

News & Update

- SVRP
- AiSP Cyber Wellness
- CAAP
- Special Interest Groups
- The Cybersecurity Awards
- Corporate Partner Event
- Ladies in Cyber
- Regionalisation
- CREST
- Upcoming Events

Contributed Contents

- Cloud Security SIG:
Should Cloud Access be considered as Privileged Access? Thoughts around Cloud Access Management Strategies from CSCIS.
- SVRP 2023 Gold Winner,
Muhammad Dinie Bin Baharudin

Professional Development

Membership

NEWS & UPDATE

Continued Collaboration

AiSP would like to thank Schneider Electric and Security Scorecard for their continued support in developing the cybersecurity landscape:



News & Updates

MOU Renewal with ISC2 Singapore Chapter on 2 Apr 24

2 April 2024 marks another milestone as AiSP signed our MOU renewal with ISC2 Singapore Chapter.



Milipol Asia Pacific on 3-5 April

AiSP was at MBS Convention Centre at the Milipol Asia Pacific from 3-5 April.



AiSP EXCO Lead Soffenny participated in closed-door discussion with PM Lee on 16 April

Ms Soffenny Yap, EXCO Lead for PME Programme participated in a closed door session with 11 other Union Reps in a Tea Session with PM Lee at Istana on PME Issues on 16 April. Thank you Soffenny to be the voice of our AiSP PMEs and share with PM Lee & PS on the issues faced by our PMEs.



Photo Credit: NTUC

Black Hat Asia on 18 and 19 April

AiSP was at MBS Convention Centre for the Black Hat Asia event from 18-19 April.



[back to top](#)

AiSP 15th Anniversary Dinner on 18 April

It was a warm and wonderful night on 18 April celebrating AiSP 15th Anniversary over a dinner with our current and past exco members, ever supporting partners and agencies graced with the presence of our AiSP Patron, SMS Tan Kiat How.

AiSP would like to take this opportunity to thank all our members and partners who have helped made this 15 years possible! Let's continue working together to strengthen cybersecurity and make the digital world a safer place for all.



Member Acknowledgment

Interview with AiSP Vice President Mr Breyvan Tan



What is your vision for your contribution in AiSP?

My vision for contributing to AiSP aligns closely with its mission to be the pillar for information security professionals and its vision to foster a safe cyberspace through a strong and vibrant cybersecurity ecosystem. I aim to achieve sustainability through the focus on talent development, which I believe is fundamental to strengthening our industry. To realise this, I plan to actively engage with all stakeholders—from our individual members, academic partners and corporate partners to government, and the broader industry. This engagement will occur through diverse platforms and opportunities for interaction, ensuring we harness a wide range of insights and expertise. I envision a collaborative approach where members, partners, and stakeholders are not just participants but active contributors to our initiatives. By encouraging them to share their views, contribute ideas, and volunteer in our activities, we create a vibrant, participatory environment that enriches AiSP and the cybersecurity ecosystem at large. The success of these efforts will circulate back to strengthen our ecosystem, benefiting all involved and advancing our shared goal of a safe cyberspace. This cycle of contribution, improvement, and benefit underscores the sustainable model I aim to foster within AiSP.

What do you think is the biggest issue in the Cybersecurity Industry?

Pulling a statement from our President Tony's recent interview, "The biggest issue in the cybersecurity industry is the ever-evolving nature of cyber threats". Among all cyber threats, I would like to highlight on ransomware attacks. These attacks not only lock and encrypt data, demanding ransom payments for release, but also have escalated in sophistication and frequency, causing significant disruptions to most enterprises, especially the SMEs. The impact of ransomware extends beyond immediate financial losses to long-term reputational damage and operational disruption, particularly troubling for SMEs where there are report shows that 60 percent of small companies close within 6 months of being hacked. This trend underscores the urgent need for enterprises to take concrete steps towards improving their cybersecurity posture and inevitably leads to the exposure of the next challenging issue, skills shortage. The cybersecurity industry faces a significant

[back to top](#)

shortage of skilled professionals, which can hinder the ability to defend against and respond to cyber threats effectively.

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?

To start with, I would first ensure I have a thorough understanding of AiSP's Mission, Vision, Values and Strategic goals. This will guide me in all my communications and interactions, ensuring that the message I deliver is consistent and aligned with the AiSP's goals. I will also actively engage external stakeholders by understanding their perspectives, concerns, and expectations. This allow me to demonstrate that AiSP values and considers external input and this would not only strengthens relationships but also enhances our credibility and relevance in the industry.

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

I am eager to contribute my expertise towards enhancing the growth and development of our members and the wider community. One of my primary goals is to enhance opportunities for continual upskilling among our members. This will be achieved not only by increasing the availability of resources but also by encouraging members to learn through active participation in events and conferences organised by AiSP. This will help to ensure that our current members remain relevant and well-equipped to meet industry needs and expectations. Additionally, I am passionate at supporting fresh graduates and career switchers who are joining the cybersecurity industry. I will look at programs tailored to help them smoothly and successfully start their careers in our profession, addressing the skills shortage challenge I mentioned earlier and infusing our industry with new talent and perspectives.

