

News & Update

- Knowledge Series
- CAAP
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Special Interest Groups
- The Cybersecurity Awards
- Regionalisation
- CREST
- Upcoming Events

Contributed Contents

- Cloud Security SIG: How HUAWEI CLOUD Harness On Cloud Security
- CTI SIG: Rantings of a Cyber Security Analyst
- Digital Value Chain Attacks on a Rapid Rise with Ransomware Victims Nearly Doubled Year over Year
- Singapore Launches OT Train-The-Trainer Programme
- Workflow automation through GlobalSign's GMO Sign
- The Cybersecurity Awards 2021 Winner – Huang Shao Fei

Professional Development

Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome Nozomi Network, Onesecure, and Vectra as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.



Continued Collaboration

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

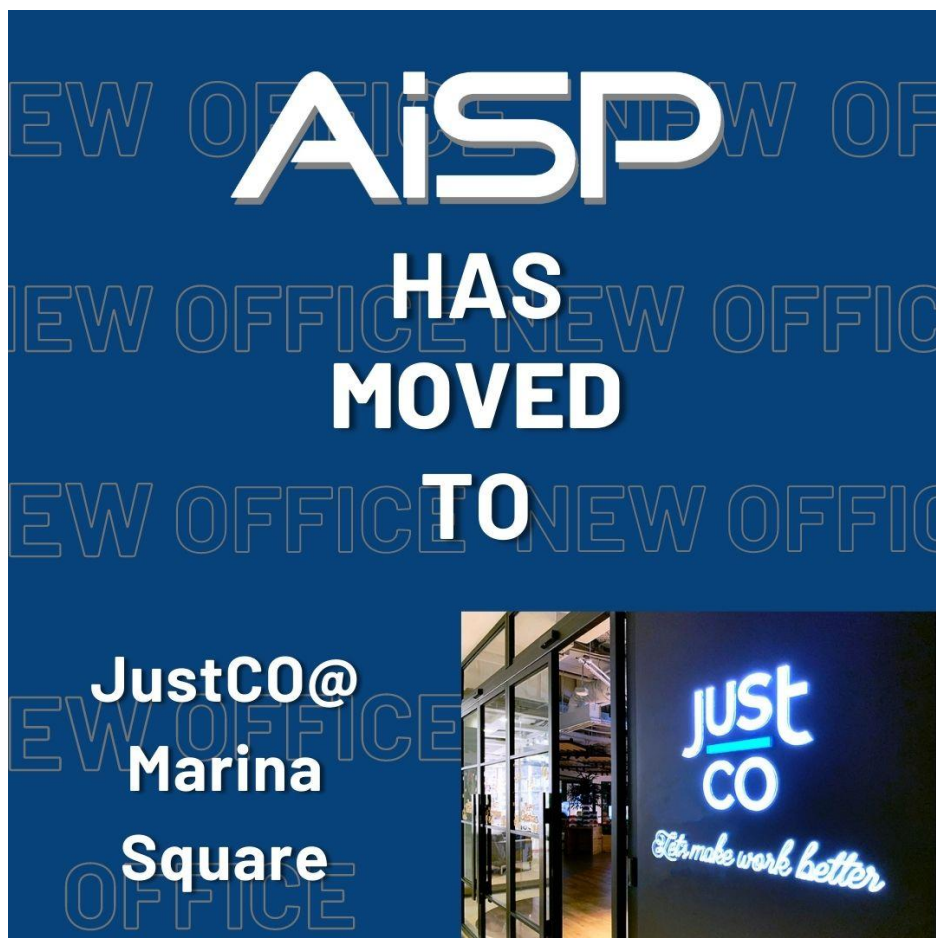


News and Updates

New office at Justco Marina Square

AiSP has shifted its office from 116 Changi Road to JustCo @ Marina Square. For visitors, please take note of our new address

6 Raffles Blvd
#03-308 Marina Square
Singapore 039594



Knowledge Series Events

Incident Response Management on 6 July

AiSP
Advance Connect Excel

AiSP Knowledge Series – Incident Response Management

AiSP Knowledge Series - Incident Response Management
6 JUL 2022 | 3PM - 5PM | ZOOM

Kevin Pang
Solutions Engineer
BeyondTrust

Victor Tan
Business Development Manager
Blackpanda

Organised by
AiSP
Advance Connect Excel

Supported by
BeyondTrust
BLACKPANDA
INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of
DIGITAL FOR LIFE

In this Knowledge Series, we are excited to have BeyondTrust and Blackpanda to share with us insights on incident response management. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

The Path to Zero Trust: From Ambition to Reality

Speaker: Kevin Pang, Solutions Engineer, BeyondTrust

Remote working is now commonplace, while hybrid and multicloud footprints continue to rapidly expand. In this increasingly perimeterless world, organizations must embrace zero trust security principles, such as least privilege, continuous authentication and monitoring, segmentation, and microsegmentation to stay secure, while moving digital transformation forward.

Join BeyondTrust to understand:

- What Is Zero Trust?
- Zero Trust vs. Zero Trust Architecture – Are They Different?
- The Path to Zero Trust
- How Privileged Access Management (PAM) Enables Zero Trust

Beyond Incident Response - The Rise of Ransomware

Speaker: Victor Tan, Business Development Manager, Blackpanda

Cyber breaches happen quick and can cause serious damage. Being prepared in the event of a cyber breach allows organizations to successfully manage its impacts and reduce operational, financial and reputational damages by activating an efficient incident response plan, helping your business through a cyber catastrophe. In this webinar, Victor delves deep into the impacts of the various types of cyber incidents due to system vulnerabilities and human errors. Join us to learn more about the correct approach to managing a ransomware based on past cases Blackpanda has successfully handled.

Date: 6th July 2022, Wed

Time: 3PM – 4.30PM

Venue: Zoom

Registration:

https://us06web.zoom.us/webinar/register/8816536323919/WN_MShJhWjQQ4u0Gg8SxqDR6A

Cyber Threat Intelligence on 20 July



AiSP Knowledge Series – Cyber Threat Intelligence

AiSP Knowledge Series – Cyber Threat Intelligence

20 Jul 2022 | 3PM - 5PM | Zoom



Fabian Toh
Cyber Security Sales
Engineer
IronNet Cybersecurity



Niel Pandya
Cybersecurity Lead, APJ
Micro Focus



Organised by



Supported by



In support of



In this Knowledge Series, we are excited to have IronNet Cybersecurity and Micro Focus to share with us insights on Cyber Threat Intelligence. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

Leveraging cyber threat intelligence to benefit security posture

Speaker: Fabian Toh, Cyber Security Sales Engineer at IronNet Cybersecurity

Organisations are increasingly developing intelligence requirements, producing, consuming and sharing intelligence. Moving forward as a community, information sharing is the key to benefit organisations' security posture. Join us to hear how organisations can build actual attack intelligence and then work collectively as a community to operationalise it effectively.

Securing your Digital Value Chain with Board level, Actionable Threat Intelligence

Speaker: Niel Pandya, Cybersecurity Lead, APJ, Micro Focus

Most of today's threat intelligence is highly technical, aimed at a technical audience and sometimes lacks actionable results prioritized by impact on business. In this session we will share on how Micro Focus is developing an approach for interpreting modern day cyber threats that can be actionable from top down based on securing the value chain. We will discuss, how threats are discovered and prioritized based on location and industry and how we reduce noise to ensure our efforts are focused on the digital value chain.

Date: 20 July 2022, Wed

Time: 3PM – 4.30PM

Venue: Zoom

Registration:

https://us06web.zoom.us/webinar/register/8316553557570/WN_rIVJEDXIRVmnenlgQtgYbw

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 2022 are as follows (*may be subjected to changes*),

1. Incident Response Management, 6 July 22
2. Cyber Threat Intelligence, 20 July 22
3. Security Operation BOK Series, 24 Aug 22
4. Internet of Things BOK Series, 19 Oct 22
5. DevSecOps BOK Series, 16 Nov 22

Please let us know if your organisation is keen to be our sponsoring speakers in 2022!

Please refer to our scheduled 2022 webinars in our [event calendar](#).

Cybersecurity Awareness & Advisory Programme (CAAP)

Staying Cyber Safe with Cyber Trust & Cyber Essentials



In an increasingly digitalised environment, businesses are correspondingly more exposed to digital risks that could cause disruption to their business. Besides incurring hefty costs to recover from security breaches and restore data and systems, businesses would suffer from reputational damage and loss of business as well. CSA has recently developed a cybersecurity certification scheme comprising two certification products – the Cyber Trust and Cyber Essentials marks – to help enterprises demonstrate their level of cybersecurity.

Find out how the certification helps enterprises to determine the level of cybersecurity to put in place.

