NEWSLETTER

January 2021

Association of
Information Security Professionals

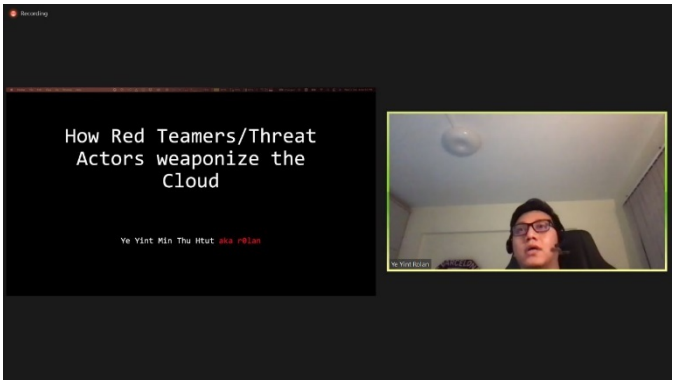
NEWS & UPDATES

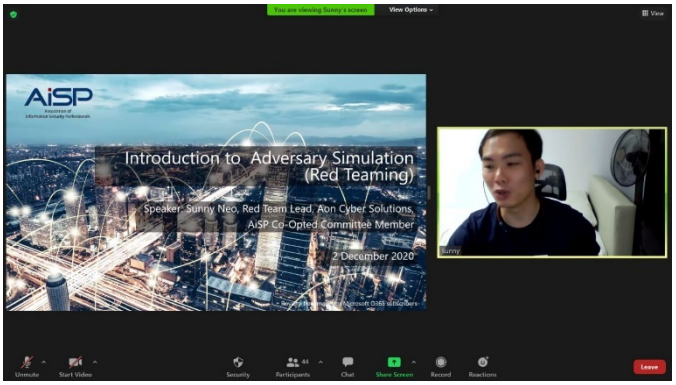
In line with Government's directives on COVID-19 pandemic and AiSP's business continuity plan, AiSP Secretariat has commenced partial telecommuting during Phase 3. Please **email us** or **WhatsApp** to our office number (+65 6247 9552), for assistance before you drop by our office.

Do check out our **community calendar of events** or follow us on social media for events and updates!

Knowledge Series Events

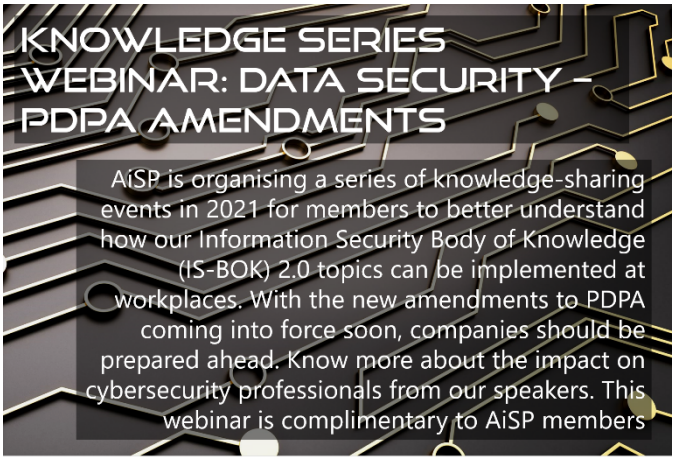
Red Teaming Webinar, 2 Dec 2020





We had our last knowledge series webinar of the year, **Red Teaming**, with insights from our speakers, **Sunny Neo** and Ye Yint Min Htut (Rolan). Our Assistant Secretary **Cecil Su** closed our very first webinar session on this topic and we look forward to kick-off the new webinars series in 2021!

Our upcoming webinar **Data Security: PDPA Amendments**, on 21 Jan 2021 focuses on how our members should be prepared ahead once the Personal Data Protection (Amendment) Bill comes into force in 2021.



Please register for our **21 Jan 2021 event**
(3 PM – 5 PM) today, registration closes by Sun 17 Jan 2021.

This is an initiative by AiSP's **Data and Privacy Special Interest Group**.

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 in 2021.