Student Volunteer Recognition Programme (SVRP)

Learning Journey to Philippines from 8 – 12 April

AiSP brought more than 30 students from different IHLs to Philippines for learning journey visits to the companies and schools from 8 -12 April.



Day 1 – 8 Apr: Visit to NCC Group

For the first day on 8 April, we visited NCC Group Philippines. Thank you WiSAP (Women in Security Alliance Philippines) for coordinating and NCC Group for hosting.



Day 2 – 9 Apr: Visit to Trend Micro Philippines

For the first visit of 9 April, we visited Trend Micro. Thank you WiSAP (Women in Security Alliance Philippines) for coordinating and Trend Micro for hosting.



Day 2 – 9 Apr: Cybersecurity Workshop by Acumen IT Training

For the second visit on 9 April, the students attended the Cybersecurity Workshop by Acumen IT Training, Inc. Thank you to our Corporate Partner, Wissen International for coordinating and Acumen IT Training Inc for hosting.



Day 3 – 10 Apr: Visit to CICC

On 10 April, as part of Singapore and Philippines 55th years bilateral relationship, we visited Cybercrime Investigation and Coordinating Center (CICC). Thank you WiSAP (Women in Security Alliance Philippines) for coordinating and CICC for hosting.



Day 4 – 11 Apr: Visit to Asia Pacific College

For the first visit on 11 April, we visited Asia Pacific College. Thank you WiSAP (Women in Security Alliance Philippines) for coordinating and APC for hosting.



Day 4 – 11 Apr: Visit to Department of Environment and Natural Resources

For the second visit on 11 April, as part of Singapore and Philippines 55th years bilateral relationship, we visited Department of Environment and Natural Resources. Thank you WiSAP (Women in Security Alliance Philippines) for coordinating and DENR for hosting.



Day 5 – 12 Apr: Visit to Asian Institute of Management

To conclude the trip, we visited Asian Institute of Management (AIM) on the last day of the trip. Thank you AIM and AiSP Member, Mr Philip Kwa for hosting.



Learning journey with ITE College West to CrowdStrike on 16 Apr 24

On 16 April, AiSP brought 40 ITE College West students on a learning journey and visited our Corporate Partner, CrowdStrike. Hope the students have gained insights from the visit.



Visit to Grab office with Assumption English School on 17 April

On 17 April, AiSP brought 30 Students from Assumption English School on a Learning Journey where they have visited our Corporate Partner, Grab's office. Hope the students have gained insights from the visit.



Learning Journey to Tenable on 26 April

On 26 April, AiSP brought around 30 students from ITE West to our corporate partner Tenable office for Learning Journey. Thank you Tenable for hosting us and the insightful sharing!






Nomination Period:
1 Aug 2023 to 31 Jul 2024

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 2023 to 31 Jul 2024

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):

<p>Example A</p> <ul style="list-style-type: none"> + Leadership: 10 Hours + Skill: 10 Hours + Outreach: 10 Hours <p>Example B</p> <ul style="list-style-type: none"> + Leadership: 0 Hour + Skill: 18 Hours + Outreach: 18 Hours 	<p>Example C</p> <ul style="list-style-type: none"> + Leadership: 0 Hour + Skill: 36 Hours + Outreach: 0 Hour <p>Example D</p> <ul style="list-style-type: none"> + 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!

Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP Cybersec Conference 2024 on 15 May



AiSP CyberSec Conference 2024

SUPPORTING PARTNERS

ORGANISED BY

AiSP
Association of Information Security Professionals

SUPPORTING AGENCIES

SILVER SPONSORS

BRONZE SPONSORS

AiSP CyberSec Conference 2024

Sustaining Growth & Innovation Securely In This Challenging Business Environment

15 May 2024
Suntec Convention Centre

Guest of Honour: Mr. Tan Kiat How, AiSP Patron - Senior Minister of State, Ministry of Communications and Information & Ministry of National Development

BeyondTrust

AiSP
Advance Connect Excel

Zero Trust Security: Safeguarding Your Business in the AI-Powered Era

Kevin Pang | PAM Evangelist, BeyondTrust

Join Kevin as he navigates the transformative shift towards a perimeterless world and delves into the critical adoption of Zero Trust principles. Gain valuable insights to protecting your business in an agile fashion, unraveling the intricate strategies and cutting-edge technologies that are reshaping the landscape of cybersecurity in an interconnected and boundary-free digital realm.