Agenda

1. Learn more about the actual Cyber Essentials/Trust Certification Process
2. Guided walk through of the Cyber Essentials Self-Assessment questionnaire
3. SME Sharing of its own certification journey
4. Available training to better prepare your company for the rigours of the certification

SPEAKERS' PROFILE



Mr Tony Low, Vice-President & CAAP Lead, AISP

Tony is currently part of the Value Advisory practice for the Google Cloud JAPAC region, focus on understanding client strategy and aligning cloud platform capabilities to drive tangible benefits. He also worked for leading multinational companies such as Citibank, Barclays, IBM and CA in various job roles such as Product Manager, Delivery Manager and Technical Sales Advisory.



Ms Veronica Tan, Director, Safer Cyberspace Division, CSA

Veronica is driving the Safer Cyberspace portfolio in the Cyber Security Agency of Singapore (CSA). Her areas of focus include leveraging national-level infrastructure for the delivery of baseline security controls, as well as developing broad-based and targeted programmes to raise awareness and adoption of good cybersecurity in enterprises.



Mr Baljit Singh, Business Solutions & Operations Manager, GIC Pte Ltd

Baljit has 6 years of experience in TIC industry in roles involving business development, key account management, 2nd party/3rd party auditing. He is also a Certified Scrum Master, ISO 27001 (Information Security) & ISO 23301 (Business Continuity) Internal Auditor, ISO 9001 (Quality) Lead Auditor & ISO 37001 (Anti Bribery) Lead Auditor.



Mr Dave Gurbani, CEO, CyberSafe Pte Ltd

Dave Gurbani is the Founder and CEO of CyberSafe Pte Ltd – a local firm whose primary focus is to provide Affordable, Accessible and Understandable Cybersecurity to SMEs and At-Risks groups in Singapore. His core specializations are in Blue Team Operations, Cyber & Privacy Compliance, Threat Intelligence and Open-Source Intelligence Gathering (OSINT).



Mr Nur Kamal Bin Kamari, Lead Auditor, TÜV SÜD PSB Pte Ltd

Kamal is a cybersecurity lead auditor at TÜV SÜD, with over 26 years of experience in the IT industry. He supports organisations across various industries to mitigate cyber risks and help achieve their cybersecurity goals. Kamal has taken on numerous roles including IT Security Analyst, IT Security Consultant, Trainer and Lead Auditor at various organisations.





Mr Loa Howe Yong, Training Business Manager, BSI Group Singapore Pte Ltd

As a Training Business Manager, Howe Yong leads BSI SG's commercial training business team in supporting client's organisation resilience through competency development and capacity building, with an increased focus on Digital Trust and Sustainability.

Click [here](#) to register

AiSP Cybersecurity Awareness E-Learning

	
<h3>AiSP Cybersecurity Awareness E-Learning</h3>	
<p>On 7 January 2022, the Association of Information Security Professionals (AiSP) launched the Cybersecurity Awareness E-Learning. It was launched by Ms Gwenda Fong, Assistant Chief Executive (Policy & Corporate Development) of Cyber Security Agency of Singapore.</p> <p>In this E-Learning, we will bring you through a set of materials that will prepare your Business and your employees to embark on an exciting journey in digital transformation and start your Business to be more secure.</p> <p>We will be covering:</p> <ol style="list-style-type: none"> 1. Providing businesses with an understanding of the current digital business landscape 2. Deep dive into understanding the Digital better Transformation Journey 3. Risk and threats for the Business to understand some of the most crucial aspects and assessments. 4. How you can start to explore and secure your Business by handling data securely and setting up your initial cybersecurity framework 5. Providing an understanding of your Business Obligations and the various regulations that will impact your process and impact the Business. Sharing of different policies and guidelines such as PDPA, Cybersecurity Act, Computer Misuse Act 6. Your responsibility to ensure in the event of an incident, how the enterprise should handle 	

Why Should You Take This E-Learning & How Will It Help You?

Through this E-learning, we prepare your business and your employees to kickstart your journey in digital transformation and be more cyber safe. With the various contents provided in the E-Learning which will be update consistently, you have be able to have a better understanding on the digital business landscape and how to set up your initial cybersecurity framework.

An e-certificate will be given once you have completed the core modules for the e-learning and passed the quiz.

Why Is this E-Learning Special?

AiSP works very closely with our partners to produce contents that are up to date and relevant from you and your business. The content will be updated consistently to ensure our subscribers have at least **1 new** content updated in the platform.

Subscription Plan

Individual	Bundle (Min. 5 pax)*
\$7.90/month (Before GST)	\$6.00/pax/month (Before GST)*

*Minimum 1 year subscription

*Please submit subscribers' Name, Organisation & Designation, Contact Email and Contact Number separately in Excel format.

Please contact AiSP Secretariat at secretariat@aisp.sg if you have any queries.

SME Cybersafe provides



Enhanced Security
Awareness & Training



Cohesive Security
& Knowledge Resources



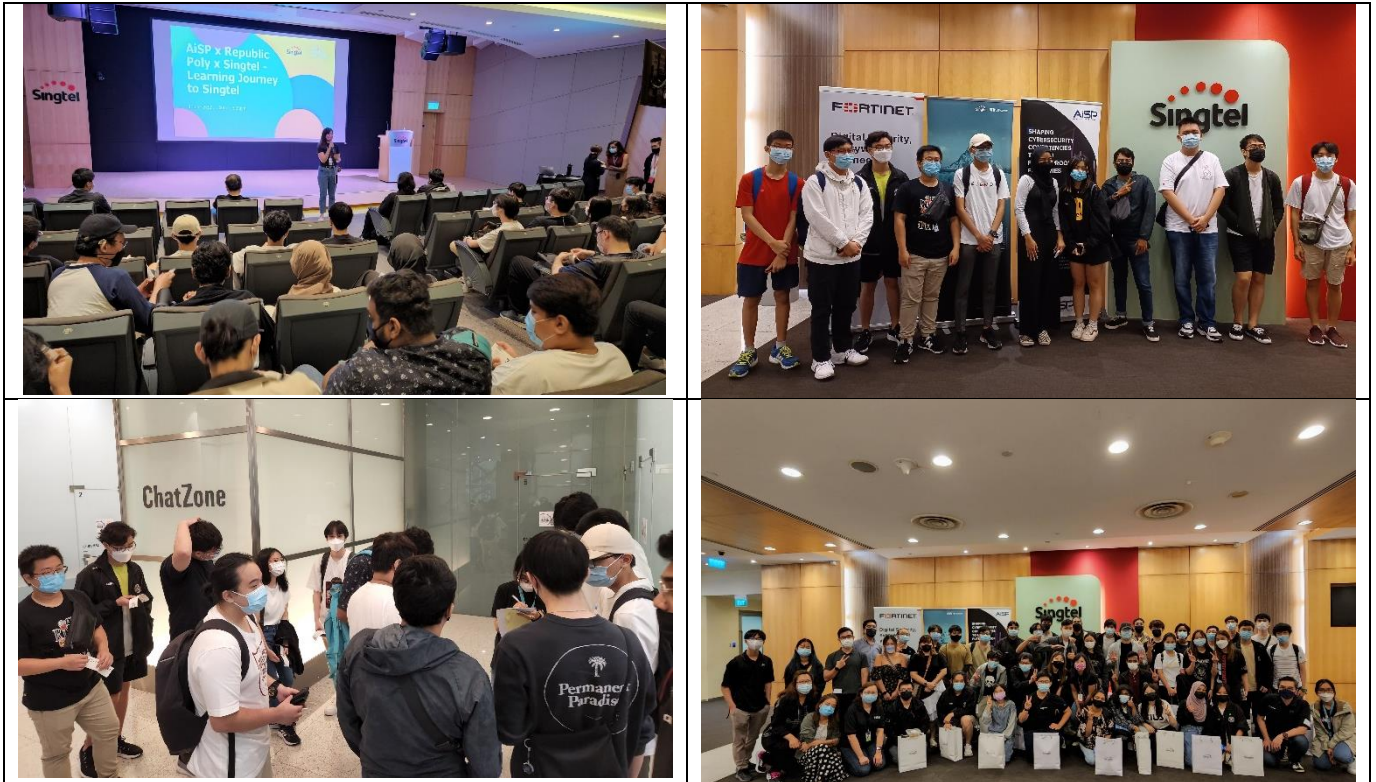
Security Solutions &
Services Support

Click [here](#) to find out more about the E-Learning.