About our Knowledge Series

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its **Information Security Body of Knowledge 2.0** topics. Our scheduled topics for webinars in 2021 are as follows (*may be subjected to changes*),

1. Cyber Threat Intelligence (CTI), Feb
2. Governance and Management, 17 Mar
3. Cloud Security SIG, 30 Mar 2021 (hybrid*)
4. Software Security, 14 Apr
5. Physical Security, Business Continuity and Audit, 12 May
6. Security Architecture and Engineering, 16 Jun
7. Data and Privacy SIG, 29 Jun (hybrid*)
8. Operation and Infrastructure Security, 14 Jul
9. OT/IOT – IoT Security, 18 Aug
10. Cyber Defence – Ethnical Hacking, 15 Sep
11. CTI SIG, 29 Sep (physical event* with recording)
12. Security Operations – Incident Response Management, 13 Oct
13. Emerging Trends - Blockchain, 10 Nov
14. Emerging Trends – AI for Cyber Security, 8 Dec
15. IoT SIG, 22 Dec (physical event* with recording)

**Subjected to Singapore Government's directives for physical events during COVID-19 pandemic.*

Please let us know if your organisation is keen to be our sponsoring speakers in 2021!

AiSP members who registered for the event, can playback the recorded event via their member profile in Glue Up. If you did not sign up for the event, please email event@aisp.sg for assistance. Please refer to our scheduled 2021 webinars in our **event calendar**.

CyberFest™ 2021

CyberFest® is a community-led initiative that would take place from 22 to 26 Feb 2021 in Singapore. With the Phase 3 announcements, we would include some virtual events during **CyberFest®** to cater to local and overseas participants.

One of our flagship events **The Cybersecurity Awards 2020** ceremony, is scheduled on Friday 26 Feb 2021. As a hybrid event, it will be held at Marina Bay Sands, Singapore and certain segments would be broadcasted "live" to cater to a wider audience.

The Cybersecurity Awards

THE CYBERSECURITY Awards 2020

The Cybersecurity Awards (TCA) 2020 seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems. In view of

COVID-19 pandemic and well-being of our guests at the award ceremony, AiSP has moved the physical event to **26 Feb 2021**.

We have received new enquires from Singapore and overseas for award nomination, after the 2020 call for nomination was closed on 30 Sep 2020. For our nominees to have more time to prepare their submission, we are pleased to commence **TCA 2022** marketing and the nomination period is tentatively planned for Jun 2021 to Jun 2022.

The Cybersecurity Awards has three (3) award categories: Professionals, Enterprises and Students -a total of eight (8) awards:

Professionals
1. Hall of Fame
2. Leader
3. Professional

Enterprises
4. MNC (Vendor)
5. MNC (End User)
6. SME (Vendor)
7. SME (End User)

Students
8. Students

The winners will be announced at The Cybersecurity Awards ceremony
Please email us (thecybersecurityawards@aisp.sg) if your organisation would like to be our Platinum, Gold and Silver sponsors!

TCA2020 Sponsors

BeyondTrust

CISCO

CyberProof
A UST Global Company

DBS

ENSIGN INFOSECURITY | CONQUER THE UNKNOWN

PCS SECURITY

RSA

THALES

TREND MICRO

ST Engineering

Singtel

wizlynx group
Your Cyber Security partner worldwide

Workforce Singapore

Student Volunteer Recognition Programme (SVRP)

The SVRP working committee has interviewed our potential Gold Awardees and has confirmed our list of Gold, Silver and Bronze Award recipients. We want to congratulate all students for their contributions and dedication during the challenging 2020 year. Against all odds, each nominee contributed an average of 99.9 hours.

Over **9,792** hours were contributed from 1 Sep 2019 to 31 Aug 2020, where

- 1,250 hours were for Leadership pillar,
- 4,411 hours were for Skills pillar
- 4,176 hours were for Event pillar

Our **SVRP 2021 nomination form** is available now for IHL students to apply! To encourage more students to volunteer, secondary school and pre-university students are welcome to participate! Please refer to **SVRP framework** and **SVRP 2021 nomination form for secondary school and pre-university students**!

We are having a student volunteer drive from now till Dec 2021 for those are interested to volunteer but not sure where to start. Please **click here** to apply today!