Securing the Digital Supply Chain - Ensuring Trust in All of Your IT Infrastructure

Wes Dobry | Global Director, Sales Engineering

In recent years, there has been a significant surge in attacks on IT infrastructure, making it a prominent category of exploited vulnerabilities. Nearly half of all ransomware infections now target vulnerabilities in commonplace software and devices. This escalating threat landscape underscores the need for organizations to mitigate risks to their infrastructure from complex and global technology supply chains.



How to Strengthen Your Organisation's Last Line of Defense: Your Human Firewall

Philip Tnee | Head of North and South Asia | KnowBe4

"Social Engineering attacks, in the form of phishing, Business Email Compromise, and Ransomware attacks are becoming ever more commonplace. The number of cyberattacks that start by manipulating a human into allowing access to protected systems or sensitive information steadily increases.

Old-school awareness training does not hack it anymore. Your email filters have an average 7-10% failure rate; you need a strong human firewall as your last line of defence. This session will help you better understand how you can keep your users on their toes with security top of mind. It will also include a product demonstration of the innovative Kevin Mitnick Security Awareness Training Platform, which will show how easy it is to train and phish your users.

- Send fully automated simulated phishing attacks, using thousands of customisable templates with unlimited usage.
- Train your users with access to the world's largest library of up to date awareness training content.
- AI-Driven phishing and training recommendations based on your users' phishing and training history.
- Use assessments to gauge proficiency of your users in security knowledge and security culture attitudes.
- Easy user management using Active Directory or SCIM integration.



Recover Faster From Cyber Attacks with Digital Forensics

Jankang Tao | Regional Director, APAC

Business environments are increasingly experiencing complex threats and needed critical insights into incident response investigations, including ransomware attacks, data exfiltration, and business email compromise (BEC) scams. The increased need for DFIR is driven by the harsh reality facing today's organizations: that falling victim to a security event isn't a matter of if, but of when.

Today's corporate DFIR professionals are under enormous pressure to conduct fast and thorough investigations, especially when part of incident response. New approaches and technology can help DFIR professionals do their jobs faster and with more precision, enabling them to determine the root cause of incidents and address vulnerabilities in their environment.

In this session, our speaker will highlight:

- The importance of determining the root cause of incidents to increase your security posture and mitigate future cyber incidents
- Tactics and tools that help organizations manage the soaring volume of cybersecurity investigations as well as the diversity of data sources
- How modern solutions and automation can help organizations keep pace with the growing demands on cybersecurity teams



Malicious Bots: Protecting Your Digital Business From The Foot Soldiers Of Modern Cyber Attacks

Stewart Boucher | CTO of Veracity Trust Network

Learn what malicious bots are up to on your web estate (websites, web apps and mobile apps) and why this is impacting your opportunity for growth and exposing you to risk. Understand how to use innovation against bots to gain a competitive advantage and better secure your organisation from cyber threats.



Enterprise Journey Towards Digital Security

Veronica Tan | Director (Safer Cyberspace Division)
Cyber Security Agency of Singapore

"Transformation as usual" has become the new norm, replacing "business as usual", as new or emerging technologies such as cloud and Artificial Intelligence (AI) reshape the enterprise digital transformation journey. As the cybersecurity landscape evolves, enterprises should prepare to make the shift towards new frontiers and evolve their approach to achieve digital security.



Cybersecurity in a Budget, Essential Protections for your growing Business

Mohamad Azad Zaki Haji Mohd Tahir | President of
Brunei Cyber Security Association (BCSA) &
Deputy Chief Information Security Officer (ITPSS)

While recognizing the financial limitations of many SMEs and the common perception of cybersecurity as costly, this presentation will focus on essential, budget-friendly methods to protect your growing business. We'll explore identifying your most critical data ("crown jewels"), implementing low-cost practices like strong passwords and employee training, and utilizing affordable security solutions. We'll also guide you in prioritizing and implementing these solutions with practical steps and readily available resources.

Business owners of small and medium enterprises (SMEs) and Enterprise are only focused on business needs and are not aware of the digital risks and cybersecurity resources available for them. The purpose of the AiSP CyberSec Conference is to help Enterprises, SMEs and

individuals to be more cyber aware and the different solutions out in the market that can help them in it.

Organised by the Association of Information Security Professionals (AiSP), the AiSP CyberSec Conference is a unique event that brings together organisations to discuss the importance of being cyber aware and stay protected. The event will provide our speakers with the opportunity to share their experience, skills and knowledge to show how cybersecurity can help companies to stay protected. AiSP aims to elevate cybersecurity awareness among companies and establish a self-sustaining ecosystem with active participation from government agencies, business associations, cybersecurity communities, and solutions provider.

Our theme for this year conference is “Sustaining growth and innovation securely in this challenging business environment”.

