AiSP NEWSLETTER
November 2022

NEWS & UPDATE

New Partners

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

Continued Collaboration

AiSP would like to thank INTfinity, Kaspersky and Rajah & Tann Cybersecurity for their continued support in developing the cybersecurity landscape:

News and Updates

AiSP @ Cyber Security World Summit on 12-13 October

On 12-13 October, AiSP was part of the Singapore Pavilion to set up a booth at the Cyber Security World Summit to share on what AiSP is about and encourage signups for membership. We also shared on the initiatives and events that AiSP provides for members and the community in general.

ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS (AISP)
B50
SINGAPORE
AiSP
ELEVATE YOUR INFORMATION SECURITY KNOWLEDGE & STANDING BEYOND FRONTIERS
AiSP Association of Information Security Professionals

back to top

GovWare 2022 on 18-20 October and Memorandum of Understanding (MoU) signing with CREST

AiSP was present at the GovWare 2022 on 18 – 20 October to share on what AiSP is about and encourage signups for membership. As part of GovWare, AiSP organised a Memorandum of Understanding (MoU) signing with CREST on 19 October. The purpose of the MoU between CREST International and AiSP is to create a formal basis for cooperation and collaboration between the two organisations to participate in and benefit from each other's respective initiatives to create a vibrant and dynamic international information and cybersecurity ecosystem in Singapore.

AiSP is pleased to have Mr Ak Mohd Farid Zulhusni Pg Aziz, Senior Operation Officer from IT Protective Security Services (ITPSS) from Brunei to visit our booth and explore collaborations between AiSP and ITPSS. Senior Leadership personnel from Huawei (AiSP CPP) also invited AiSP to their booth during the event.

AiSP also held a networking session for our Ordinary and Associate members on 19 October where they gathered for drinks and chit-chat session with our committee members. AiSP would like to thank Image Engine who invited us to GovWare 2022 and share on AiSP to local and foreign professionals.

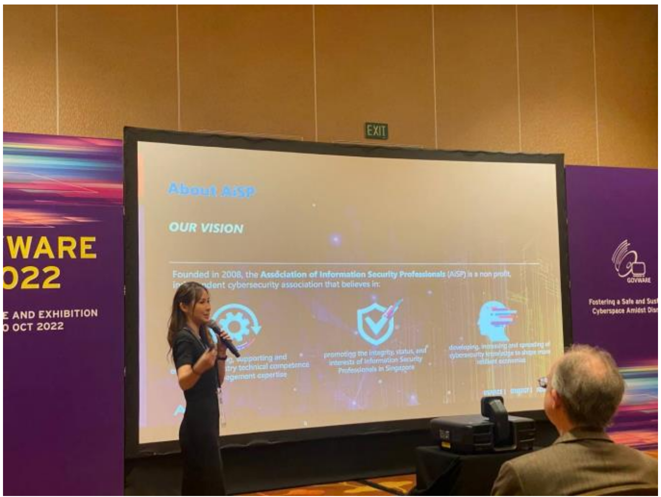
AiSP
GOVWARE 2022
Memorandum of Understanding Between
AiSP
Advance Connect Excel
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS (AiSP)
OUR VISION
SHAPING CYBERSECURITY COMPE
TO BUI
FUTURE
ECONO
CLOUD SECURITY

back to top

Knowledge Series Events

Internet of Things on 19 October

On 19 October, AiSP organised the monthly Knowledge Series focusing on Internet of Things at Marina Bay Sands where Govware was held. Our Corporate Partners, Boston Consulting Group , NetWitness and wizlynx group shared insights to our attendees on IoT.



EXIT
GOVWARE 2022
CONFERENCE AND EXHIBITION
18 - 20 OCT 2022
ur Classic Cybersecurity IT Skills
Not Ensure a Smooth IoT Journey
NETWITNESS

back to top

Upcoming Knowledge Series

DevSecOps on 17 November

AiSP Knowledge Series – DevSecOps

In this Knowledge Series, we are excited to have Checkmarx, Kroll and Scantist to share with us insights on DevSecOps. 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.

Delivering Security at the Speed of DevOps
Speaker: Aaron Zhou, Regional Sales Engineer, Checkmarx

Security must be embedded into developer workflows during every stage of the SDLC. Software development, delivery, and deployment is a continuous process. This webinar provides tips to help you move to a DevSecOps environment with ease. By taking this approach to DevSecOps, organizations can be confident in the security of their applications. Embedding the right security solutions and approaches help you achieve the benefits of DevSecOps.
Learn:

- What is DevSecOps and why is it challenging to move to DevSecOps
- Benefits of DevSecOps to the whole organization
- Tools and best practices – how to move DevSecOps

back to top

DevSecOps Mythbusters
Speaker: Aakash Goel, Vice President, Cyber Risk, Kroll

This talk would touch upon the foundations of a successful DevSecOps practice, how shifting left the AppSec practices is not a theoretical concept but a sound reality, and what benefits does agile practices bring to the table when it comes to implementing DevSecOps principles to threat modelling, penetration tests, etc.

Open Source Security: Challenges, Solutions, and Opportunities
Speaker: Prof. Liu Yang, Co-founder, Scantist

open-source software (OSS) has become increasingly popular in software development to simplify and shorten the developing cycle. Unfortunately, the reuse of OSS also brings security risks that OSS vulnerabilities could be excessively amplified. Therefore, identifying, managing, remediating, and governing the potential risks throughout the OSS supply chain is promptly required to be further investigated. we will discuss the rigorous situation of the vulnerable software supply chain, as well as the challenges we are facing to secure the OSS environment. We will also show our recent efforts and solutions in securing the OSS supply chain, including our techniques on software component analysis (SCA), OSS supply chain analysis, license-related risk management, artificial intelligence-based security vulnerability analysis, and our larger scope of governing OSS with health profiles for both open-source software, as well as corresponding development teams. We also highlight the potential opportunities of OSS security and call for research in this direction.

Date: 17 November 2022, Thursday
Time: 3PM – 5PM
Venue: Zoom
Registration:
https://us06web.zoom.us/webinar/register/8016658255646/WN_vemZUAt8QmCzaVVPXLEOQA

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. DevSecOps BOK Series, 17 Nov 22
2. Data & Privacy, 18 Jan 23
3. Software Security, 22 Feb 23
4. Business Continuity, Physical Security & Audit, 22 Mar 23

Please let us know if your organisation is keen to provide speakers! Please refer to our scheduled 2022 webinars in our event calendar.

back to top

Cybersecurity Awareness & Advisory Programme (CAAP)