Student Volunteer Recognition Programme (SVRP)

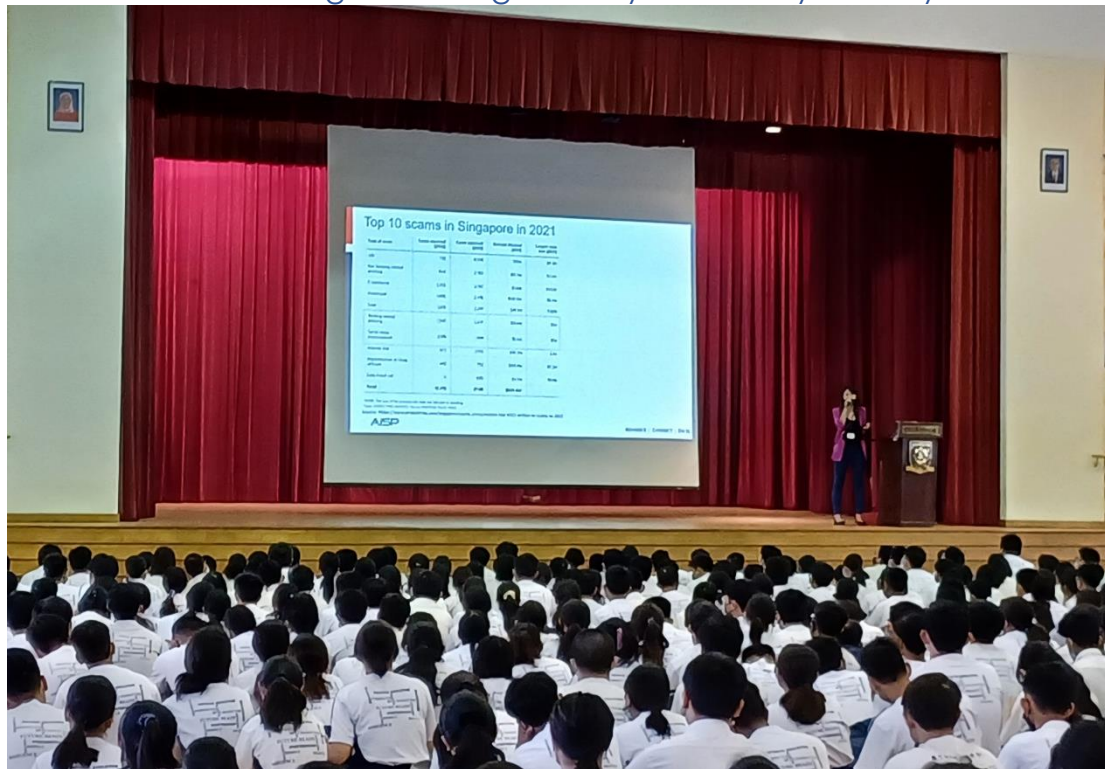
Learning Journey to Singtel office on 1 June

On 1 June, AiSP brought students from Republic Polytechnic on a learning journey to our Corporate Partner Singtel office for a morning of industry experience and scam awareness. We would like to thank Singtel for hosting us and Fortinet for their sponsorship of the F&B for the students.



School Talk at Broadrick Secondary School on 27 June

On 27 June, AiSP Vice President, Ms Sherin Lee went to Broadrick Secondary School to conduct talks on cyber hygiene and cybersecurity career prospects. Over 900 students benefitted from the talk and gained insights to cybersecurity industry.



AiSP Youth Symposium

As part of Singapore Youth Day 2022, AiSP will be organising the inaugural Youth Symposium where we will invite about 100 to 150 Youths (Subjected to COVID restrictions) from our Student Chapters to come together physically for a day of celebration and enriching activities ranging from Dialogue Session, Recruitment Talk, Internship Opportunities by some organisations and free Courses to help the students improve in their digital skills and booths from our partners to promote and share more on their plans of involving more Youths in the future.

Event Date: 2 July 2022

Event time: 12.30 PM – 4PM

Event Venue: *SCAPE

AiSP

YOUTH SYMPOSIUM





2 JUL 2022, SATURDAY
12.30 PM - 4 PM
*SCAPE

Register now!

Key Highlights:



Justin Wang
Manager
Cyber Security Agency of
Singapore

Cybersecurity: an opportunity for the young, bold and industrious!

Compared with many other professionals from various industries, pure-play cybersecurity professionals we are training today can catch up much more quickly than their more established colleagues in the industry. This is an opportunity unique to those in the cybersecurity field.



Glenice Tan
Associate CyberSecurity
Specialist
GovTech

Starter pack to Cybersecurity

Brief on the sharing:

- About GovTech's Cyber Security Group and what we do
- My personal experience as a CyberSecurity Specialist
- What you can do to kickstart your own journey in CyberSecurity



Nancy Zhang
PR Director, Huawei
International

Skills Up with Huawei

In its 21 years journey in Singapore, Huawei International has been committed to creating values for customers and communities. Bearing in mind the vision of "Bring digital to every person, home and organization for a fully connected, intelligent world", Huawei International has been actively engaging in various kinds of talent training programs in partnerships with communities, IHLs, JCs and government. By doing so, we wish to provide customized contents for audience from different backgrounds.



Dr. Raymond Chan
Assistant Professor, SIT

Madness of Metaverse: Secure or Not secure?

A number of new technologies like Metaverse, Non-fungible token (NFT), and Quantum computing have been drawing everyone's attention in recent years. In this presentation, we introduce how those technologies could impact the cyber security industry and are going to change the game.



Cyber Defenders – Guardians of the Cyber Space

The proliferation of digitization comes with vulnerabilities to cyber threats. Strengthening cyber resilience requires a robust system of capabilities that comprises People, Processes, and Technology. Elaine will provide insights into what it takes to be a Cyber Defender and how an individual may grow and develop an exciting career with Info-Security as a guardian of the Cyber Space.

Elaine Chong
AVP, Head of HR, Cyber,
ST Engineering

Panel Discussion



Soffenny Yap
SVRP Lead, AISP
Moderator



Sun Xueling
Minister of State, Ministry of
Home Affairs and Ministry of
Social and Family Development
Panelist



Tay Gao Jun
SVRP Honorary Ambassador,
Ngee Ann Polytechnic Student
Panelist



Thomas Lim
CyberSecurity Specialist,
GovTech
Panelist



Dr. Raymond Chan
Assistant Professor, SIT
Panelist



Dr. Lim Woo Lip
Chief Technology Officer,
Cyber, ST Engineering
Panelist

Organised by:



Supporting Agencies:



Supported by:



Sponsors:



Our student volunteer drive is ongoing till Dec 2022 for those who are interested to volunteer but not sure where to start. Please click [here](#) to apply today. Nomination period is from 1 Aug 2021 to 31 Jul 2022.

Nomination Period:
1 Aug 2021 to 31 Jul 2022

Nomination Period:
1 Aug 2021 to 31 Jul 2022

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

Example A Leadership: 10 Hours Skill: 10 Hours Outreach: 10 Hours	Example C Leadership: 0 Hour Skill: 50 Hours Outreach: 0 Hour
Example B Leadership: 0 Hour Skill: 20 Hours Outreach: 20 Hours	Example D Leadership: 0 Hour Skill: 0 Hour Outreach: 60 Hours

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

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

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

AiSP Cyber Wellness Programme

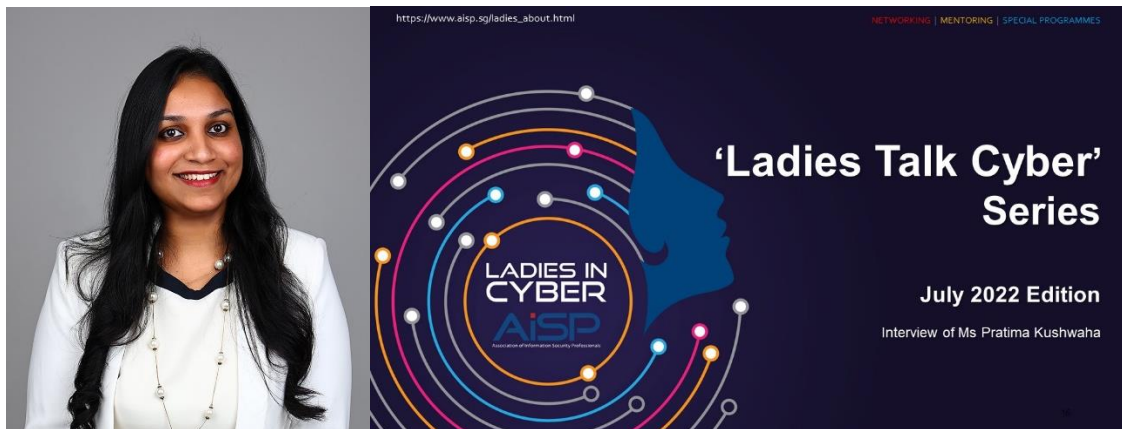
Organised by:	Supported by:	In Support of:
 Advance Connect Excel	 INFOCOMM MEDIA DEVELOPMENT AUTHORITY	 DIGITAL FOR LIFE
<p>The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. 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."</p>		 SCAN ME
<p>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.</p>		

 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 some career advice on Information Security.	 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!

Ladies in Cybersecurity



Ladies Talk Cyber Series

For the Fourteenth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Pratima Kushwaha, cybersecurity practitioner who has been working for almost 10 years, holding a master's degree in Cyber Law and Information Security.