Objectives of the conference include:

1. The importance of Cybersecurity for business growth and Innovation
 - What are the trends that are forcing customers to look for new ways to work and drive businesses
 - How businesses can leverage on technology to scale their businesses securely
2. The latest cybersecurity trends and tools available to protect your business from cyberattacks
 - What is the software that you can introduce into the organization
 - Areas to look out for
3. Cybersecurity best practices for SMEs and staff
 - Awareness
4. Getting support from the government to sustain Growth Enterprise Innovation Scheme
 - Areas to get help from the government in supporting developing innovative solutions, where Security can be built in rather than bolted later
5. The future of Cybersecurity
 - GenAI's Impact on Security

As part of AiSP Cybersecurity Awareness and Advisory Programme (CAAP), this event is for Singapore Enterprise and SMEs to know more about cybersecurity as a business requirement and how they can implement solutions and measures for cyber-resilience. CAAP hopes to elevate cybersecurity awareness as integral part of business owner's fundamentals and establish a self-sustainable support ecosystem programme with active participation from agencies, business associations, security communities and solutions provider.

Date : 15 May 2024

Time : 9AM – 3PM

Venue : Suntec Convention Centre

Guest of Honour:

AiSP Patron – Senior Minister of State, Ministry of Communications and Information & Ministry of National Development - Mr Tan Kiat How

Register here: <https://www.eventbrite.sg/e/802128306357?aff=oddtcreator>

Special Interest Groups

AiSP has set up four **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

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 CISO SIG Meetup on 5 June

AiSP
Advance Connect Excel

AiSP CISO SIG Meetup

AiSP Schneider Electric

AiSP CISO SIG Meetup

Foster Network of Trust & Thought Leadership

5th June 2024
6PM - 8.30PM

Schneider Electric Auditorium
(Level 1)

Register Now!

AiSP has recently formed our new Special Interest Group (SIG) - CISO SIG. Our Key Focus Areas are:

- Network of Trust to enable more effective and responsive cyber defence of our respective organisations
- Thought leadership and open exchange of ideas to help enhance universal cyber maturity
- Support organization for professional challenges and trials faced by senior cybersecurity leaders
- Socialising because not everything has to be a crisis

Our Vision is to enable CISO's to collaborate, network and exchange thought leadership in the pursuit of a mature cyber defence for their respective organizations and the community at large.

AiSP will be having our next SIG Activity focusing on "What is the definition of a CISO in Singapore" and we would like to invite you to do join us for the meetup.

In the ever-expanding digital landscape, the role of Chief Information Security Officers (CISOs) has become pivotal in safeguarding organizations from cyber threats. As we stand at the intersection of technology and security, it is imperative to focus on nurturing the next generation of CISOs who will shape the future of cybersecurity.

Event Date: 5th June 2024, Wednesday
Event Time: 6.00pm - 8.30pm (Registration Starts at 5.45pm)
Event Venue: Schneider Electric Auditorium (Level 1)

Agenda:

5.45PM – 6PM: Registration
6PM – 6.15PM: Opening and Introduction by CISO SIG Lead, Mr Andre Shori
6.15PM – 7.15PM: Facilitated Discussion by Mr Andre Shori on "What is the definition of a CISO in Singapore?"
7.15PM – 8.30PM: Dinner & Networking

Registration Link: <https://forms.office.com/r/87TgxWu7tr>

The Cybersecurity Awards



The Cybersecurity Awards 2024 nominations HAS BEEN EXTENDED TILL 31 MAY!

Professionals

1. Hall of Fame
2. Leader
3. Professional

Enterprises

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

Students

4. Students

In its seventh year, The Cybersecurity Awards 2024 seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems. The Awards are organised by the Association of Information Security Professionals (AiSP), and supported by Cyber Security Agency of Singapore and the following professional and industry associations that are part of the Singapore Cyber Security Inter Association – Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Chapter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)2 Singapore Chapter, Operational Technology Information Sharing and Analysis Center (OT-ISAC), The Law Society of Singapore, Singapore Computer Society and SGTech.

If you know any individuals and companies who have contributed significantly to the cybersecurity industry, it is time to be recognized now! Nomination forms are attached for the submission according to the categories.



Send in your nominations to thecybersecurityawards@aisp.sg

For any enquiries, please email thecybersecurityawards@aisp.sg

Nomination has been extended till **31 May 2024**. All submissions must reach the secretariat by **31 May 2024**.

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

Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors for The Cybersecurity Awards 2024! Limited sponsorship packages are available.

Corporate Partner Event

Does Your Organization Suffer from an Identity Crisis? On 23 April

On 23 April, in collaboration with our Corporate Partner, BeyondTrust, we have invited Mathew Soon, Kevin Pang and Yum Shoen Yih where they shared on the risks associated with poor identity security disciplines, the techniques that external threat actors and insiders leverage, and the operational best practices that organizations should adopt to protect against identity theft, account compromises, and to develop an effective identity security strategy.