Malware Awareness Day on 6 January 2023

Malware Awareness Day

Date/Time : 6th Jan 2023, 3PM – 4.30PM

Venue : Huawei Digi X Lab

Dennis Chan
AiSP Exco
Country Cybersecurity & Privacy Officer
Huawei

Yum Shoen Yih
Former Director of CSPC
Cyber Security Agency of Singapore

Ferdinand Fong
Cyber Security Practitioner
wizlynx group

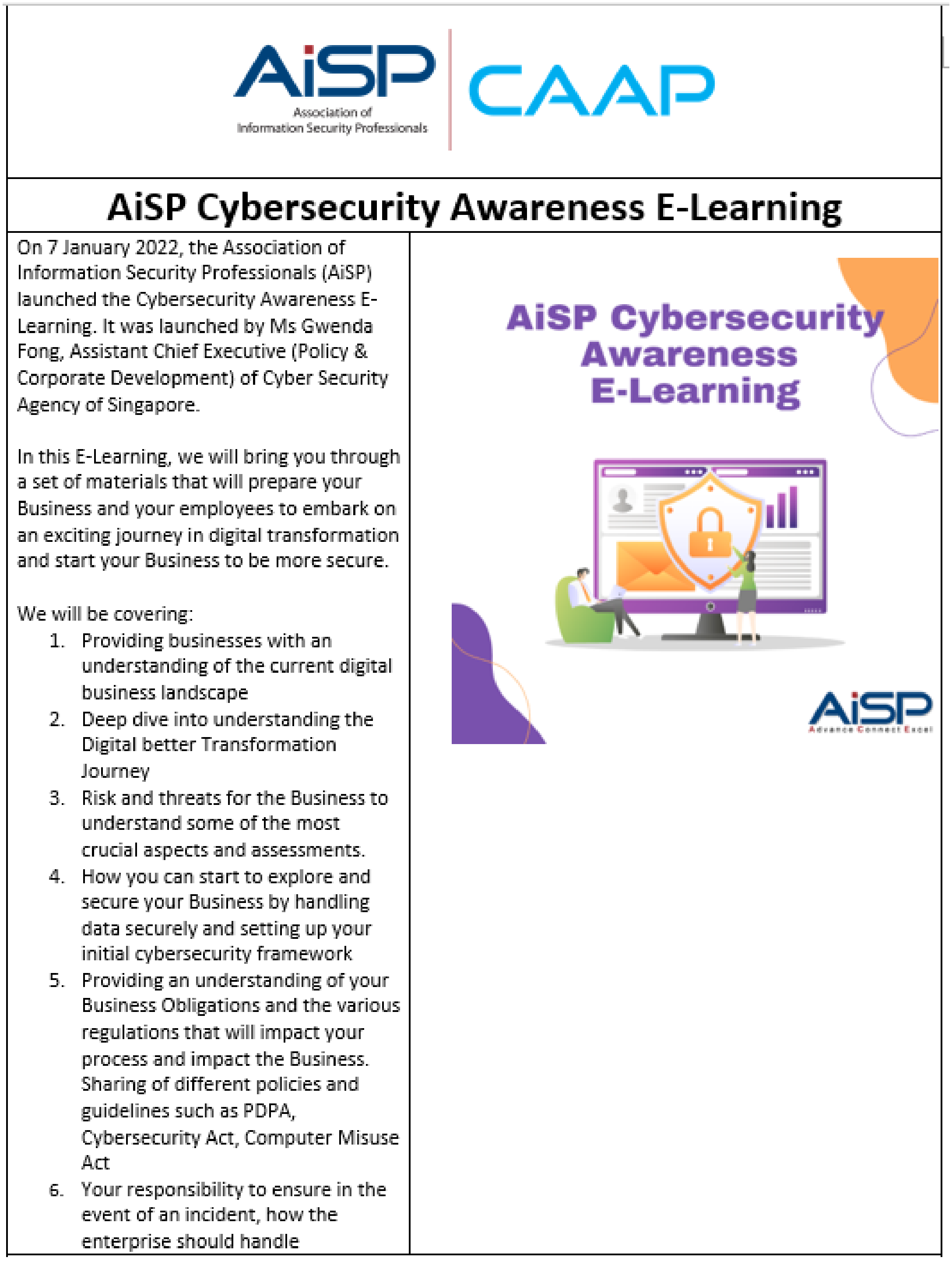
Jeffery Zhang
CTO Data Center and Storage Solution Sales
Huawei

6th January has been dedicated as Anti-Malware Day. On this day we will like to honor all the cybersecurity professionals at the frontline and behind the scene on the collective effort to stamp out on malware. There is no better way to prevent malware than raising awareness hence Huawei together with AiSP will like to present you Malware Awareness Day on 6th January at Huawei DigiX Lab. Come and hear from our VIP speakers Mr Yum from CSA, Ferdinand Fong from Wizlynx and Jeffery Zhang from Huawei.

Email karen.ong@aisp.sg to RSVP now.

back to top

AiSP Cybersecurity Awareness E-Learning



AiSP Association of Information Security Professionals | CAAP

AiSP Cybersecurity Awareness E-Learning

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.

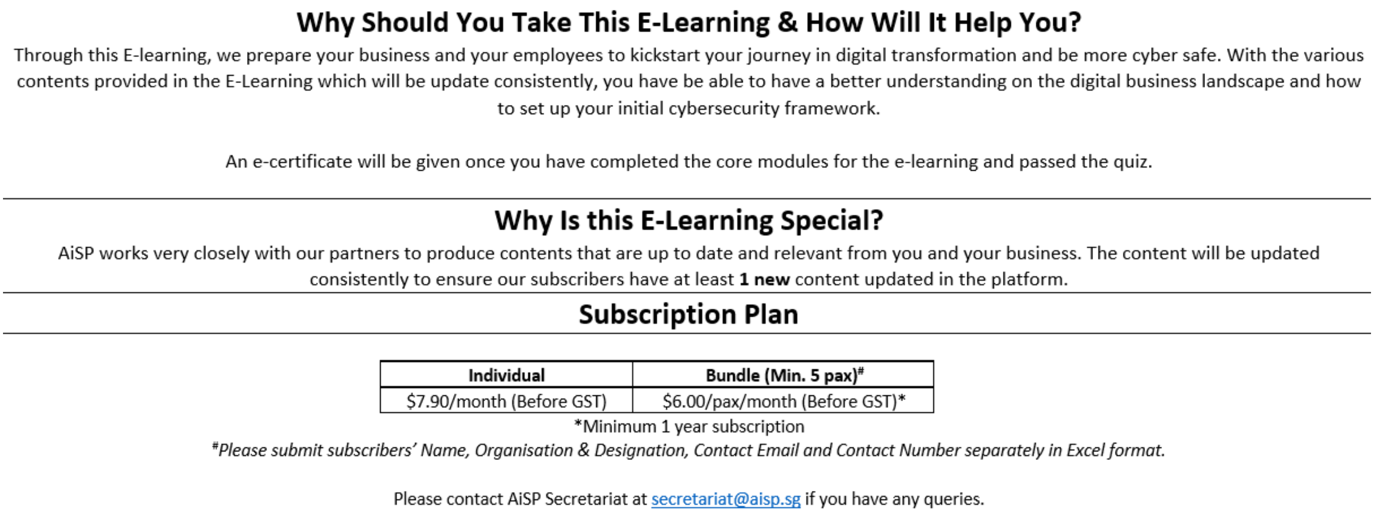
In this E-Learning, we will bring you through a set of materials that will prepare your Business and your employees to embark on an exciting journey in digital transformation and start your Business to be more secure.

We will be covering:

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

AiSP Cybersecurity Awareness E-Learning
AiSP Advance Connect Excel

back to top



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.

back to top

Student Volunteer Recognition Programme (SVRP)

Learning Journey to CISCO for ITE West on 13 October

As part of Digital for Life Movement, AiSP brought 42 ITE West students on a learning journey to our Corporate Partner, Cisco. We hope the students have gained insights from the learning journey.

Student Volunteer Recognition Programme Awards Ceremony on 16 November 2022

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.

SVRP Nomination has officially concluded, and results has been released on our website here. The fourth SVRP Awards Ceremony will be held on 16 November 2022 at SIT@Dover.