How to be successful in cybersecurity field

In celebration of [SG Women year](#), AiSP's secretariat decided it was timely to launch a series of interviews of female leaders across industries who fulfil high impact roles, and learn about their journeys, experiences and insights. The initiative aims to shed some light on what it takes to make it in this field. The interviews can be source of invaluable career insights as well as opportunities for those in the field to get a deeper understanding of the industry, and how its leaders are innovating to disrupt the cyber landscape.

Introducing women with a deep interest in cybersecurity

Pratima is a cybersecurity practitioner who has been working for almost 10 years, holding a master's degree in Cyber Law and Information Security. Her key focus area is in cybersecurity risk & resiliency, risk governance, and compliance. She is currently working with Keppel T&T holding a Cyber Security Lead role in IT/OT risk management, compliance, and cybersecurity incident management. Aside from work, she is a member of AiSP CAAP and Ladies in Cyber Programme. Also, she is part of ISC2 Mentorship programme cohort and volunteer in ISACA Sheleadstech programme. Engaging in volunteer work in non-profit associations is something that helps keep her abreast in the field of cybersecurity.

Please click [here](#) to view the full details of the interview.



Webinar with (ISC)2 Colombo Chapter - Emotional Effects of Cyber Bullying on the Society

AiSP (Association of Information Security Professionals) Ladies in Cyber Team and (ISC)2 Colombo Chapter Sri Lanka organised our first joint webinar as part of our MOU on the topic on Cyber Bullying on 23 June. The opening address was done by AiSP Vice-President & Founder for AiSP Ladies in Cyber Charter, Ms Sherin Y Lee. AiSP EXCO Member & Ladies in Cyber Mentor Ms Eileen Yeo was one of the panellist who shared her experience and thoughts at the Panel Discussion with (ISC)2 Colombo Chapter Sri Lanka on What can we do to prevent or lessen the impact of emotional effects of cyber bullying on the society? For those who was not able to join in the session, catch the playback video [here](#).



AiSP x WiSAP Spill the Tea Webinar on 14 July

AiSP x WiSAP SPILL THE TEA | 14 JULY | 7PM - 8PM (SGT) Zoom

Organised by: AiSP, LADIES IN CYBER, WISAP

- Faith Chng**
AiSP Secretary & Ladies in Cyber Co-Lead
Associate Director, Product Management
Trustwave, a Singtel company
- Justine Co**
Deputy CISO, Bayad
- Sherin Y Lee**
AiSP Vice-President & Ladies in Cyber Founder
Vice President of Marketing, Brand and Communications,
Ensign InfoSecurity
- Lav Tambuyat**
Chief Information Security Officer, Philippine Bank of Communications (PBCOM)
- Sandy Cheong**
Assistant Director, Cyber Defence Group - Policy, Risk & Capability Development, Integrated Health Information Systems Pte Ltd (IHIS)

Click [here](#) to register

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
- Data and Privacy
- Cyber Threat Intelligence
- IoT

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



The Cybersecurity Awards



TCA 2022 Call for Nominations extended to 1 July!

SINGAPORE AWARDS CATEGORY		
<u>Professionals</u> <ul style="list-style-type: none">• Leader• Professional	<u>Enterprises</u> <ul style="list-style-type: none">• MNC(Vendor)• MNC(End-User)• SME(Vendor)• SME(End-Uder)	<u>Students</u>

Nomination extended to 1st July!
For more Information: www.thecybersecurityawards.sg

REGIONAL AWARDS CATEGORY
NOMINATE A NON-PROFIT ASSOCIATION NOW!
Nomination extended to 1st July!
For more Information: www.thecybersecurityawards.sg

In its fifth year, The Cybersecurity Awards 2022 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, The Law Society of Singapore, Singapore Computer Society and SGTech.

Visit www.thecybersecurityawards.sg for more information.

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

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

Students

4. Students

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



Organised by



Supported by



Supporting Associations



Community Partner



Supporting Organisation



Platinum Sponsors



Gold Sponsors



Silver Sponsors



Regionalisation

ENTICE Event at Kuala Lumpur, W Hotel on 7 June

AiSP was invited by Malaysia Board of Technologies (MBOT) to attend the ENTICE event at Kuala Lumpur, W Hotel on 7 June. A MOU between AiSP & MBOT was signed at the event too. Booth was set up during the event to create awareness of our activities and programmes. It was a fruitful trip for AiSP as we get to meet many Malaysian counterparts and share with them on what AiSP does and how we could further deepen the collaboration beyond borders.



CREST

An update from CREST

CREST has been working with multiple internal and external stakeholders to redefine our vision and mission. When CREST was initially formed back in 2005, it was built to serve the needs of the technical assurance industry in the UK. As we reflect on 2022, the organisation has come a long way. We are now a truly international organisation with almost 300 members; we deliver examinations in all corners of the globe and Asia, and across the multiple cybersecurity disciplines, including penetration testing, threat intelligence, Intelligence-led testing, vulnerability assessments, SOC, and incident response. As a result, it is time for us to recalibrate our focus and publish updated statements on where we are heading on what we strive to achieve.

An evolved identity

CREST is rebranding. We are listening, adapting, and responding to our member's needs. We have a newly appointed leadership team — evolving and improving our organisation process and examination strategy. The rebrand is an evolution, not a revolution; however, it is a clear signal that we are changing, with a renewed focus on our members and our exam takers.

A new website aimed at connecting buyers with CREST member companies.

We have launched a new website that supports governments, regulators, and buyers to engage with CREST accredited companies. This allows our members to create content that showcases their capabilities. The site works harder to guide buyers to capable service providers. We provide sales leads, data, and analytics to members about what buyers are searching for to provide our members with commercial opportunities.

Exam updates in 2022

A new exam delivery model is coming that will leverage remote proctoring to provide exam takers with the ability to take exams anytime and anywhere. This will allow us to deliver exams across the globe whilst enabling exam takers to take examinations from the convenience of their own homes. The movement to this model will take time. However, it will commence in 2022, with both registered and certified exams available during the year.

Improved pathways into CREST

CREST is delighted to announce strategic relationships with Hack The Box and Immersive Labs. We are working together to develop training pathways through Hack The Box and Immersive labs that will enable exam takers to better prepare for CREST examinations. As part of the relationships, CREST accredited companies will be given access to dedicated environments that will provide a series of CREST aligned learning and development instances.

In addition, by being a member of CREST, Hack The Box and Immersive Labs will provide reduced-cost access to some of their wider lab environments. This is a massive win for both exam takers wanting to build skills and member companies looking to develop learning and development pathways.

Evolving accreditation process

We have launched an updated accreditation process requiring all individuals involved in scoping, delivering, and sign-off of a CREST accredited service to demonstrate their current skills and competencies. As we move through 2022, we will run a series of industry consultations to shift to a tiered accreditation model that we hope to launch in 2023.

A consistent international governance structure

At the end of 2021, CREST ran a series of elections across all our regions. We now have elected council members operating in Asia, Australasia, the US, Europe, and the UK. This new structure facilitates local decision-making geared to supporting CREST member companies domestically and internationally. Through these new councils, we are already forming new strategic alliances with multiple governments and regulatory stakeholders, all with the intention of driving opportunities for CREST member companies.

The cybersecurity industry is evolving rapidly, and the needs and expectations of members and external stakeholders are continually increasing. We aim to be the go-to global organisation for cybersecurity accreditation and certification through our continuous focus on improvement.

With a renewed focus on the exam candidate experience and significantly enhanced member benefits, we aim to enhance the CREST member company experience continually. CREST is committed to all our exam takers and our CREST member companies. We are laser-focused on supporting our members to build and enhance their skills and competencies across the industry in Asia. We are actively pursuing pathways that drive inclusion and maximise existing returns on investment.