Ladies in Cyber

The 2nd Women in Cyber: Breaking Barriers, Driving Excellence on 25 April 2024

On 25 April, AiSP was at Putrajaya for the 2nd Women in Cyber organised by National Cyber Security Agency (NACSA), Malaysia. Thank you YB Datuk Seri Dr. Noraini binti Ahmad, Deputy Minister of Women, Family, and Community Development for visiting our booth. Thank you Judy Saw, our Ladies in Cyber EXCO Lead for coming down to Putrajaya to share about AiSP LIC Programme with Deputy Minister and hosting her at AiSP booth.



Regionalisation

SEACC Webinar – Cloud Security on 31 July



SEA CC Webinar – Cloud Security



ALVIN YEO
Cloud Specialist, Tenable, APJ



31 JULY 2024
3 – 5 PM SGT



MON GALANG
CyberSecurity Head, GoTyme Bank and
WISAP Technical Committee Expert

ORGANISED BY:



The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2024. The upcoming webinar will be focusing on Cloud Security where speakers will be sharing insights on the best practices for cloud security.

How Tenable Cloud Security Zaps the Risk You Cannot See
Speaker: Alvin Yeo, Cloud Specialist, Tenable, APJ

Cloud infrastructure is an attacker’s playground – you need to reveal the risk you cannot see.

Join Tenable’s Alvin Yeo, Cloud Specialist to hear how CNAPP empowers teams with full asset discovery and risk analysis, runtime threat detection and compliance reporting for multiple clouds.

In this session you will learn how to:

- Automate cloud infrastructure security with identity-driven CNAPP.
- Close cloud security gaps through powerful visualization, prioritization and remediation.
- Reduce your attack surface with least privilege and JIT.

Cloud Security Measures in a Modern Banking Environment

Speaker: Mon Galang, Cyber Security Head, GoTyme Bank and WISAP Technical Committee Expert

In the dynamic landscape of modern banking, robust cloud security measures form the bedrock of trust and integrity. Banks fortify their cloud infrastructure against cyber threats, ensuring the confidentiality and integrity of sensitive financial data. Continuous monitoring and stringent access controls further safeguard against unauthorized access, bolstering customer confidence in the digital banking ecosystem.

Date: 31 July 2024, Wednesday

Time: 3PM – 5PM (SGT)

Venue: Zoom

Registration: https://us06web.zoom.us/webinar/register/2017139507734/WN_coq_DDdfTD-hVwllvS7LcQ

CREST

Latest Exam Updates from CREST

Following the launch of our new syllabuses for our Certified Tester – Infrastructure (CCT INF) and Certified Tester – Application (CCT APP) exams, we wanted to share our next set of exciting updates to these exams.

[CREST Certified Tester - Infrastructure](#)

[CREST Certified Tester - Application](#)

What are the upcoming changes?

The major updates for both the CCT INF and CCT APP exams are detailed on the new web pages for both exams. In addition to the updated syllabuses and content, we have also:

- **Increased the choice of locations:** all elements of the exam are being delivered with our exams delivery partner, Pearson VUE, meaning candidates can take the exams at over 1,100 Pearson VUE centres at locations around the globe, including Singapore and across Southeast Asia

- **Changed the exam components:** the certification has been divided into two parts: a multiple choice and written scenario exam - note the scenario element will no longer be combined with the practical element - and a separate practical exam

[back to top](#)

- **Created great flexibility in the approach:** candidates are now able to pick the order in which they take the components of the exam
- **Ensured the whole exam can be concluded within a day:** candidates can now book to sit both the written and practical elements of the exam on the same day and
- **Changed the use of own machine and tooling:** candidates will in future be able to access tooling within the Pearson VUE exam environment rather than bringing their own laptops, supported by access to the toolset ahead of the exam and the ability to upload materials in advance to assist you when taking the exams.

Information on these latest updates can be found on our dedicated web pages at:

[CREST Certified Tester - Infrastructure](#)

[CREST Certified Tester - Application](#)

Subsequent updates to watch out for

- Updated syllabuses for the Certified Simulated Attack Specialist (CCSAS) and Certified Simulated Attack Manager (CCSAM) exams
- Don't forget to check out our recently relaunched exams in Singapore for [CRTI](#) and [CPSA](#)

Let's stay in contact!

To get the latest CREST communications via email, message marketing@crest-approved.org and ask to 'Subscribe to CREST News'.

You can also see us on social media here: <https://www.linkedin.com/company/crest-approved/> and here: [CREST \(@CRESTadvocate\) / X \(twitter.com\)](#), and on our website www.crest-approved.org.