The Awards Ceremony is sponsored by:

HUAWEI

back to top

NTU – Scantist DevSecOps Networking Session

NTU-Scantist DevSecOps Networking Session
Transform Yourself to Make the Cyber World Safe
Event Organisers:
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
SCANTIST
OpenSSF
Event Supporters:
AiSP
HUAWEI
SPARK
IMPERVA INCAPSULA
azul

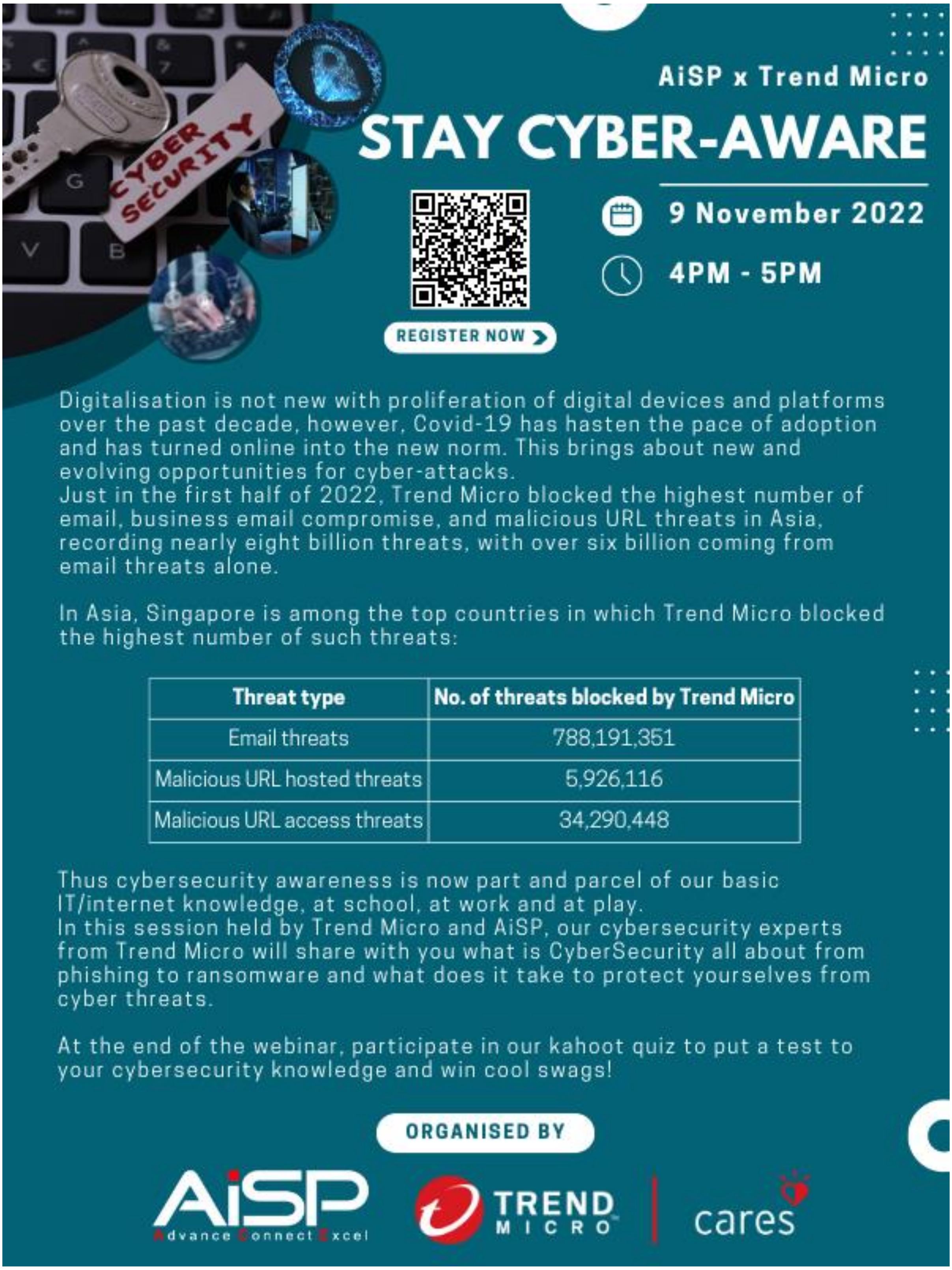
The NTU-Scantist DevSecOps Professional & Tools course is offered in collaboration with Cyber Security Research Centre @ NTU (CYSREN), with a focus on addressing cybersecurity risks at the software development level. Join the networking event organised for you to meet the DevSecOps course lecturers, graduates, professional cyber experts and our guest-of-honour, Julian Gordon, APAC Vice President, from OpenSSF. OpenSSF is working with the fast-growing list of member companies like AWS, Google, Microsoft, and Redhat and leading government agencies on a community-led effort to address this issue, and Scantist is proud to be the first Singaporean company to join them.

AiSP will be there to promote our membership and upcoming activities that you can participate in too. We hope to catch up with you over drinks, and provide insights on the following topics:
Open Source Security: Challenges, Solutions, and Opportunities
IT Career with Professional Cyber Security Qualification
Overview of Program NTU-Scantist DevSecOps Course

Register now by clicking here.

back to top

AiSP x Trend Micro Stay Cyber-Aware



CYBER SECURITY

AiSP x Trend Micro

STAY CYBER-AWARE

9 November 2022

4PM - 5PM

REGISTER NOW

Digitalisation is not new with proliferation of digital devices and platforms over the past decade, however, Covid-19 has hasten the pace of adoption and has turned online into the new norm. This brings about new and evolving opportunities for cyber-attacks.
Just in the first half of 2022, Trend Micro blocked the highest number of email, business email compromise, and malicious URL threats in Asia, recording nearly eight billion threats, with over six billion coming from email threats alone.

In Asia, Singapore is among the top countries in which Trend Micro blocked the highest number of such threats:

Threat type	No. of threats blocked by Trend Micro
Email threats	788,191,351
Malicious URL hosted threats	5,926,116
Malicious URL access threats	34,290,448

Thus cybersecurity awareness is now part and parcel of our basic IT/internet knowledge, at school, at work and at play.
In this session held by Trend Micro and AiSP, our cybersecurity experts from Trend Micro will share with you what is CyberSecurity all about from phishing to ransomware and what does it take to protect yourselves from cyber threats.

At the end of the webinar, participate in our kahoot quiz to put a test to your cybersecurity knowledge and win cool swags!

