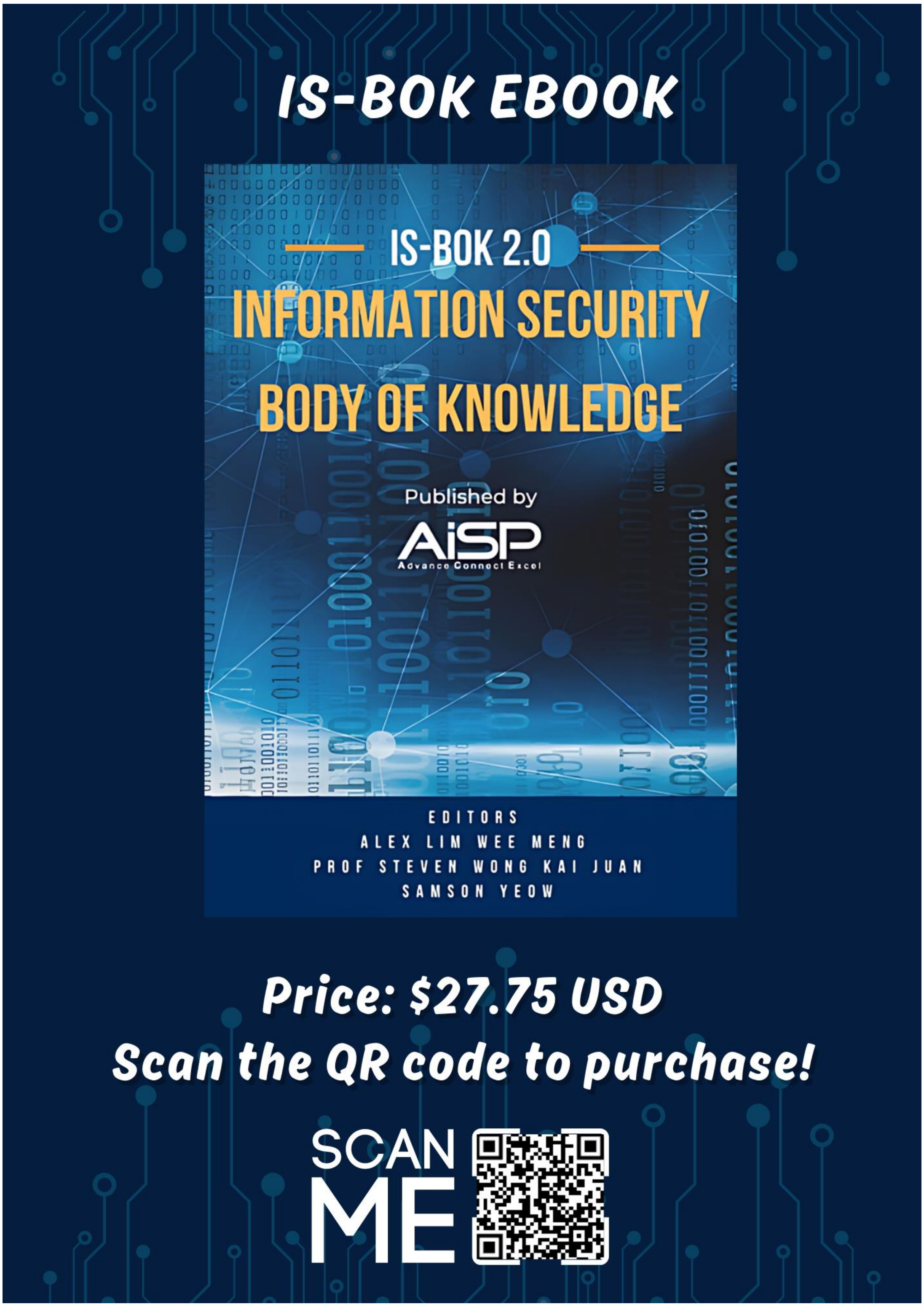
Get our **Limited Edition** Information Security Body of Knowledge (BOK) Physical Book at **$87.20 (inclusive of GST)**.