We are here to enhance the cybersecurity ecosystem. Please feel free to get in touch with our Regional Advocate and Chair for CREST Asia, Emil Tan - emil.tan@crest-approved.org

Visit our website for further news and updates: 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
2 Jul	AiSP Youth Symposium	AiSP
4 Jul	Learning Journey to Singtel with ITE West Students	AiSP & Partner
6 Jul	Knowledge Series – Incident Response Management	AiSP & Partner
12 Jul	Learning Journey to Acronis with ITE West Students	AiSP & Partner
12 – 13 Jul	Operational Technology Cybersecurity Expert Panel Forum 2022	Partner
12 – 13 Jul	PhilSec 2022	Partner
14 Jul	AiSP x WISAP Spill the Tea webinar	AiSP & Partner
19 Jul	AiSP x JTC PDD Networking Session	AiSP & Partner
19 – 22 Jul	Cyber Security Digital Summit: APAC 2022	Partner
20 Jul	Knowledge Series – CTI	AiSP & Partner
23 – 24 Jul	Skills for Good 2022 Carnival	Partner
27 Jul	Cybersecurity Awareness Webinar with 5hue	AiSP & Partner
28 Jul	SCCCI CAAP Workshop	AiSP & Partner
4 Aug	LawSoc Cybersecurity Conference	AiSP & Partner

15 Aug	School Talk at Victoria School	AiSP & Partner
16 Aug	AiSP x MBOT Ladies in Cyber Joint Webinar	AiSP & Partner
24 Aug	Knowledge Series – Security Operations	AiSP & Partner
25 Aug	IASA BITAS Conference 2022	Partner
29 Aug – 1 Sept	Virtual AppSec APAC 2022	Partner

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

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

How HUAWEI CLOUD Harness On Cloud Security

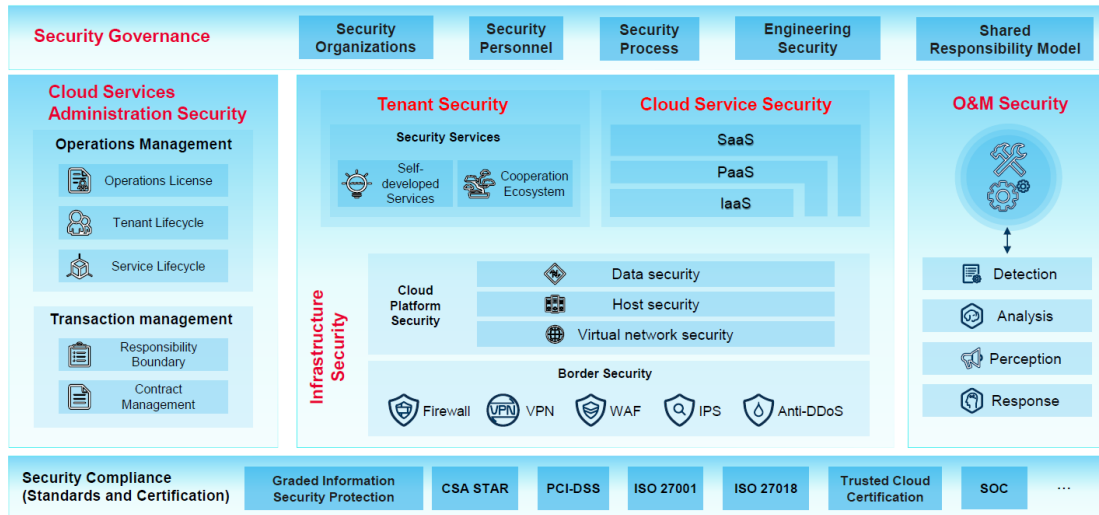
DENNIS CHAN, Country Cybersecurity & Privacy Officer, Huawei International

In recent years, especially during the pandemic, we have observed that there has been a strong demand of enterprises and companies that are accelerating their digitalization journey and migrating to the cloud is in most organizations' roadmaps. At the same time, new and complex cyber threats have also emerged at an alarming pace, and customers need to continuously review their cybersecurity posture and business processes to mitigate risks and threats.

Huawei has established comprehensive set of cloud security strategies and best practices as security baseline, with multi-layered security architecture to provide in-depth defense that is compliant with all relevant standards and regulations. Huawei designs and builds security into cloud architecture and continues to improve the security of commonly used services like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). To support all of these, both Huawei Research and Development (R&D) and Operations and Maintenance (O&M) teams stay abreast on latest security developments; using DevSecOps methodologies to optimize the security of Huawei Cloud. Together with our ecosystem partners, we continue to make our customers as our top priority and deliver high-quality cloud services with value added security functions, providing advanced cloud security services and security consulting services.

Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment, had released a list of top threats like data leakage, misconfigurations and change control, identity authentication, key management, account hijacking, etc. HUAWEI CLOUD has established a security architecture and solution (see figure below) to mitigate the CSA top threats.

[back to top](#)



Infrastructure Security as a core component of HUAWEI CLOUD multi-dimensional, full-stack cloud security system, where we have enhanced the security and compliance of our data centers, networks, and other infrastructure based on industry best practices.

HUAWEI CLOUD is deployed in multiple regions and availability zones (AZs) around the world. When it comes to network security design there are considerations like how to prevent any propagation of possible attacks and minimize the potential impact of attacks. Huawei has also implemented a network segregation strategy by referencing and adopting the security zoning principle of ITU E.408 and industry best practices for network security. To ensure continuity of HUAWEI CLOUD operations, different communication planes have been designed and built into HUAWEI CLOUD network based on the need of business functions, security risk levels, and access privileges. Security hardening for all systems and middleware and attack prevention (anti-virus, anti-APT, anti-brute force, etc) to reduce attack surface and risks of attack. It is also essential to continuously monitor processes, status and key metrics to detect abnormalities.

Tenant Security is the other area which HUAWEI CLOUD takes serious consideration on as a necessary security requirement to protect our tenants in the cloud environment. Identity and Access Management (IAM) will enforce stringent account and access creation with two-factor authentication to manage both administrators and users access privileges.

We also consider APIs as another crucial security perimeter of cloud services and there is a need to employ multilayered protection mechanisms and measures to safeguard API security. APIs can be invoked through the API Gateway which will provide the necessary API protection mechanisms while the IAM performs identity authentication on each API request. The API Gateway also controls the frequency of each user's API access to ensure the availability and continuity of API based access. One other key component in Tenant Security is Key Management Service (KMS) which is a secure, reliable, and easy-to-use key escrow service that facilitates centralized key

management for users to achieve better key security while KMS employs Hardware Security Module technology for key generation and management. There are cloud HSM services able to provide industry standard encryption or country-specific encryption algorithms and cipher suite strengths, allowing the cloud tenants to choose the most suitable option to meet their requirements.

HUAWEI CLOUD also provides a suite of cloud security services including value-added security as a service (Anti-DDoS, Vulnerability Scan Service, Web Application Firewall, etc), comprehensive security configurations and defense reports are also made available to help our tenants to achieve security compliance. In addition, HUAWEI CLOUD also provides comprehensive protection for users' data and information assets through security measures spanning many aspects such as confidentiality, integrity, availability, durability, and traceability. There is of great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. Huawei will always strive to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business.

Cybersecurity is about shared responsibilities between Cloud Service Provider and customer. Huawei helps our customers by providing secure and trusted cloud services through collaboration with our ecosystem partners and in accordance with our committed lines of business, furthering our objective to safeguard and add value to our customers' business. Today, Huawei provides cloud services that comply with mandatory security standards and regulations, such as Singapore MTCS Level 3 and other related international certification such as ISO27001 and CSA STAR. Huawei has also attained Data Protection Trustmark (DPTM) from PDPC, demonstrated both capabilities and competence in data privacy and protection.

For more details, you may visit Huawei Cloud Trust Center website:

<https://www.huaweicloud.com/intl/en-us/securecenter/overallsafety.html>

Article from Cyber Threat Intelligence SIG

[back to top](#)

Rantings of a Cyber Security Analyst

"Oh, you work in IT? Can you help me with a problem on my computer?"

I am sure anyone who works in the IT field has heard this during family gatherings. In a way, I understand there is always a misconception that people who work in the IT field are assumed to know everything about IT.

Computers, servers and all applications have always been marketed as easy to use products that can solve issues. I would draw this comparison with cars. Cars are always marketed as easy to drive, nice features and good mileage per tank or charge. No one would ever market a car with all the technical details like the camber angle, toe and so on, which made the handling of the car great (I am sure I lost some of you guys here). But that is the point, and for this example, a car mechanic would understand all these and yet, the mechanic would likely find a specialist who does alignment if there is an issue with the car pulling to one side when driving straight. This also translates to the business world where some smaller companies hire a single IT Manager to deal with all things that fall under the IT umbrella.

Information Technology is a name that covers a very wide field of specializations; there is Networking, Database, Application Developers, Security and so on. For me, I have gone towards the path of security and have dedicated myself towards this field. Sure, I may know some networking concepts, but I am not the right guy to deploy complex networking with various proprietary network protocols (FabricPath and QFabric comes to mind) or attempt to build and maintain a database.

Most of us can pull out the administrator guide and understand what all those text means. This helps us to do the basic stuff, like installing the application or service into the server, but that does not mean we know how it works.

Most small IT teams do their best to manage many things. Making sure everyone's laptop and workstations are working normally, all business applications are installed, new users are created on the Active Directory with the right user roles, deploying security controls, maintaining the servers and cloud instances... the list is long. This does not mean they know how everything works, and usually they would ask the respective vendor or partner for assistance. This all works out well as all these activities can be planned and assistance can be arranged prior.

However, security is always a complex subject. Sure, there are tons of solutions out there that can be deployed and installed, but all these solutions are threat deterrence. Think of this as installing a gate for your home. The gate does not fully prevent people from breaking in, it just adds a layer of deterrence but would not stop an extremely determined individual from trying to break in. You can add CCTV cameras, but again, that does not stop the determined individuals and if no one is constantly watching the CCTV feeds, no one is going to react accordingly. And unlike solutions that help to

[back to top](#)

increase productivity and bring profit to organizations, security spending is often hard to justify when the management does not look at it from a risk perspective.