Under AiSP's **Academic Partnership Programme (APP)**, the IHLs would include AiSP Student Chapter in their respective institutes. Please refer to our **Student Chapters** for the list of current committee members and we look forward to expand the list in 2021!

Ladies in Cybersecurity Charter

Under our **Ladies in Cybersecurity Charter**, AiSP's volunteer team of female cybersecurity professionals have been mentors to female students through our Ladies in Cyber Mentorship Programme. We welcome female volunteers and students to join our programme as **mentors** and **mentees** (please refer to the online forms).

AiSP hopes to work closer with our industry partners to attract more female cyber professionals in Singapore. Please **contact us** if your organisation would like to take this conversation further.

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:

- Cloud Security
- Cyber Threat Intelligence
- Data and Privacy
- IoT

Please contact us if you are keen to be part of our SIGs as we are actively recruiting members for 2021!

For AiSP Members only

As we are always looking for new ways to engage our members, AiSP has categorised the various ways for **member-only access** as part of our digital engagement during COVID-19 pandemic,

1. Members-only access for **webinar playback**
2. **LinkedIn closed group**
3. Participate in **member-only events** and closed-door dialogues by invitation
4. **Volunteer** in our initiatives and interest groups, as part of career and personal development

If you have missed our virtual events, some of them are made available for members' access via Glue Up platform. Please email (event@aisp.sg) if you need any assistance.

We wish to remind our members to renew their 2021 membership before Chinese New Year!

Call for Volunteers

As AiSP focuses in raising the professional standing of information security personnel and professions in Singapore since 2008, we have been running various initiatives to address diverse needs and developments. Please **email us** for more details!

PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®) Course

QISP® is designed for entry to mid-level Information Security Professionals, and any IT Professionals who are keen to develop their knowledge in this field. It will be enhanced to complement AiSP's Information Security Body of Knowledge (IS-BOK) 2.0. Our online examination via Pearson VUE platform would be deployed worldwide in Q1 2021.

Please **contact AiSP** if you are keen to leverage the enhanced QISP® for your learning and

development needs, or you would like to develop courseware based on AiSP's IS-BOK 2.0 overseas.

BOK 2.0 Knowledge Series

As information security developments are accelerating during COVID-19 pandemic and the trend is expected to be the same for 2021, we have covered the application and implementation of our BOK 2.0 topics at workplaces in our past webinars. This series is useful for working professionals who are preparing for our **QISP®** examination so that their knowledge remains current.

CREST SINGAPORE CHAPTER

The CREST Singapore Chapter was formed by CREST International in partnership with CSA and AiSP to introduce CREST penetration testing certifications and accreditations to Singapore in 2016.

Temporary suspension of CCT Info and CCT App exams till early 2021

As of 3 Sep 2020: CREST is investigating the deposit of confidential exam material into the public domain.

CRESTCon Singapore 2020/2021

The CREST Singapore Chapter is organising the **first CRESTCon Singapore 2020/2021** in Q1 2021 and the Organising Committee is reviewing the papers submitted. Please **email secretariat** if your organisation is keen to sponsor the event!

UPCOMING ACTIVITIES/ EVENTS

Ongoing Activities

Date	Event	By
Jan-Dec'21	Call for Female Mentors (Ladies in Cyber)	**AiSP**
Jan-Dec'21	Call for Volunteers (AiSP Members, Student Volunteers)	**AiSP**
Jun'21-Jun'22	Call for Nomination for The Cybersecurity Awards 2022	**AiSP**

Upcoming Events

Date	Event	By
2 Jan	SINCON 2020 Conference	Partner
13 Jan	[CPP] PDPA 2.0 Manage. Respond. Report.	Partner
14 Jan	[SVRP] Holy Innocents' High School Career Talk	Partner
21 Jan	[BOK] Knowledge Series Webinar: Data Security — PDPA Amendments	**AiSP**
27-28 Jan	Cyber Security For Critical Assets	Partner
1 Feb	[CAAP] AiSP x NTUC Career Talk for PMETs	**AiSP & Partner**
4 Feb	[SVRP] ITE West Industry Sharing	Partner

Date	Event	By
23 Feb	[SVRP] Bukit Panjang Government High School Career Talk	Partner
22 Feb	Ladies in Cyber networking seminar	**AiSP**
24 Feb	SVRP Award 2020 ceremony	**AiSP**
25 Feb	CRESTCon Singapore 2020/2021	**AiSP & CREST SG Chapter**
26 Feb	The Cybersecurity Awards 2020 ceremony	**AiSP**
Feb	[BOK] Knowledge Series Webinar: Cyber Threat Intelligence	**AiSP**

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

Contributed Contents

Insights from our event sponsor RSA

21 Predictions for 2021
Cybersecurity for a Changed and Changing World

This time, the future unfolds in the shadow of the past.