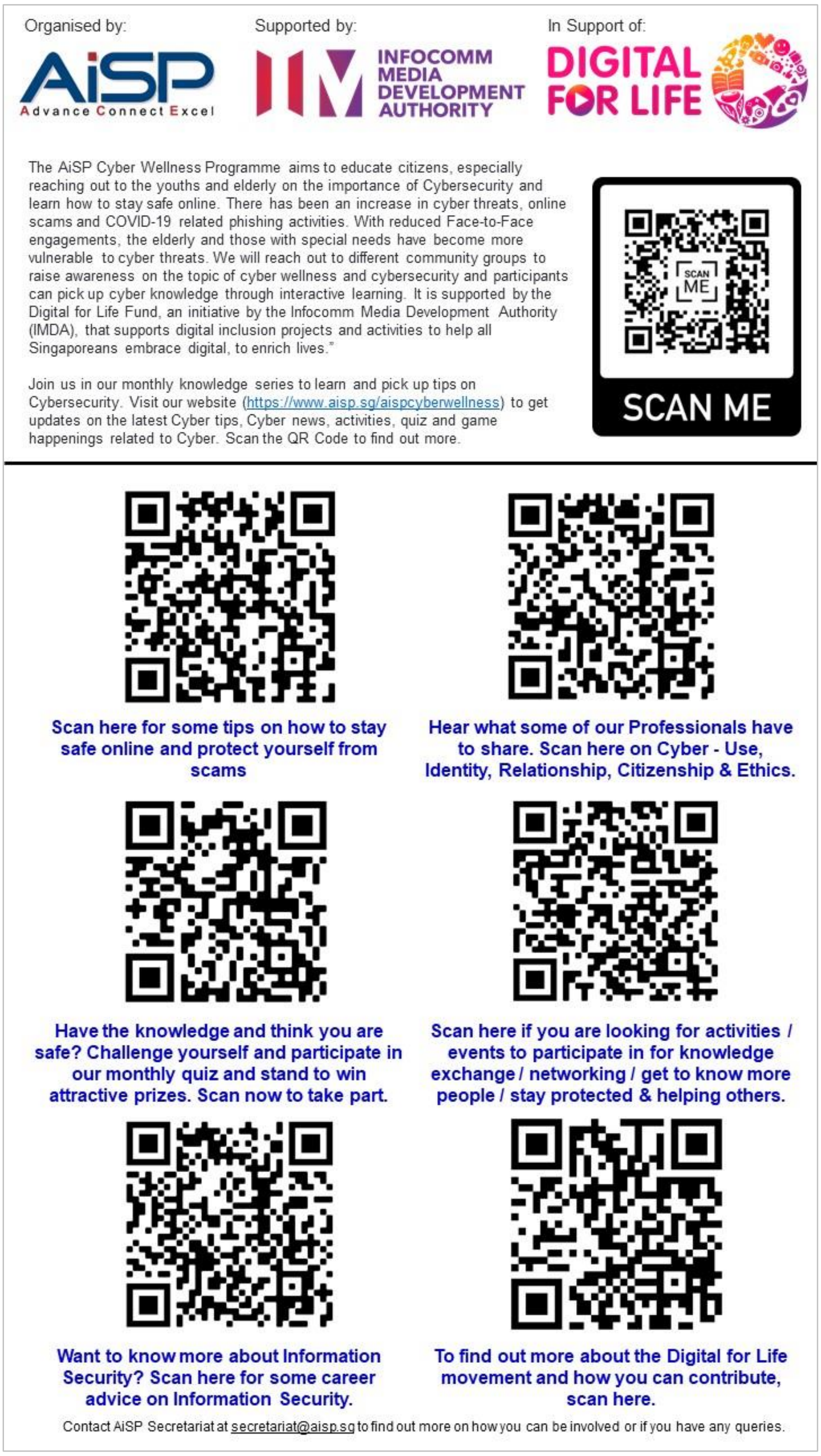
ORGANISED BY

AiSP Advance Connect Excel | TREND MICRO | cares

Click here to register.

back to top

AiSP Cyber Wellness Programme



Organised by: AiSP Advance Connect Excel

Supported by: INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In Support of: DIGITAL FOR LIFE

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

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

SCAN ME

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!

back to top

Ladies in Cybersecurity

https://www.aisp.sg/ladies_about.html
NETWORKING | MENTORING | SPECIAL PROGRAMMES
LADIES IN CYBER
AiSP
Association of Information Security Professionals
'Ladies Talk Cyber' Series
November 2022 Edition
Interview of Dr Magda Chelly

Ladies Talk Cyber Series

For the Sixteenth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Dr Magda Chelly, who is currently working as a Managing Director and founder of her own company – Responsible Cyber.

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

Dr Magda Chelly is a world-renowned cybersecurity professional. She has actively built cybersecurity strategies for companies and provided guidance on topics from governance and security architecture to security operations as a Certified Information Systems Security Professional (CISSP) and Certified Information Security Officer (S-CISO). Her vast industry experience comes from taking on roles ranging from IT consultant to Information Security Officer and most recently, Head of Cyber Risk Consulting at Marsh Asia, where she developed a quantitative measure for cyber risks and built on their risk identification and risk transfer capabilities.

Please click here to view the full details of the interview.

back to top

Ladies in Cyber Webinar on 1 November

Association of Information Security Professionals (AiSP) and Malaysia Board of Technologists (MBOT) Ladies in Cyber Webinar on 01 November 2022 from 2pm to 4pm:

Join AiSP Vice-President and Founder for AiSP Ladies in Cyber Charter Ms Sherin Y Lee and Chief Information Security Officer of Telekom Malaysia, Ms Raja Azrina for an afternoon sharing and discussion on the **Importance of Cybersecurity and Career Options in the Industry.**

Ms Raja Azrina will be sharing on the Cyber Threat Landscape and Cyber Resiliency and Ms Sherin Y Lee will share on the Career Option in Cybersecurity. Join us to hear their personal experience in their day-to-day job and how they are coping between their career and personal life. Join us to find out their motivation on what motivate them to stay them on and what are some of their biggest setbacks that they faced in their journey and what they hoped to achieve in the future. Anyone with an interest in Cybersecurity are welcome to join in the session by scanning the below QR Code to register for the event. We looked forward to having you with us at the session.

ONLINE

AiSP x MBOT Ladies in Cyber Webinar

Importance of Cybersecurity and Career Options in The Industry

01 November 2022

2PM - 4PM

LIVE

Cyber Threat Landscape and Cyber Resiliency

YBrs. Puan Raja Azrina Raja Othman
Chief Information Security Officer
Telekom Malaysia

Career Option in Cyber Security

Sherin Y Lee
Vice-President & Founder of Ladies in Cyber Charter
AiSP

Organised By

AiSP Association of Information Security Professionals

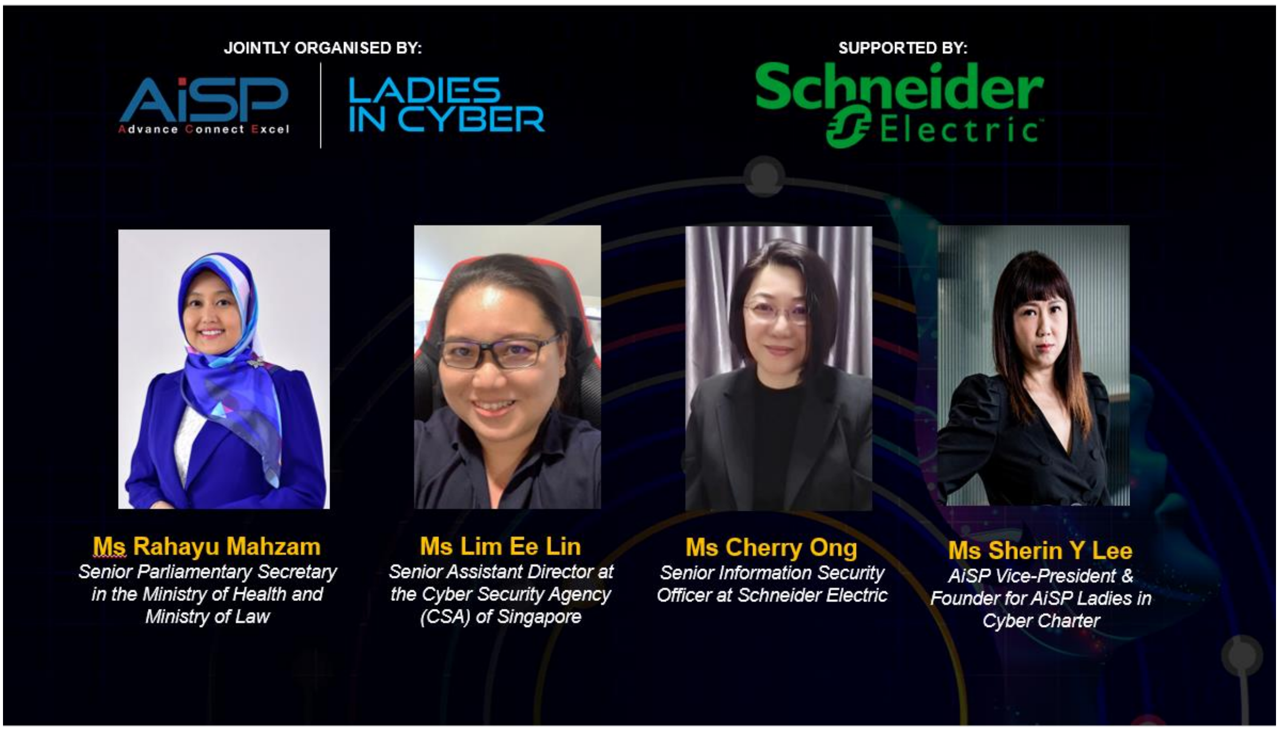
MBOT LEMBAGA TEKNOLOGIS MALAYSIA

ELIGIBLE FOR CPD POINTS

Click here to register if you are unable to scan the above QR Code.