Fortunately, more organizations are starting to understand this, and more are building a structured IT team or getting outsourced services to help them out. So please give the single IT personnel a break. He or she may not know everything about security and having the individual burnt at the stake for something beyond his or her expertise is uncalled for. And to the very first question... No, I will not help you fix your computer.

Harvey Goh is a cyber security specialist having been in the cyber security industry for over 15 years as a technical personnel. Currently he is working as part of Sophos' Managed Threat Response team. Views and opinions expressed in this article are my own and do not represent that of my places of work. While I make every effort to ensure that the information shared is accurate, I welcome any comments, suggestions, or correction of errors.

Article from our CPP Partner, Micro Focus

Digital Value Chain Attacks on a Rapid Rise with Ransomware Victims Nearly Doubled Year over Year

CyberRes, a [Micro Focus](#) line of business, released the [2022 CyberRes Galaxy Annual Report](#) on the current state of cyberthreats and an overview of cyber events in 2021. This strategic report signifies another milestone of the advanced threat research journey that started with the launch of the immersive Galaxy Online platform in January 2022 to deliver better cyber resiliency to the market.

[CyberRes](#)' Research shows that threats have rapidly evolved to target the growing threat surface of organizations that have incorporated digital into their business growth DNA. As organizations move quickly to adopt digital as a competitive differentiator, adversaries are equally quick at exploiting vulnerabilities in the digital value chain.

The 2022 CyberRes Galaxy Annual Report is the first in a series to provide a perspective on geopolitical, regional and industry threat conditions and what to expect throughout the year. Some of the key findings for 2021 outlined in the report include:

- North America topped the list of most impacted regions, experiencing 33.5% of the cyber issues reported, followed by Asia-Pacific at 23.5% and Europe at 20%.
- Globally, approximately 19.3% of the cyberattacks were ransomware.



total

[back to top](#)

- The services sector was most targeted globally, with 33.7% of cyberattacks, followed by the public sector (21.4%).
- There was a 200% growth in cyberattacks targeting the financial sector.
- Almost 69% of the cyberattacks in North America were motivated by financial gain.
- Germany (21.6%) and France (18.3%) were the two countries affected most by cyberattacks in Europe.
- Approximately 33% of the total cyberattacks conducted in the Asia-Pacific region were meant for cyber espionage, followed by financial gain.
- In Latin America, LockBit ransomware accounted for 28.3% the region's total ransomware attacks, followed by Prometheus ransomware with a share of 13%.
- In the Middle East and Africa, 31% of the geopolitical and cybersecurity events were motivated by financial gain and political advantage.
- The telecommunication and technology sectors experienced the most cyberattacks in the Australia-New Zealand region with 35.7%, followed by financial services at 18.5% and the healthcare sector at 11.4%.

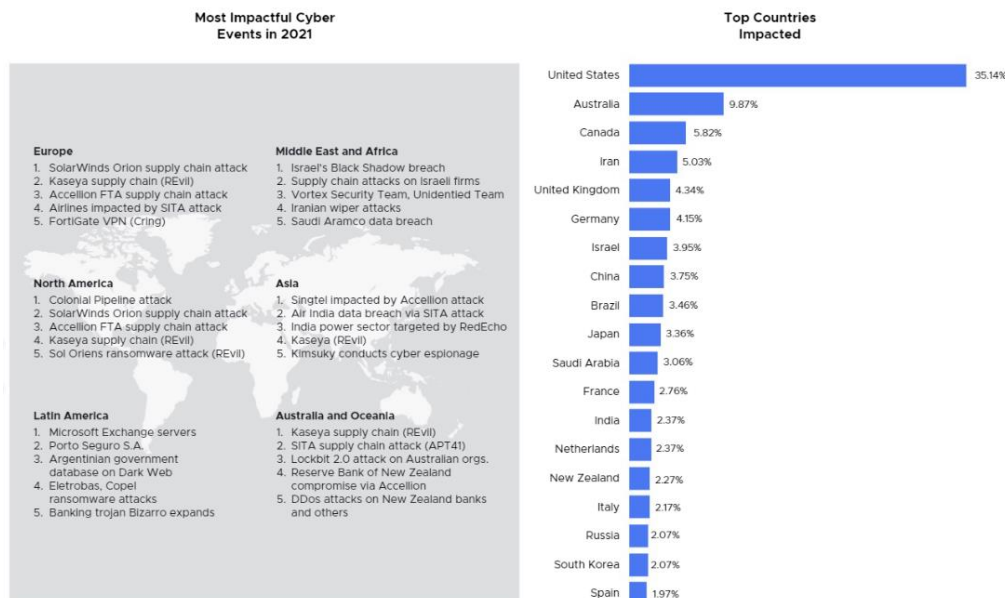


Figure 1 - Top cybersecurity events by region and top countries impacted by cybersecurity events in 2021

“Everyone is at risk from feeling direct or indirect impacts from cyberattacks, as all records were smashed last year in terms of the sheer number of cyberattacks on government entities, private-sector organizations, and individuals,” said Mark Fernandes, Global CTO at CyberRes. “Unfortunately, this trend is continuing in 2022. One of the key effective defenses is to maintain a clear understanding of the current landscape, tactics, and threats that could be emerging.”

This Annual Report was compiled by experts in the [CyberRes Galaxy Threat Research Program](#), which continuously tracks existing and emerging global cybersecurity threats. In addition to active threats, the program continuously tracks geopolitical and social events, as research has shown that they have a direct correlation to cyber activity and the constantly evolving threat landscape.

The report is available [here](#).

Article from our Youth Symposium Partner, CSA

Singapore Launches OT Train-The-Trainer Programme

Cyber Security Agency of Singapore (CSA) launched the Operational Technology (OT) Cybersecurity Competency Framework (OTCCF) on 8 October 2021 to guide OT organisations in talent attraction and development.

During the development of this framework, industry and academic stakeholders also highlighted the lack of local OT trainers. To build up a pool of local trainers, CSA launched an OT Train-The-Trainer (OT TTT) programme. In line with OTCCF, this programme equipped them with a valuable skillset of conducting foundational OT cybersecurity training. To provide realistic hands-on exercises, OT TTT was conducted at Singapore University of Technology and Design (SUTD)'s renowned iTrust research centre water test bed.

The first run of the OT TTT was conducted in November 2021 and it was attended by local tertiary educators. Subsequent runs will also include OT practitioners who are involved in conducting in-house cybersecurity training in OT organisations.

The OT TTT consists of two modules:

a) Module 1 Cybersecurity Industrial Control Systems Engineer Plus (CSIE+)

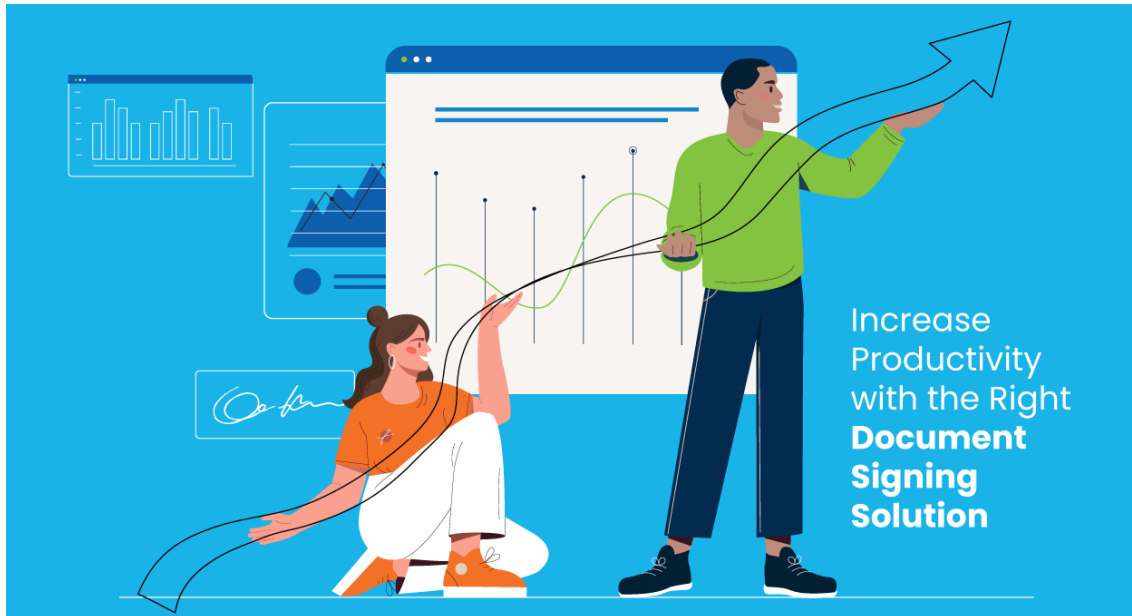
This 4-day technical training equips trainees with the technical knowledge in defending OT networks and detecting OT attacks. Hands-on sessions provide trainees with a deeper understanding of the various tools whilst acquiring control systems cybersecurity skills. It includes a one-day cyber exercise that allows trainees to apply what they learn in a realistic OT environment and react to impeding cyber-attacks.

b) Module 2 Project with Practicum

Trainees will propose their own project after completing Module 1. The scope of the project should cover various topics of OT cybersecurity aligned with OTCCF. Such project work provides participants with the opportunity to deepen their hands-on skills in tackling real-world OT issues. Trainees will present their completed projects to a panel who will assess the quality of project work. Project outcomes will also be shared among the community and used by the faculty in their OT curriculum.