2020 may be over, but organisations will continue to feel its impact in 2021, when plans and decisions will be profoundly influenced by the challenging events of the past year.

Unprecedented changes in how we work, play and connect are not going away anytime soon. We will continue to work from home, do more shopping online and stream much of our entertainment, to varying degrees. These shifts will continue to affect how organisations handle identity and access management, threat detection and response, fraud prevention, and risk management in 2021 and beyond.

What can you expect in 2021?

Inundated with new cybersecurity threats in an expanded attack environment, organisations will take a serious look at taking action to adopt zero trust, consolidate cybersecurity operations, deploy new fraud prevention technologies, and rethink their approach to risk and regulation.

We share 21 predictions for 2021 that illustrate the many ways in which 2020 is changing the shape of cybersecurity, and the challenges and opportunities that will redefine security and risk in the year to come.

#1 Doubling down on digital transformation

The unprecedented events of 2020 did not slow digital transformation—they accelerated it. From securing the remote workforce to extending cybersecurity to the cloud, this acceleration will continue. Building on the insights and experiences of 2020, organisations will embrace transformation with

even greater urgency to regain competitive advantage.

Identity and Access Management
Organisations will continue to find it challenging to ensure that people are who they claim to be when they seek access to work apps and data, personal financial accounts and other resources online.

#2 A more critical role for identity governance

As the workforce continues to evolve in light of some people returning to the office and others continuing to work remotely, organisations will benefit from a focus on ensuring that they can easily manage changing user rights and access privileges.

#3 Cybercriminals exploiting access changes

Organisations should anticipate ongoing attempts to steal credentials when many in the workforce are continuing to access resources from home. It will be critical to work to limit the negative impact by addressing issues such as use of unhardened devices, cloud application access outside the VPN and sharing of work devices with family members.

#4 The shift to zero trust

Cybersecurity will pivot to embrace zero trust, as security teams rethink their defense postures to adapt to an expanding attack surface and a growing reliance on third parties. Zero trust defence postures will combine a range of governance processes, multi-factor authentication methods and other measures to manage emerging identity-based threats.

#5 Stepped-up DDoS attacks

Distributed denial-of-service (DDoS) attacks will rise as the attack surface expands and dependence on the internet grows, building on a threefold increase in DDoS attacks in 2020. The shift to zero trust (#4) will help combat DDoS attacks by rejecting the concept of trusted systems—a concept that is vital to successful DDoS attacks.

#6 Youthful vulnerability and synthetic identity

Synthetic identity theft, in which pieces of legitimate user information are combined with fictitious information to create a fake identity, will increase as fraudsters specifically target younger users who may not monitor their identities closely. This will ultimately lead to a massive surge in new account fraud.

Threat Detection and Response
More kinds of threats and threat actors will target more organisations across a vastly expanded attack surface, prompting the adoption of new strategies, tactics and technologies for defending against threats.

#7 The remote workforce is here to stay—and so is the risk that comes with it

While many workers will return to the workplace, some degree of remote work will remain a permanent feature of many employees' workdays. The expanded attack surface associated with remote work will still create cause for concern as the workforce continues relying on a combination of personal networks, third-party resources and new resources.

#8 Dangerous times for healthcare

Healthcare organisations, already targeted for cyber-attacks throughout the pandemic, will continue to face ransomware demands that threaten to expose sensitive data, as well as dangerous spear-phishing attacks aimed at stealing IP. Vaccine companies in particular will increasingly be the focus of attacks as they race to get vaccines into widespread distribution.