back to top

Learning Journey to Schneider Electric on 15 Nov



JOINTLY ORGANISED BY:
AiSP Advance Connect Excel | LADIES IN CYBER

SUPPORTED BY:
Schneider Electric

Ms Rahayu Mahzam
Senior Parliamentary Secretary in the Ministry of Health and Ministry of Law

Ms Lim Ee Lin
Senior Assistant Director at the Cyber Security Agency (CSA) of Singapore

Ms Cherry Ong
Senior Information Security Officer at Schneider Electric

Ms Sherin Y Lee
AiSP Vice-President & Founder for AiSP Ladies in Cyber Charter

AiSP will be organising the Ladies in Cyber Learning Journey to Schneider Electric on 15 Nov 22. As part of the Learning Journey, we will be having a dialogue session at the event itself. The dialogue session will be sharing about support ladies in their career in Singapore.

We are honoured to have Ms Rahayu Mahzam (Senior Parliamentary Secretary in the Ministry of Health and Ministry of Law) for the dialogue session together with Ms Lim Ee Lin (Senior Assistant Director at Cyber Security Agency of Singapore), Ms Cherry Ong (Senior Information Security Officer at Schneider Electric). Ms Sherin Y Lee, AiSP Vice-President and Founder for Ladies in Cyber Programme will be the moderator for this event. The event is open to all female students in tertiary level.

The details for the event are as follow:

Date: 15 Nov 22 (Tues)
Time: 6.15pm to 9pm
Venue: Schneider Electric, 50 Kallang Avenue, Singapore 339505
Dress code: Smart Casual (No wearing of shorts and slippers)
Guest of Honour: Ms Rahayu Mahzam, Senior Parliamentary Secretary in the Ministry of Health and Ministry of Law

Click here to register.

back to top

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

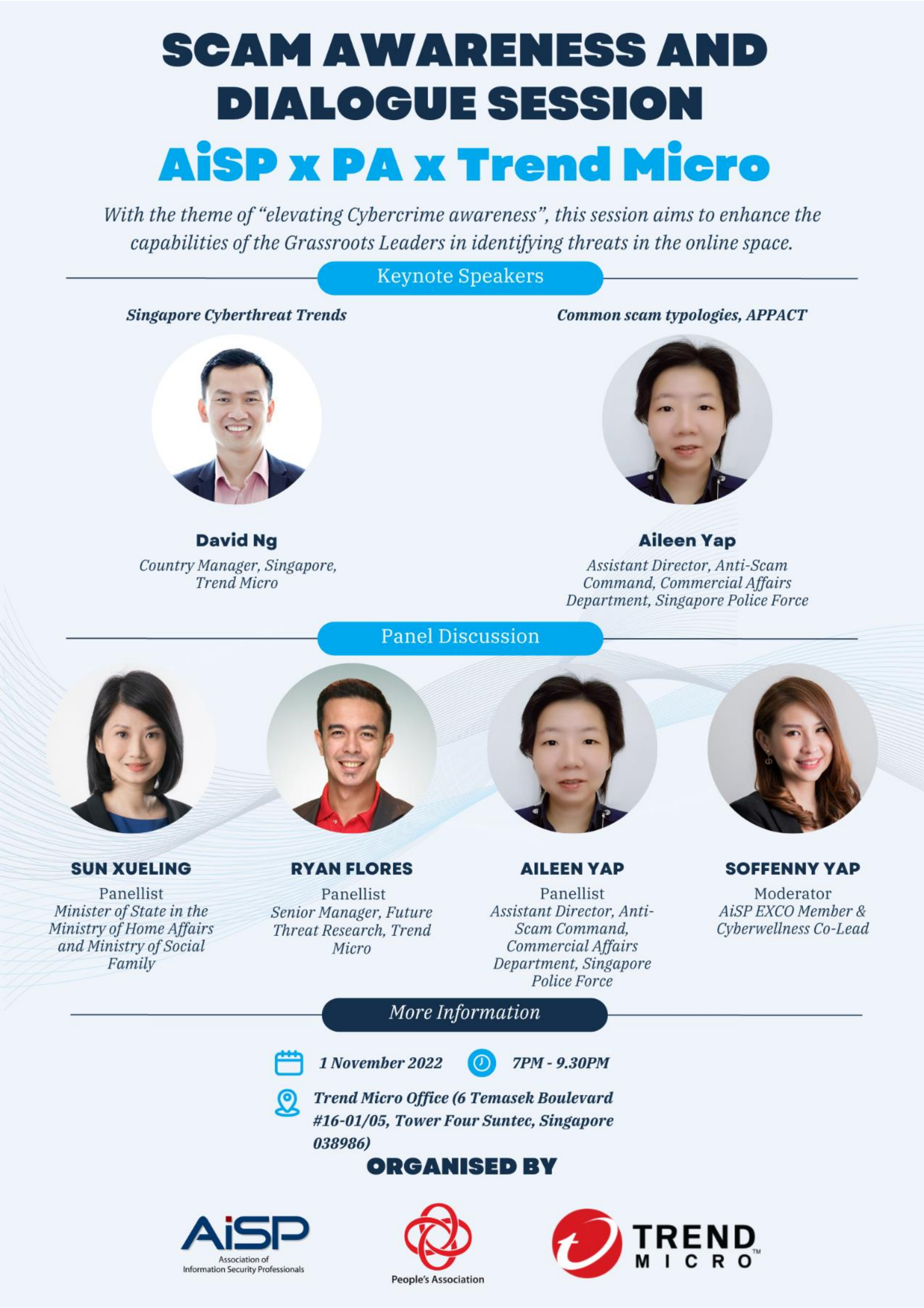
Digital for Life

Celebrate Digital @ Kebun Baru on 23 October

AiSP went down to Kebun Baru Community Club on 23 October and shared with the residents on scam awareness. The residents had a good time participating in the activities and CyberWatch which they won attractive prizes from.

back to top

AiSP x PA x Trend Micro Scam Awareness and Dialogue Session on 1 November (Closed Door Event)



SCAM AWARENESS AND DIALOGUE SESSION

AiSP x PA x Trend Micro

With the theme of "elevating Cybercrime awareness", this session aims to enhance the capabilities of the Grassroots Leaders in identifying threats in the online space.

Keynote Speakers

Singapore Cyberthreat Trends

David Ng
Country Manager, Singapore, Trend Micro

Common scam typologies, APPACT

Aileen Yap
Assistant Director, Anti-Scam Command, Commercial Affairs Department, Singapore Police Force

Panel Discussion

SUN XUELING
Panellist
Minister of State in the Ministry of Home Affairs and Ministry of Social Family

RYAN FLORES
Panellist
Senior Manager, Future Threat Research, Trend Micro

AILEEN YAP
Panellist
Assistant Director, Anti-Scam Command, Commercial Affairs Department, Singapore Police Force

SOFFENNY YAP
Moderator
AiSP EXCO Member & Cyberwellness Co-Lead

More Information

1 November 2022 ***7PM - 9.30PM***

Trend Micro Office (6 Temasek Boulevard #16-01/05, Tower Four Suntec, Singapore 038986)

ORGANISED BY

AiSP Association of Information Security Professionals
People's Association
TREND MICRO™

The Cybersecurity Awards

THE CYBERSECURITY Awards 2022

Thank you for all your nominations.
Results will be announced on 11 November 2022

In its fifth year, The Cybersecurity Awards 2022 seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems.