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
12 May	Cybersecurity Scam Awareness Workshop	Partner
13 -17 May	Hosting of Brunei Cyber Security Association in Singapore	AiSP & Partner
15 May	CyberSec Conference	AiSP
16 May	MTech Security Exchange 2024	Partner
18 May	Cybersecurity Scam Awareness Workshop	Partner
21 May	AiSP x NUS x Sailpoint Event - Sharing at NUS	AiSP & Partner
21 May	School Talk at Serangoon Secondary	AiSP
30 May	AsiatechxSingapore 2024	Partner
31 May	QISP Workshop	AiSP
3-7 Jun	Taiwan Digital Economy - InnoVex 2024	Partner
5 Jun	AiSP CISO SIG Meetup	AiSP
18-19 Jun	ASEAN Bug Bounty	AiSP & Partner
20 Jun	SEA CC Webinar - Web3/Metaverse	AiSP & Partner
25 Jun	CAAP Advisory Clinic	AiSP
28 Jun	Youth Symposium	AiSP
29 Jun	PROTECT 2024 in Phillipines	Partner

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

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

Should Cloud Access be considered as Privileged Access? Thoughts around Cloud Access Management Strategies from CSCIS.



Rajnish Garg, CISSP CSCIS Cloud Security Member

Digital transformation has led to a significant rise in cloud adoption by organisations of all sizes and across all industries. The adoption of cloud computing has enabled businesses to leverage new technologies and platforms, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), to improve their operations, enhance customer experiences, and gain a competitive edge. However, this transformation also introduces new security risks that organisations must address to protect their data and assets.

In this blog post, we will explore one of the security risks that arise from digital transformation and discuss strategies for mitigating these risks.

What's the security risk

Cloud consoles have become an attractive target for cybercriminals due to the single point of access they provide to an organization's cloud infrastructure. Cybercriminals can exploit vulnerabilities in cloud console authentication mechanisms, such as weak passwords or compromised credentials, to gain unauthorised access to the console. Once they have access, they can carry out a range of malicious activities, such as deleting or modifying data, creating new user accounts, or launching new instances.

It's worth noting that rogue employees with access to cloud consoles can also cause significant harm to an organization's security.

In addition to the above threats, session cookie stealing is a type of attack that poses a significant and persistent threat.

How real the risk is?

- According to Sysdig, a significant number of DevOps users (27%) still rely on root user accounts for daily tasks, and a concerning 45% of accounts lack protection through multi-factor authentication.
- Given the potential damage that unauthorised access to cloud environments can cause, Gartner notes that "All IaaS accounts are privileged."
- Furthermore, the problem is compounded by Microsoft's State of Cloud Permissions Risk report, which indicates that identities use only 1% of their granted permissions, with over 50% of these permissions being high-risk and capable of causing catastrophic damage if used improperly.
- Most organisations have Dozens to hundreds of accounts across various cloud platforms such as AWS, Azure, or GCP. Organisations typically grant users access to entire Org or OU, creating a standing access problem. This means that anyone with access to credentials or session cookies can obtain the same level of access at any time, 24x7x365.

What Organizations can do to contain the risk:-

- Consider implementing Multi-Factor Authentication (MFA) for all users, including root users. The selection of a secure MFA method can be discussed in a separate blog post.
- Least privilege approach can be leveraged by reviewing the permissions used by identities in the last 90 days and assigning only necessary permissions to reduce the risk of unauthorised access.
- To improve access management, organisations can consider adopting the following practices:
 - I. Utilize Daily Operation Roles to carry out routine tasks and reduce the need for high privilege access.
 - II. Use Highly Privileged Roles such as AWS Administrator, Azure Global Admin, Azure Subscription Owner, or GCP Project Owner with a proper workflow to ensure controlled access.
 - III. Do not allow Standing Access at all for Production Accounts or Production OU's.
 - IV. Require Proper Workflow Approval with Appropriate Justification for any access to the production environment to ensure security and accountability.

What Technologies organisations can leverage upon?

- **Least Privilege Permissions-** Use Cloud Infrastructure Entitlement Management (CIEM) solutions or Cloud Native tools such as AWS Access Analyzer or GCP IAM Recommender to enforce the principle of least privilege and reduce the risk of over-privileged access.
- **Access Management-** Top Cloud Service Providers offer extensive API-driven approaches to manage access. Use automation tools to create custom workflows

or consider commercial solutions to facilitate efficient and controlled user management to the specific role or permission sets, mitigating the risk of standing access.

Benefits of mitigating such risks:

- Reduction of the blast radius of attacks.
- Progress towards a Zero Trust-based approach to security.

In our upcoming blog series, we will discuss upon the Cloud APIs provided by AWS, Azure and GCP. Stay Tuned.

Article from SVRP 2023 Gold Winner, Muhammad Dinie Bin Baharudin (RP)



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

SVRP has gave me motivation to try out different events and aspects of cybersecurity which is extremely beneficial to me in the long run when I can use all that I had learnt to combine into a final project that I am planning to pioneer in the future.

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

SVRP has made me understand how to give back towards the community that has taught me, which would mean in the future, others will do the same in a continuous loop. The

[back to top](#)

evolution of learning will soon lead to an increase in creativity and innovation as more perspectives and knowledge mix hands into the cybersecurity pool.