For any enquiries, please contact Mr Simon Lam at Simon_LAM@csa.gov.sg

Article from our CPP Partner, Globalsign



Increase Productivity with the Right Document Signing Solution Workflow automation through GlobalSign's GMO Sign

Document signing is a key aspect in an organisation's workflow. Whether it is in purchasing or entering into agreements, document signing is integral in solidifying contracts globally. Traditionally, the use of wet-ink signatures was the only way to do this. However, as technology has advanced, signing solutions have also evolved. Digital signatures can now be utilised to make workflows more efficient and secured. They serve as the backbone for advanced document signing solutions.

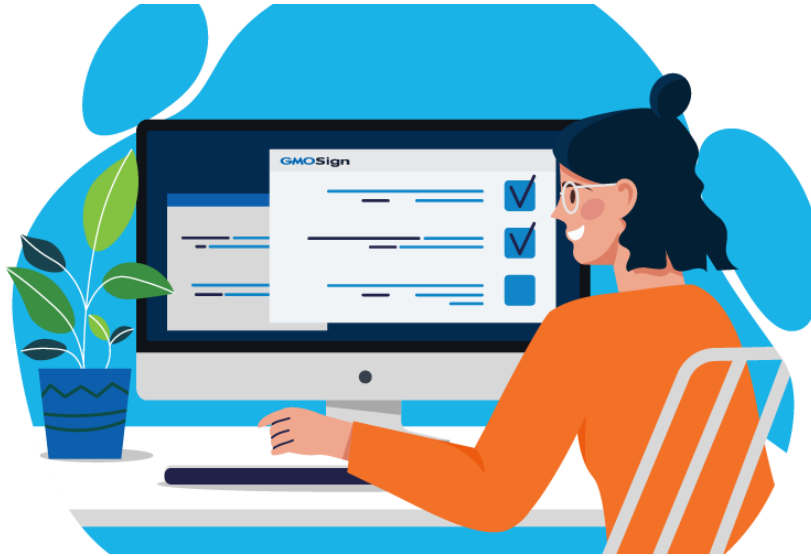
What is a digital signature?

Workplace transformation has increased the need for digital signatures. The digital signature is a certificate-based signature that follows an encryption technique called Public Key Infrastructure (PKI) that uses mathematical algorithms to generate keys. Digital signatures are considered the most secure way of signing documents. PKI protects the creation and saving of keys through a trusted Certificate Authority (CA) that serves as a guarantor of the public key's authenticity and integrity. Additional features, such as timestamping and audit trails, ensure that the document is tamper-free and protected throughout the process. The high level of security has made digital signatures globally accepted and considered compliant in various industries.

What is a document signing solution?

Traditionally, organisations are hesitant to adapt digital signatures due to the difficulty in managing certificates. As time passed, document signing solutions have been developed to address this need.

Document signing solutions combine digital signatures and other technology to streamline organisation workflows. These solutions are meant to increase efficiency in the workplace and manage certificates attached to the digital signatures used in the organisation.



Do all document signing solutions work the same?

While having the same goal of streamlining and securing workflows, not all document signing solutions are built the same way. Some signing solutions go beyond digital signatures. Thus, it is important to assess the document signing solution that will be the best fit for your organisation's needs. Considerations in choosing include:

1. **The ease of use.** Digital signatures allow users to cut down manual processes. However, if a document signing solution is hard to use, there is a tendency for the process time to take longer. Document signing solutions should be accessible and easy to use – having a user-friendly interface, global support, and certificate management features.
2. **The solution's compliance.** Globally, there are different regulations attached to signing documents. An organisation must ensure that the document signing solution will meet all compliance requirements attached to the industry or territory they operate in.
3. **The price and scalability of the solution.** Streamlining workflows require an initial investment. The document signing solution's benefits to the organisation must outweigh the costs involved. Similarly, it should cater to the need of the organisation, be it a small business or a multinational company.

What is GMO Sign?

GMO Sign is an all-in-one document signing solution that allows organisations to automate and secure workflows through digital signatures and document management. Developed by GlobalSign, this thoughtfully crafted solution goes beyond digital signatures. GMO Sign also serves as a document management system, helping you not just to sign the document, but also efficiently manage and track documents that have been signed by people in your organisation.

Being an all-in-one document signing solution, GMO Sign offers features that allow workflow automation, such as integration with other document signing solutions, secured cloud data storage, record keeping system, and support to various signature types such as AATL digital signatures and eIDAS-compliant advanced electronic signatures. All these features come at an affordable price point, allowing your organisation to start your digital transformation journey in a cost-effective way.



Workflow automation with GMO Sign

Workflow automation refers to the method of making manual processes, documentations, and communications independently performed. This is commonly used in repetitive tasks and procedures that need to improve in accuracy, such as document signing. With GMO Sign double hatting as a digital signature and a document management solution, workflow automation is made possible. GMO Sign allows users to digitally sign and file important paperwork using only one platform. HR, Finance, Sales, or any other team in your organisation can automate their document signing and archiving process with ease using the five-step method:

- 1) uploading a document or selecting an existing template.
- 2) inputting document information and set a sign position.
- 3) automated signing workflow.
- 4) reviewing the document and signing.
- 5) downloading and archiving the signed document.

Following these five easy steps, your organisation can cut down process time and effort used in manual document signing and archiving, while also ensuring that the documents are kept safe from the sender up until storage.

With GMO Sign, a frictionless document signing experience can be built within your organisation. Workflow automation is made possible with this solution.

Why is workflow automation important?

In today's fast paced environment, workflow automation is essential for businesses to succeed. Automating workflows is beneficial for various reasons – including the overall increase in productivity, faster operations, and improvement in accuracy of manual processes. Workflow automation can also lead to cost savings and better adherence to industry regulations.

For organizing documents, user group and folder access management settings are in place to ensure documents are secure and in the right hands. Robust search and archiving functionality also give users an enhanced view into the document's history.

Digital transformation in business

Businesses are now moving towards digital transformation. This practice integrates digital technology in all business areas to create new value for customers. Digital transformation begins with automation of workflows within the organisation. Therefore, to generate new value, it is necessary to optimise areas like document signing and archiving. [With GlobalSign's GMO Sign, your business can ensure an efficient and secured workflow.](#)

FEATURES YOU WILL ENJOY

- ✓ Secures a document
- ✓ Capable of encryption
- ✓ Timestamping and long-term validation features
 - ✓ Proves authorship and identity of the signer
 - ✓ Legally valid and admissible
 - ✓ Has audit trail
 - ✓ Authorised and regulated by a trusted Certificate Authority (CA)
- ✓ Assurance that standard e-signatures does not provide.
- ✓ Free bundle feature by GlobalSign.

DO NOT MISS THIS OFFER!

Contact us today at
sales-apac@globalsign.com / 3158 0349
quoting the subject: "AiSP Special + your company name".

For further enquiries, please contact GlobalSign APAC at sales-apac@globalsign.com

Article from The Cybersecurity Awards 2021 Winner – Huang Shaofei



I am deeply grateful to the Cyber Security Agency (CSA), the Singapore Cyber Security Inter-Association (SCSIA) organising committee and panel of judges, and the Singapore cybersecurity professional community for the honour of winning The Cybersecurity Awards 2021 (Leader Category).

The Cybersecurity Awards carry special significance for me personally, as they represent firm recognition of individuals' abilities to:

- Co-create the Singapore cybersecurity eco-system in partnership with the Government, the industry, and trade chambers and associations;
- Promote international recognition of Singapore cybersecurity professionals, standards and industry events; and
- Lead, contribute and grow the Singapore cybersecurity community.

Since the early years of my cybersecurity career, I have somehow participated (or sometimes, "arrowed" to participate) in both Singapore and international cybersecurity communities in some capacity. From SIG² (hint of how young I am!) to ISC2 (I was a volunteer proctor, before online exams became the norm), then to the Singapore Computer Society Cybersecurity Chapter, and then AISP ... and the list goes on! And when I was the CISO at Land Transport Authority, I was honoured to co-chair the Cybersecurity Working Group at the UITP (Union Internationale des Transports Publics) i.e. the International Association of Public Transport. These experiences have shaped my approach to leadership, and at the same time, my hope and dream for the Singapore cybersecurity eco-system in the future.