Visit www.thecybersecurityawards.sg for more information.

back to top

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

Students

4. Students

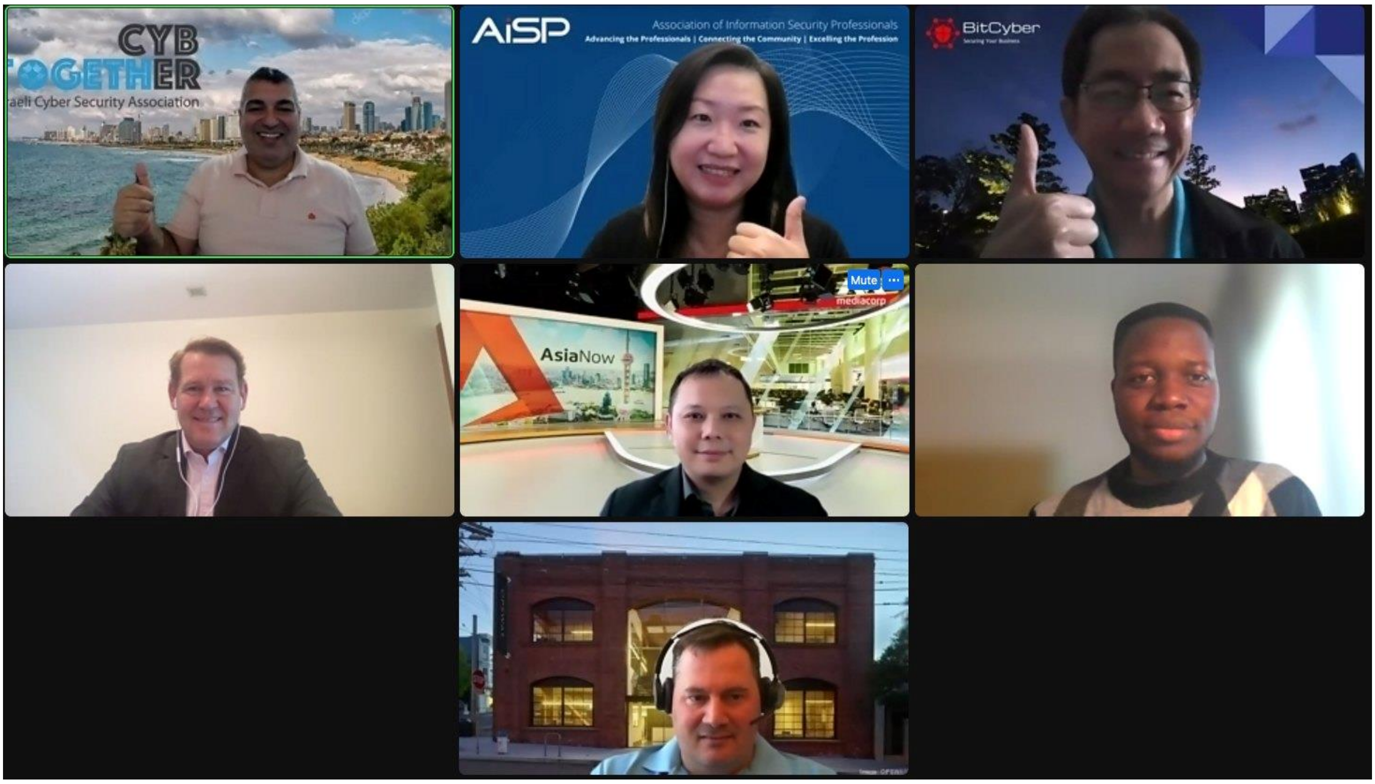
Enterprises

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

Regionalisation

AiSP x CyberTogether Cyber Leaders Series on 26 October

In collaboration with CyberTogether, AiSP organised a webinar on 26 October for the Cyber Leaders Series. AiSP would like to thank AiSP EXCO Member, Ms Faith Chng & Mr Alon Refaeli from CyberTogether for the opening address. We would also like to thank Mr Philip Ng (BitCyber), Mr Tzer Yeu Pang (Mediacorp), Dr Fene Osakwe (Forbes Technology) and Mr Itay Glick (OPSWAT) for sharing insights with our attendees. A big thank you to Mr Malcolm Rowe (OPSWAT) for moderating the panel discussion.


CYB
TOGETHER
aeli Cyber Security Association
AiSP
Association of Information Security Professionals
Advancing the Professionals | Connecting the Community | Excelling the Profession
BitCyber
Mute
mediacorp
AsiaNow

back to top

South East Asia Cybersecurity Consortium on 23 – 24 November

Cybersecurity is borderless and the COVID-19 crisis has pushed many individuals and organisations to leverage the digital economy for sustainable development and growth. AiSP setup the Southeast Asia Cybersecurity Consortium (SEA CC) to:

1. Create a consortium of like-minded individuals and organisations that have a part to play in the Southeast Asia.
2. Drive initiatives and events that bring together a community of stakeholders for knowledge exchange, communication, and strategy.
3. Drive the cybersecurity strategy for the Southeast Asia region.

The inaugural Southeast Asia Cybersecurity Consortium (SEA CC) Forum 2022 is an important event of the year, organised by the AiSP. The programme schedule comprises of key notes, discussions and sharing by the various South-East Asia country's cyber security associations on their cybersecurity programmes and initiatives on developing technical competence, innovation, talent development and spreading of cyber security knowledge amongst its citizens.

This event is organized for anyone with an interest or wish to find out more or understand more on the Cyber Security landscape and work with cyber security associations from Brunei, Cambodia, Indonesia, Malaysia, Myanmar, Thailand and Vietnam. We are expecting 150 attendees, subject to COVID restrictions, at this physical event. We will be inviting a Political Office Holder (POH) to be our distinguished Guest of Honour for the opening and witness the MOU signing between Brunei, Cambodia, Indonesia, Malaysia, Myanmar, Singapore, Thailand and Vietnam Cyber Security Associations.

All AiSP Academic Partners (APP) and AiSP Corporate Partners (CPP) are cordially invited to attend the event at Life Long Learning Institute on Wednesday, 23 November 2022 from 10.00am to 5.00pm which is complimentary.

Academia and Corporations who wish to participate at the SEA CC 2022 can contact Secretariat@aisp.sg to sign up as an Academic or Corporate partner, as well as for sponsorship opportunities.

23 Nov 22 – Day 1 (Open to All including AiSP members for 150pax)
Venue : Life long Learning institute, 11 Eunos Road 8 Level 1 Event Hall, Singapore 408601
Signing of MOU between the 8 Associations
Sharing by the 8 Associations
Key-Note Sharing

24 Nov 22 – Day 2 (Closed Door Discussion for 50pax)
Venue : 6 Raffles Boulevard, JustCo, Marina Square, #03-308, Singapore 039594

back to top

Participating Association

AiSP Association of Information Security Professionals

APTIKNAS Asosiasi Pengusaha TIK Nasional Indonesian ICT Business Association

ISAC-CAMBODIA CYBERSECURITY SHARING PLATFORM

ITPSS

MBOT LEMBAGA TEKNOLOGIS MALAYSIA MALAYSIA BOARD OF TECHNOLOGISTS

MiSA MYANMAR INFORMATION SECURITY ASSOCIATION

TISA

VNISA VIETNAM INFORMATION SECURITY ASSOCIATION

SME Cybersecurity Conference

SME CYBERSECURITY CONFERENCE 2022

30 November 2022 | 10AM - 3.30PM
NTUC Centre Auditorium, Level 7, One Marina Boulevard. Singapore 018989

Guest of Honour: Ms Yeo Wan Ling, Member of Parliament for Pasir Ris-Punggol GRC and NTUC U SME Director