#9 The rise of XDR

Organisations will increasingly extend detection and response from the user, through the network and into the cloud, to provide visibility anywhere and everywhere data and applications live.

Extended detection and response—XDR—will be critical for security teams to stay ahead of sophisticated and aggressive threats.

#10 Cybersecurity consolidation: out of many, one

Forced by the expanded attack surface to fundamentally rethink defence postures and plan for increased risk, organisations will continue to move toward a cybersecurity strategy built on a single, cohesive operation. This is in contrast to the multiple point solutions they relied on previously to meet specific needs.

#11 Automation and AI in the SOC

Security teams will focus on how to approach threat detection and response in an expanded threat environment where there may be much less control. One response will be to add automation security and artificial intelligence (AI) to help identify new threats and prioritise responses in the security operations centre (SOC).

Fraud Prevention
Fraudsters who hit the jackpot in 2020 by taking advantage of surging online activity will be looking for ways to continue their success into the next year—and retailers and consumers will need to be ready to fight back.

#12 Victimising the vulnerable

Until a robust economic recovery is underway, fraudsters will continue to find ways to profit by exploiting people in desperate financial straits. Using phishing, rogue mobile apps and other types of fraud attacks to offer easy money, they will trick recipients into sharing bank account numbers or other sensitive information.

#13 A bigger role for AI/ML in fraud prevention

As merchants work to balance fraud prevention and regulatory compliance with frictionless customer experiences, we will see AI/machine learning (ML) advance to the point where merchants can more easily assess transaction risk and comply with SCA and other regulatory requirements.

#14 3-D Secure 2.x: Take that, CNP fraud

The surge in e-commerce that the pandemic brought in 2020 came at a price: a corresponding rise in targeted card-not-present (CNP) fraud. The urgent need to recognise and reduce transaction risk, while also reducing customer friction, will lead more U.S. merchants and card-issuing banks to adopt the 3-D Secure 2.x authentication protocol.

#15 Surges in QR code and BOPIS fraud

Cybercriminals will exploit consumer demand for contactless transactions, driving surges in buy-online-pickup-in-store (BOPIS) fraud, where fraudsters use stolen cards to buy online and send mules to retrieve purchases at curbside, and quick response (QR) code fraud, including QRs that request payment or personal information or that trick users into downloading malicious programmes.

#16 Loyalty points looted when no one's looking

Travelers who are not traveling as much anymore are also likely not checking their airline and hotel loyalty points and account balances as much either.

That is not lost on cybercriminals, who will quietly use credential-testing and account takeover to harvest points when they know few people are paying attention.

Integrated Risk Management
More and changing regulation in response to a changing world will expose organisations to more regulatory risk, forcing them to re-examine how they manage that risk.

#17 Consolidated, proactive risk management

For many organisations, enabling the remote workforce revealed outdated, fragmented risk management processes. These will give way to systems and structures designed to help proactively manage risk, as organisations consolidate risk management, compliance and governance into a total managed view, and prioritise having risk data that is as close to real-time as possible.

#18 Regulatory landscape complexity, continued

The recent rise in regulatory compliance regimes around security and privacy, and the ongoing emergence of new regulations, will continue to create complexity. These challenges will force organisations to grapple with simplifying their internal data architectures to achieve a better understanding of their own compliance posture.

#19 More data regulation—and tougher penalties

The value of data will continue to increase, leading to more data privacy and security regulations being developed, debated and enacted, particularly when it comes to critical infrastructure. There will also be harsher penalties for failing to protect data, not disclosing attacks or otherwise being out of compliance with applicable laws.

#20 Assigning accountability in a breach

The issue of regulatory accountability in a growing third-party ecosystem will come to a head, likely because of a high-profile General Data Protection Regulation (GDPR) case in which an organisation suffers a data breach due to an application programming interface (API) integration—and the courts end up having to determine who is responsible for paying the fine.

#21 AI regulation: all eyes on the EU

The speed with which EU organisations have been adopting AI will put increasing pressure on European regulators to prioritize it over other areas for regulatory initiatives. Indeed, 2021 could bring the first draft of formal AI regulations in the EU, along with guidance on how to adopt AI ethically.

Note: AiSP's house style is UK English while RSA's article was first published in UK English.