What motivates you to be a student volunteer?

I've always felt a sense of joy when another person that I teach understands a certain problem they had faced and then giving their own solution to the project. It makes so that they understand the foundation of how problems are solved and have the flow mindset of how to tackle problems in the future.

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

From continuing other projects that I had created within the last year and expanding to bigger projects with more manpower and creativity.

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

New versions launched!



Stay ahead of the curve with EC-Council certification programs!

The all popular Certified Network Defender (CND), Certified Threat Intelligence Analyst (CTIA) and Certified Hacking Forensic Investigator (CHFI) are now available in the latest versions!

Master advanced network security requirements with CND, excel in predictive threat intelligence CTIA and build ultimate investigative skills with CHFI. With the latest tools and technologies in these programs building job-ready skills, you can set yourself up for success!

Available
as self-paced learning kits,
each
bundle includes EC-Council instructor-led training videos,
e-book,
virtual labs and remote proctored exam voucher.

Special discounts available for AiSP members, please email enquiry@wissen-intl.com for details!

[back to top](#)

Qualified Information Security Professional (QISP®)

QISP Workshop on 31 May



AiSP
Advance Connect Excel

AiSP QISP Workshop





QISP WORKSHOP
ONE-DAY MASTERCLASS FOR
THE QISP® PROGRAMME

Workshop Details

-  **31 May 2024**
Friday
-  **8.30AM - 5PM**
Registration closes at 8.50AM
-  **51 Cuppage Road**
Level 3, Singapore 229469



ORGANISED BY  SUPPORTING AGENCY  TRAINING PARTNER 

REGISTER NOW!

This one-day masterclass is designed to prepare candidates for the Qualified Information Security Professional (QISP®) examination. Participants will gain a comprehensive overview of the key principles across all domains defined in the Information Security Body of Knowledge (IS BOK) 2.0, with a focus on effective exam preparation strategies. The session is ideal for individuals aiming to certify or enhance their expertise in managing cybersecurity threats and incidents.

Objectives:

- Understand the core principles and domains of IS BOK 2.0.
- Identify strategies for effective preparation and success in the QISP® exam.
- Discuss real-world applications of information security management to enhance practical understanding.

Target Audience:

- Information security professionals seeking QISP® certification.

- Individuals with 1-5 years of experience in information security or related formal training.
- Professionals holding or pursuing certification in information security.

Agenda:

8.30AM	Registration and Welcome Coffee
9AM – 10.30AM	Session 1 - Introduction to QISP® and Exam Overview <ul style="list-style-type: none"> • Overview of QISP® certification, its importance, and benefits. • Detailed breakdown of the IS BOK 2.0. • Examination criteria and scoring.
10.30AM – 10.45AM	Morning Break
10.45AM – 12.15PM	Session 2 - Governance, Management, and Business Continuity <ul style="list-style-type: none"> • Key concepts in Governance and Management of information security. • Understanding Physical Security and Business Continuity Planning. • Discussion of past exam questions and successful answering strategies.
12.15PM – 1.15PM	Networking Lunch
1.15PM – 2.45PM	Session 3 - Technical Domains: Architecture, Software, and Cyber Defense <ul style="list-style-type: none"> • Security Architecture and Engineering principles. • Software Security essentials. • Cyber Defense tactics and operations. • Analyzing case studies for a practical understanding.
2.45PM – 3PM	Afternoon Break
3PM – 4.30PM	Session 4 - Operation, Infrastructure Security, and Examination Preparation <ul style="list-style-type: none"> • Key issues in Operation and Infrastructure Security. • Final tips and strategies for preparing for the exam. • Practice test and review of answers.
4.30PM – 5PM	Q&A and Closing Remarks <ul style="list-style-type: none"> • Open floor for participant questions. • Summary of key takeaways. • Strategies for continued learning and preparation up to the exam date.

* Materials for trainees, printed and pdf slides, printed and pdf case studies, printed and pdf Cert of Participation. 2 Coffee breaks with snacks + Bento Lunch (all halal) will be provided.