Supporting Partners
CSCIS
CREST
CSA cloud security alliance
CzechTrade SINGAPORE
DivO
HTCIA
IASA
ISACA Singapore Chapter
(ISC)² Official Chapter
ntuc
Singapore Business Federation
SCS
SFA Singapore Fintech Association
AHK
SGTECH
SiAA
The Law Society of Singapore
Organised by
AiSP
Co-Organised by
Tech Talent AssemBly
U sme
Supporting Agency
CSA Singapore
Gold Sponsor
BLACKPANDA
Sponsors
FORTINET
GlobalSign by GMO
ONESECURE
softScheck
xcellink.pte.ltd.

back to top

Panel Discussion

Ready To Build A Secure Digital Business

Michael Lew
Panellist
Managing Director, Ankura
Chair, Cyber Risk Sub-Comm, SFA

Gene Yu
Panellist
Founder & CEO, Blackpanda

Garion Kong
Panellist
Member of TTAB Executive Committee
President, (ISC)2 Singapore Chapter

Tony Low
Moderator
AiSP Vice-President, CAAP Lead

Yeo Wan Ling
Panellist
Director of NTUC U SME and U Women and Family

Securing Your SME's Technology for the Threats of Today

Speaker

BLACKPANDA

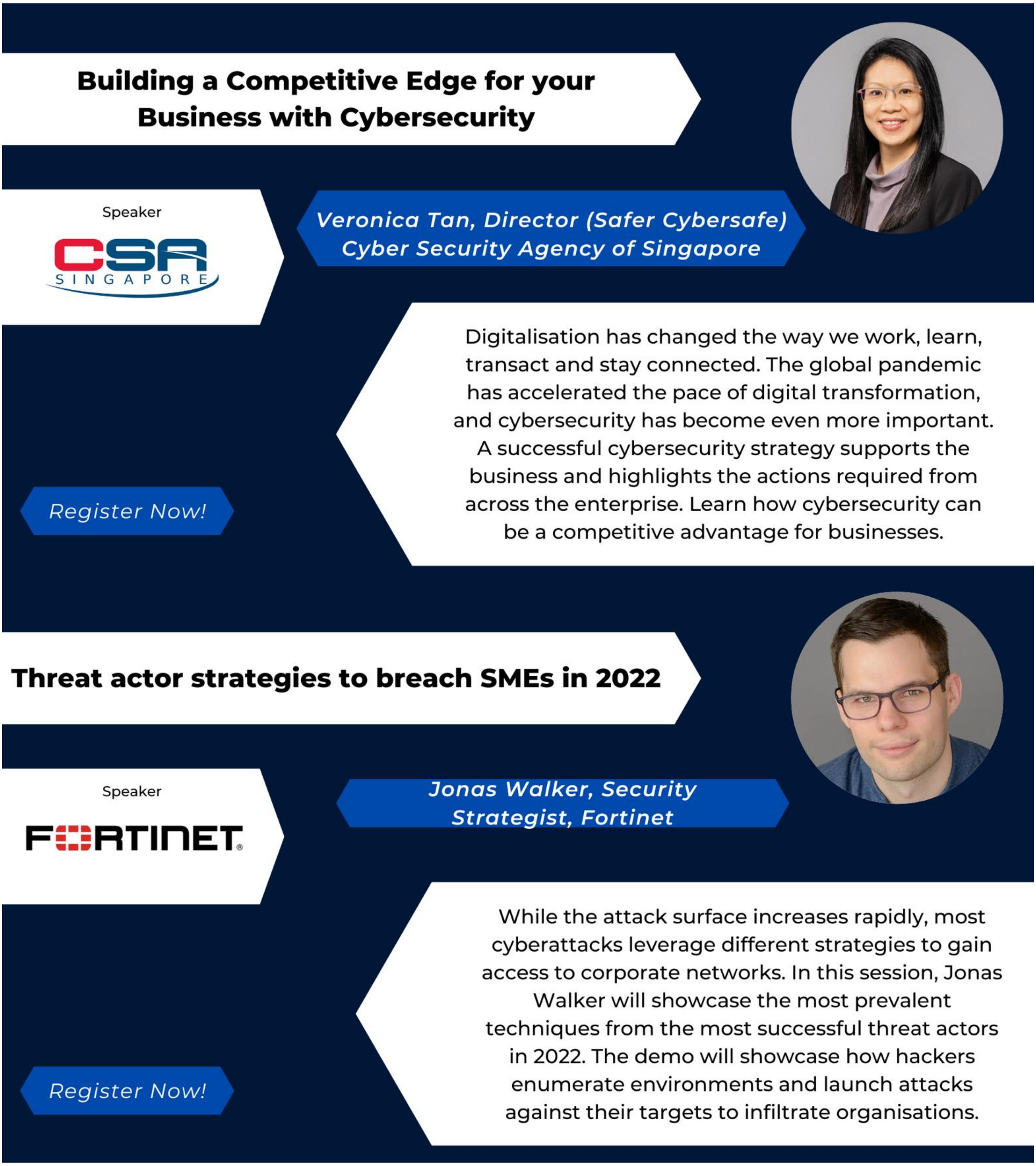
Gregor Vand, CTO, Blackpanda

Many SMEs mistakenly assume that cyber attackers are more interested in going after the big fish. As a matter of fact, 58% of all cyber attacks are targeted towards the smaller businesses. While good defences are available for those who stay aware of the potential dangers but SMEs often lack effective strategies for end-to-end cyber security to keep threat actors at bay.

With the rise of cyber attacks in today's digital age, businesses can only leap into the next phase of growth with their technology secured by understanding the threats they face and implement effective measures.

Register Now!

back to top



Building a Competitive Edge for your Business with Cybersecurity

Speaker

CSA SINGAPORE

Veronica Tan, Director (Safer Cybersafe)
Cyber Security Agency of Singapore

Digitalisation has changed the way we work, learn, transact and stay connected. The global pandemic has accelerated the pace of digital transformation, and cybersecurity has become even more important. A successful cybersecurity strategy supports the business and highlights the actions required from across the enterprise. Learn how cybersecurity can be a competitive advantage for businesses.

Register Now!