This knowledge-sharing article was by RSA, please click **here** to watch their presentation at our SME Cybersecurity 2020 Conference.

Keen to share your organisation's initiatives, updates and insights to the cybersecurity community? Please email to **secretariat@aisp.sg** if you would like to be our event sponsors or corporate partners!

MEMBERSHIP

AiSP membership cycle starts on 1 Jan, this means all members on annual fee should pay 2021 membership before 2020 ends. This is to ensure there is no disruption to your membership and benefits.

We encourage Ordinary and Associate Members to pay for 3-year membership for the convenience and there is saving as compared to making annual fee payment regularly.

Under **AiSP's Constitution**, annual subscriptions are payable in advance within the first month of the calendar year. Secretariat has reached out to members for their annual membership renewal every fourth quarter (Q4) of each preceding year.

Members who are no longer active and did not respond to our membership renewal emails and edms, must re-apply for membership admission if they wish to re-join AiSP.

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: 2020 to 2021) from 1 Jul 2020 to 30 Jun 2021. 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 **WhatsApp** (+65 6247 9552).

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

Your AiSP Membership Account on Glue Up

AiSP has moved its digital membership to EventBank, now known as Glue Up, an all-in-one cloud platform for event and membership management. You can access the web portal or the mobile application (App Store, Google Play), **using the email address you have registered your AiSP membership for**.

There is no need to create another profile if you are using a different email address; you can just update your alternative email address in your membership profile. The platform allows our members to sign up for events and voluntary activities, and check membership validity.

Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!

Type	Benefits
Individual Membership	▪ Recognition as a Trusted Infocomm Security Professional. You can use the designation of AVIP (AiSP Validated Information Security Professionals) or MAISP (Ordinary Member) as your credentials. ▪ Regular updates on membership activities. ▪ Free and discounted rates for events organised by AiSP and partners. ▪ One-time discount for QISP® examination fee for Affiliate members who are working professionals. ▪ Priority for activities, talks and networking events. ▪ AVIP members enjoy Professional Indemnity coverage in Singapore and overseas.

Type	Benefits
Corporate Partner Programme (CPP)	▪ Listing on AiSP website as a Corporate Partner ▪ Free and discounted rates for events organised by AiSP and partners. ▪ Complimentary AiSP Affiliate membership for organisation's personnel. ▪ Special invite as speakers for AiSP events. ▪ One complimentary job advertisement or knowledge-sharing article on AiSP platform per month (i.e. a total of 12 ads or articles in a year).

Type	Benefits
Academic Partnership Programme (APP)	▪ Inclusion of an AiSP Student Chapter for the Institute. ▪ Ten (10) complimentary AiSP Affiliate membership

Type	Benefits
	for personnel from the Institute. ▪ Complimentary AiSP Affiliate membership for all existing full-time students in the Institute, not limiting to cyber/infosec domains. ▪ Listing on AiSP website as an Academic Partner. ▪ One annual review of Institute's cybersecurity course curriculum. ▪ AiSP speakers to speak at Student Chapter events, including briefings and career talks. ▪ Free and discounted rates for events organised by AiSP and partners. ▪ One complimentary info/cybersecurity or internship post in AiSP website per month.

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.

AVIP Membership

AiSP Validated Information Security Professionals (**AVIP**), the membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development and career progression for our professionals. Interested applicants should be qualified AiSP Ordinary Members (Path 1) to apply for AVIP.

CONTACT US

Please contact **secretariat@aisp.sg** on membership, sponsorship, volunteerism or collaboration.

AiSP outreach and programmes are made possible by our Partners.

Corporate Partners

Academic Partners

Association of Information Security Professionals

+65 6247 9552 (**WhatsApp**)

secretariat@aisp.sg

www.aisp.sg

116 Changi Road
#04-03 WIS@Changi
Singapore 419718

The Association of Information Security Professionals (AiSP), formed in 2008, is an independent cybersecurity association that believes in developing, supporting and enhancing industry technical competence and management expertise to promote the integrity, status and interests of Information Security professionals in Singapore.

We believe that in promoting the development of cybersecurity and increasing and spreading of cybersecurity knowledge can shape more resilient economies.

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

- promoting the integrity, recognition 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.