As I reflect on my cybersecurity career over the past 24 years, there are numerous superiors, colleagues, ex-colleagues, family and friends, industry partners, and even people whose names I have forgotten (but apologetically so). All of whom I am indebted to, in one way or another. To each and everyone of you, thank you.

And in the same way as I benefited from those who inspired me on my journey, I will continue to lead, contribute and inspire our future cybersecurity leaders in Singapore!

Visit <https://www.aisp.sg/publications> for more contributed contents by our partners.

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International



Ready to Crack the Toughest Cyber Challenges?

CyberQ
Fully Cloud Orchestrated Military-Grade Cyber Range

Master core cyber skills and techniques with performance-based skills pack on EC-Council's cyber range platform!

VULNERABILITY RESEARCH FOR HACKERS AND PEN TESTERS SKILL PACK
10 distinct exercises with up to three attempts for each challenge!

Vulnerability research techniques covered:

- advanced google hacking
- source code analysis
- traffic analysis
- exploitDB search
- searchsploit search
- SQL vulnerability scanning
- vulnerability scanning using burpsuite

WHO IS IT FOR?
Blue/red team technician, CND auditor, ethical hacker, IS engineer, internal enterprise auditor, pen-tester, network security engineer, reverse engineer, risk/vulnerability analyst and technical surveillance countermeasures technician

SPECIAL PRICE \$112 FOR AISP MEMBERS
EMAIL AISP@WISSEN-INTL.COM NOW!

Brought to you by **Wissen International - EC-Council** Exclusive Distributor

Ready to crack the toughest cyber challenges?

Master core cyber skills and techniques with performance-based skills pack on EC-Council's cyber range platform that covers 10 exercises in vulnerability research techniques such as source code analysis, exploitDB search and more.

Enjoy a special price of \$112 for AiSP members, please email aisp@wissen-intl.com now!

Listing of Courses by ALC Council



Stand out from the crowd

Cyber security offers one of the best future-proof career paths today. And ALC – with our industry-leading program of cyber certifications - offers you one of the best ways to advance your cyber career.

We offer the most in-demand cyber certifications including:

- CISM®, CRISC®, CISA®, CGEIT®, CDPSE®
- SABSA®, NIST®, ISO 27001
- CISSP®, CCSP®
- CIPM, CIPT, CIPP/E

The right training makes all the difference

Lots of things go into making a great course, but the single most important is always the trainer: their knowledge of the subject; their real-world experience that they can draw upon in class; their ability to answer questions; their communication skills. This is what makes the difference.

ALC works only with the best. That has been the core of our business model for the past 28 years. You can see the calibre of our trainers on our [Faculty](#) page.

AiSP Member Pricing – 15% discount

AiSP members receive 15% discount on all ALC training courses. To claim your discount please enter the code **ALCAiSP15** in the Promotion Code field when making your booking.

Upcoming Training Dates

Click [this link](#) to see upcoming Course Dates. If published dates do not suit, suggest an alternative and we will see what we can do.

Special Offers.

We periodically have special unpublished offers. Please contact us aisp@alctraining.com.sg to let us know what courses you are interested in.

Any questions, don't hesitate to contact us at aisp@alctraining.com.sg .

Thank you.

The ALC team



ALC Training Pte Ltd

3 Phillip Street, #16-02 Royal Group Building, Singapore 048693

T: (+65) 6227 2883 | E: learn@alctraining.com.sg | www.alctraining.com.sg

Qualified Information Security Professional (QISP®) Course



Companies around the world are doubling down on their security as cyber attacks see an increase in frequency, intensity and severity. It is thus critical for businesses and organisations to have Qualified Information Security Professionals to manage cybersecurity threats and incidents.

To support the development of personnel in this profession, the Association of Information Security Professionals (AiSP) is offering the Qualified Information Security Professional (QISP) Programme.

This special five-day training programme is based on AiSP's Information Security Body of Knowledge (IS BOK) 2.0. This course will prepare participants for the QISP examinations. After attending this course, participants will also be able to understand and attain knowledge in these areas:

- Enterprise Governance
- Risk Analysis and Management
- Security Controls
- Security Principles and Lifecycle
- Business Continuity Planning
- Develop and Implement Security Goals, Objective and Strategy and Programs
- Maintain and Review Security Operations

COURSE DETAILS

2022 Course dates can be found on https://www.aisp.sg/qisp_training.html

Time: 9am-6pm

Fees: \$2,500 (before GST)*

*10% off for AiSP Members @ \$2,250 (before GST)

*Utap funding is available for NTUC Member

TARGET AUDIENCE

- Professionals who wish to learn more or embark into Cybersecurity
- Security Professionals who will be leading or taking on a senior management/technical role in ensuring Enterprise Governance is achieved with Corporate, Security and IT Governance

COURSE CRITERIA

There are no prerequisites, but participants are strongly encouraged to have:

- At least one year of experience in Information Security
- Formal institutional training in cybersecurity
- Professional certification in cybersecurity

For registration or any enquiries, you may contact us via email at secretariat@aisp.sg or Telegram at [@AiSP_SG](https://www.instagram.com/AiSP_SG).

Program Partner

Delivery Partners





This course is suitable for people who are new to information security and in need of an introduction to the fundamentals of security, people who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification. Professionals who are in need to be able to understand and communicate confidently about security terminology.

To support the development of personnel who are new to information security and wish to pursue career in this profession, the Association of Information Security Professionals (AiSP) is offering the Cybersecurity Essentials Course. With the completion of this course, participants will have an overview on cybersecurity. The course will build on the foundation to prepare participants for Qualified Information Security Professional (QISP) course.

Course Objectives

This 3-day training program is for those who have very little knowledge of computers & technology with no prior knowledge of cyber security. After attending this course, participants will also be able to understand and attain knowledge in these areas:

- Introduction to Security
- Risk Management
- Cybersecurity IT Platform
- Securing the Server
- Securing the Network
- Cloud Computing
- Cybersecurity Operations

COURSE DETAILS

Training dates for year 2022 can be found on https://www.aisp.sg/cyberessentials_training.html

Time: 9am-6pm

Fees: \$ \$1,600 (before GST)*

*10% off for AiSP Members @ \$1,440 (before GST)

*Utap funding is available for NTUC Member

TARGET AUDIENCE

- New to cybersecurity
- Looking for career change
- Professionals need to be able to understand and communicate confidently about security terminology

Please email us at secretariat@aisp.sg to register your interest.

Program Partner



Delivery Partners



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: 2021 to 2022) from 1 Sept 2021 to 31 Dec 2022. 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.

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. Interested applicants should be qualified [AiSP Ordinary Members \(Path 1\)](#) for at least a year to apply for AVIP.



Sign up for

AVIP MEMBERSHIP

AVIP membership is the FIRST in Asia to bundle the Professional Indemnity for professionals involved in cybersecurity related work, to give them greater assurance undertaking projects in Singapore and worldwide.

BENEFITS

- Recognition as a Trusted Infocomm Security Professional. You can use the designation of **AVIP (AiSP Validated Information Security Professionals Member) as your credentials.**
- **Special Invite** to Exclusive Activities & Events.
- AVIP members enjoy the **Professional Indemnity Coverage in Singapore and Overseas (FIRST in Asia)!**
- AVIP members will be invited for key dialogue sessions with national & industry leaders for their opinions on cyber security.
- AVIP members will be invited to **represent AiSP for media interviews** on their opinions on cyber security.

PRICE

CPP: \$321* (One-time fee)
Ordinary (Path 1) Members: S\$481.50 (1st 100 applicants in 2022)
Annual Membership: \$267.50
*Price includes GST

EMAIL MEMBERSHIP@AISP.SG TO SIGN UP AND FOR ENQUIRIES

Your AiSP Membership Account

AiSP has ceased its digital platform, Glue Up and are currently exploring other options to provide our members a better and user-friendly experience.

Membership Renewal

Individual membership expires on 31 December each year. Members can renew and pay directly with one of the options listed [here](#). We have GIRO (auto - deduction) option for annual auto-renewal. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.

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

Please check out our website on [Job Advertisements](#) by our partners.

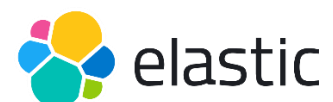
For more updates or details about the memberships, please visit

www.aisp.sg/membership.html

AiSP Corporate Partners



Acronis





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

AiSP Academic Partners



Our Story...

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

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

Our Vision

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

Our Mission

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

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



 www.AiSP.sg

 secretariat@aisp.sg

 +65 8878 5686

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

Please [email](mailto:secretariat@aisp.sg) us for any enquiries.