Date: 31 May 2024, Friday

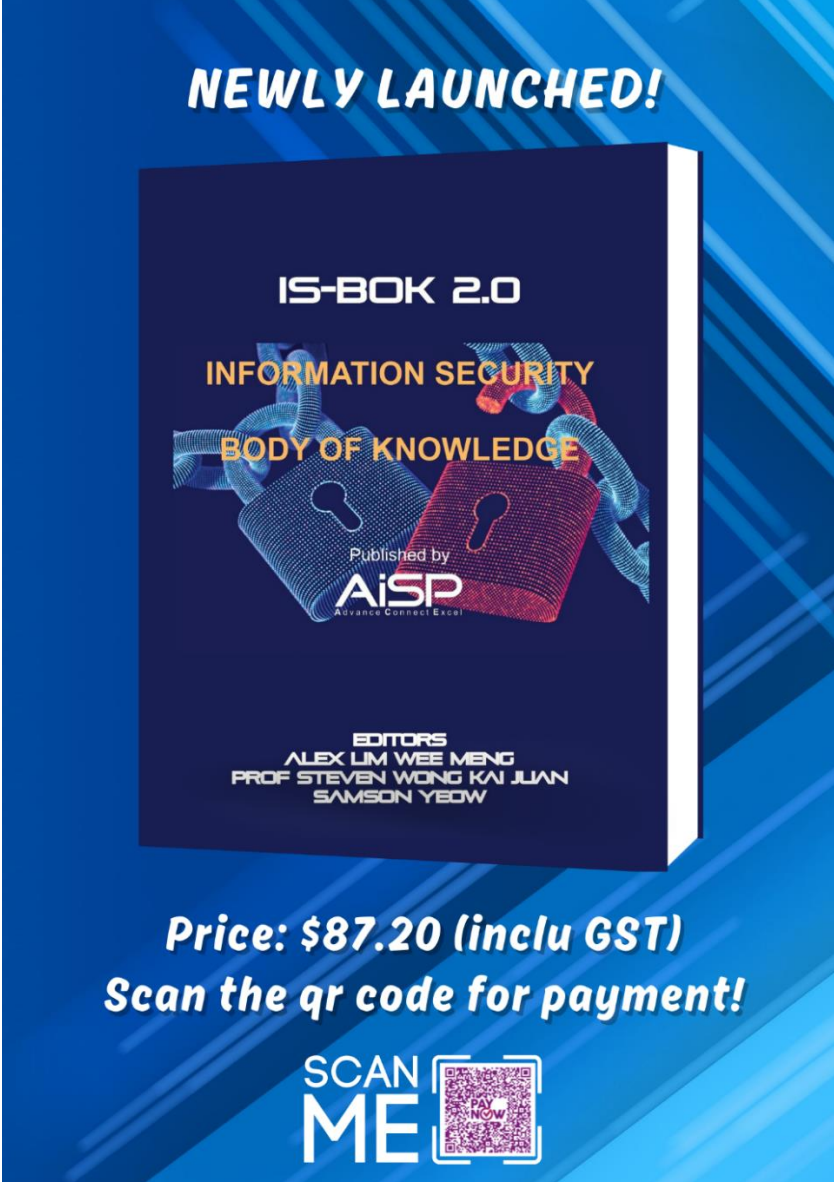
Time: 8.30AM – 5PM (Registration closes at 8.50AM)

Venue: Venue: 51 Cuppage Road, Level 3 Singapore 229469

Registration: <https://forms.office.com/r/x5WcjdDPJ>

Body of Knowledge Book

Get our newly launched Information Security Body of Knowledge (BOK) Physical Book at **\$87.20 (inclusive of GST)**.



NEWLY LAUNCHED!


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 YEOH

Price: \$87.20 (inclu GST)
Scan the qr code for payment!

SCAN ME 

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. **Limited stocks available.**

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

Online Course launched on 1 March 2024!



QISP Exam Preparatory E-Learning Course

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

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

Grab the exclusive launch offer at SGD 499 nett!

Special price of SGD 429 nett for AiSP members!

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

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

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

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

MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

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

Complimentary Affiliate Membership for NTUC Members

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 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

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!

NTUC Social Membership



WORK, LIVE, PLAY
LIKE NEVER BEFORE
WITH THE NTUC-U ASSOCIATE
MEMBERSHIP COLLABORATION!

READY TO ADD SPARK TO YOUR MEMBERS' LIVES AND LIVELIHOODS?
The NTUC-U Associate Membership Collaboration is an exclusive add-on membership for professional associations in the U Associate network. It will give your members access to exciting career, lifestyle and leisure benefits!

What are the benefits for your association?

- ▶ Additional privileges for your association members.
- ▶ Opportunities to engage your members at NTUC Club venues or participate in interest-based activities.
- ▶ Leverage U Associate's resources to reach out to a database of close to **300,000** professionals.

What are the benefits for your members?

- ▶ Career advancement and professional development through U PME Centre's suite of career advisory services.
- ▶ Enhanced lifestyle through interest-based leisure activities.
- ▶ Savings on lifestyle products and services through the Link Rewards Programme.

Some benefits include

Benefits and privileges from RX Community

Member Programme

<https://www.readyforexperience.sg/>

Please fill in the form below and make payment if you would like to sign up for the membership.

<https://forms.office.com/r/qtjMCK376N>

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



bugcrowd



CLIXER



CYBERSAFE
YOUR SECURITY, OUR PRIORITY



DEAC



ENSIGN
INFOSECURITY



FORTINET®



Grab





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



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



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.