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

back to top

Body of Knowledge E Book



IS-BOK EBOOK

IS-BOK 2.0
INFORMATION SECURITY
BODY OF KNOWLEDGE

Published by
AiSP
Advance Connect Excel

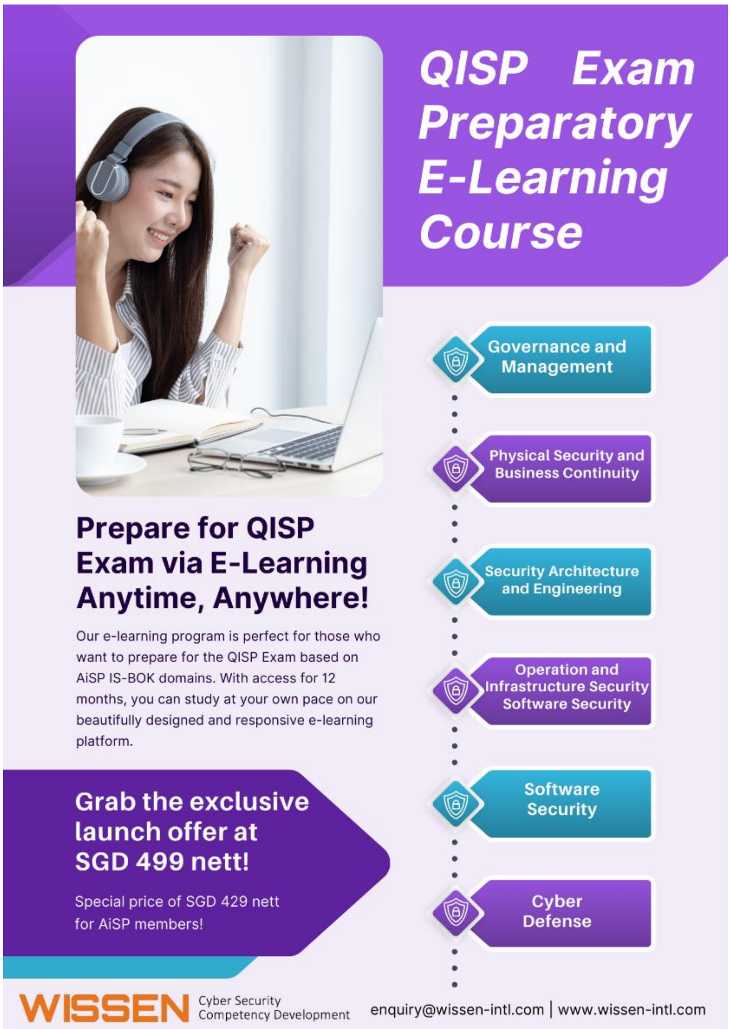
EDITORS
ALEX LIM WEE MENG
PROF STEVEN WONG KAI JUAN
SAMSON YEOW

Price: $27.75 USD
Scan the QR code to purchase!

SCAN ME

back to top

Online 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!

back to top

MEMBERSHIP

AiSP Membership

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

Complimentary Affiliate Membership for NTUC Members
AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2024) from 1 Jan 2024 to 31 Dec 2024. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. This does not include Plus! card holder (black-coloured card), please clarify with NTUC on your eligibility.

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

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

CPP Membership

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

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

For any enquiries, please contact secretariat@aisp.sg

back to top

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

Membership Renewal
Individual membership expires on 31 December each year. Members can renew and pay directly with one of the options listed here. We have GIRO (auto - deduction) option for annual auto-renewal. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.
Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!

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

AiSP Corporate Partners

Acronis
athena dynamics
AZ ASIA-PACIFIC
BD
BeyondTrust
BLACKPANDA
CISCO
CLIXER
C8N+FINITY
CSA SINGAPORE
CSIT Centre for Strategic Infocomm Technologies
CYBERSAFE YOUR SECURITY, OUR PRIORITY
DBS
DETACK
DSTA Defence Science & Technology Agency
eclypsium
ENSIGN INFOSECURITY
FORTINET

back to top

Genesis NETWORKS

GOVTECH SINGAPORE

Grab

HORANGI CYBER SECURITY

HTX

HUAWEI

illumio

image engine

INTfinity

IT SEC ASIA

KnowBe4 Human error. Conquered.

MAGNET FORENSICS®

MySQL™

M.TECH Your Preferred i-Security Partner

oneSECURE®

opentext™

OPSWAT.

PARASOFT.

proofpoint.

RAJAH & TANN CYBERSECURITY

Responsible Cyber

RSM

SailPoint.

SCANTIST

Schneider Electric

Security Scorecard

Singtel

softScheck We Build Trust

ST Engineering

TEMASEK

tenable

TREND MICRO™

Veracity Trust Network

back to top

VOTIRO

wizlynx group

WISSEN
Cyber Security Competency Development

xcellink.pte.ltd.
completing your technology chain

YesWeHack

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

ITE
Institute of Technical Education

NYP NANYANG
THE INNOVATIVE POLYTECHNIC

NGEE ANN
POLYTECHNIC

NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

NUS
National University of Singapore

REPUBLIC POLYTECHNIC
DISCOVER. TRANSFORM. ACHIEVE

SiT
SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SMU
SINGAPORE MANAGEMENT UNIVERSITY

SUTD
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek
POLYTECHNIC

back to top

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

Freddy Tan
Director

Vincent Toh
Associate Director

Elle Ng
Senior Executive

Karen Ong
Executive

AiSP Advance Connect Excel

🌐 www.AiSP.sg
✉ 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.

back to top