Threat actor strategies to breach SMEs in 2022

Speaker

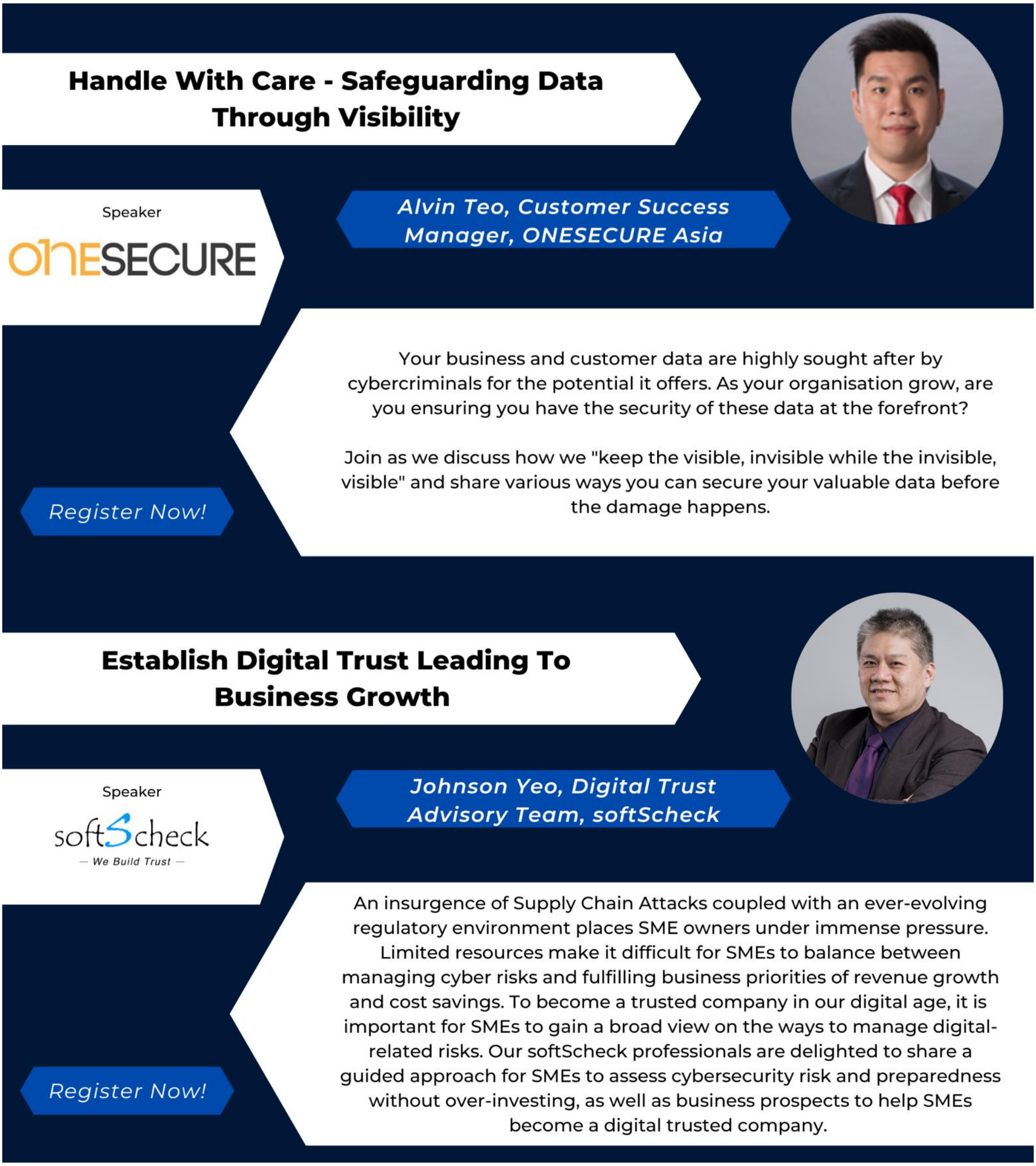
FORTINET

Jonas Walker, Security Strategist, Fortinet

While the attack surface increases rapidly, most cyberattacks leverage different strategies to gain access to corporate networks. In this session, Jonas Walker will showcase the most prevalent techniques from the most successful threat actors in 2022. The demo will showcase how hackers enumerate environments and launch attacks against their targets to infiltrate organisations.

Register Now!

back to top



Handle With Care - Safeguarding Data Through Visibility

Speaker

ONESECURE

Alvin Teo, Customer Success Manager, ONESECURE Asia

Your business and customer data are highly sought after by cybercriminals for the potential it offers. As your organisation grow, are you ensuring you have the security of these data at the forefront?

Join as we discuss how we "keep the visible, invisible while the invisible, visible" and share various ways you can secure your valuable data before the damage happens.

Register Now!

Establish Digital Trust Leading To Business Growth

Speaker

softScheck — We Build Trust —

Johnson Yeo, Digital Trust Advisory Team, softScheck

An insurgence of Supply Chain Attacks coupled with an ever-evolving regulatory environment places SME owners under immense pressure. Limited resources make it difficult for SMEs to balance between managing cyber risks and fulfilling business priorities of revenue growth and cost savings. To become a trusted company in our digital age, it is important for SMEs to gain a broad view on the ways to manage digital-related risks. Our softScheck professionals are delighted to share a guided approach for SMEs to assess cybersecurity risk and preparedness without over-investing, as well as business prospects to help SMEs become a digital trusted company.

Register Now!

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

back to top

associations, cybersecurity communities, and solutions provider.

Our theme for this year conference is "Ready to build a secure digital business".
Objectives of the conference include:
1. Understand the digital building blocks for a digital business
2. What are the pitfalls of getting onto digital
3. How to manage my remote workforce securely
4. Who should I turn to for help
5. What tools and people should I build up internally.

Date : 30 November 2022
Time : 10AM – 3.30PM
Venue : NTUC Centre Auditorium, Level 7, One Marina Boulevard. Singapore 018989
Guest of Honour: Ms Yeo Wan Ling, Member of Parliament for Pasir Ris-Punggol GRC and NTUC U SME Director

Register here now

Exclusive Benefit for AiSP from Blackpanda
IR-1
12-month Incident Response Solution for SMBs

Cyber attacks have catastrophic impact on SMBs. Did you know that **60%** of SMBs go out of business within six months of a data breach or a cyber attack? **43%** of these attacks are aimed at smaller businesses and **86%** are unable to defend themselves when an unfortunate event hit.

Be sure to have the fastest and effective cyber fire-fighters backing you up 24/7/365 upon a cyber attack.

- **24/7** incident Response Capabilities
- **1x** Incident Response Activation Credit
- **Preferred Rates** for Cyber Risk Services
- **Unlimited Access** to Cyber Risk e-Resources

For more information, please visit https://www.blackpanda.com/blackpanda-ir1.

Enjoy AiSP rate at **S$1500** (UP S$2100). Sign up here!

back to top

CREST

An update from CREST

CREST AGM & Future Plans

It was great to have an opportunity to engage with so many CREST members at our AGM in June. This provided a great platform for us to share a strategic update on our plans and aspirations for the next 24 months.

There is a significant focus on increasing our member benefits, and the AGM provided a great opportunity to share some of the plans we are working on to deliver additional value to members in all corners of the globe.

CREST OVS Programme

As most of you will recognise, cyber security never stands still. There are a huge number of initiatives and programmes we are working on to help shape and enhance the ecosystem. A significant amount of our discussions is focused on defining and raising standards across the key programmes we operate.

We are planning to release a series of new programmes throughout the next 12 months, and the first of these launched recently through the CREST OVS programme.

Read more about this initiative in consultation with OWASP –
https://www.crest-approved.org/membership/crest-ovs-programme/

Skilled Person Register

We hope these programmes will help buyers of cyber security services identify suitably skilled and competent organisations to engage with. As a result, you can expect further updates to our accreditation process and our Skilled Persons Register throughout the quarter ahead.

Read more here about how to register your employees -
https://www.crest-approved.org/membership/registering-your-skilled-professionals/

Updating Examinations

Examinations are a major focus for CREST, and several updates are taking place to certified level assessments.

We have listened to the feedback from recent exam takers, and we are using this insight to shape and enhance the exam experience. We hope to be able to communicate more tangible details about the planned changes this year.

International Events

back to top

It was great to see and meet many of you at recent events in the Middle East, Singapore, Malaysia, RSA and Infosec. We are delighted that so many people attended our recent CRESTCon; the CREST team was delighted to speak to you in person after so many months of virtual events and virtual meetings. We thank all our sponsors for helping to support CRESTCon.

CREST Communications

Make sure you follow us on LinkedIn and keep an eye out for some email-based member communications.

It is exciting times, and with your support and engagement, CREST hopes to materially enhance cyber security standards across large swathes of the cyber security landscape.

Rowland Johnson, CREST President

Keep up-to-date with CREST:
www.crest-approved.org
www.linkedin.com/company/crest-approved/

CYBER SECURITY ASIA 2022
Developing Cyber Resilience for a Future Ready Organization
15-16 August 2022 | Sheraton Imperial Hotel Kuala Lumpur
Panel Discussion | 16 August 2022
CRITICAL INFRASTRUCTURE SECURITY:
IS CHANGE OUR GREATEST ALLY OR JUST A PAINFUL EXERCISE?
Germaine Tan
Director of Analysis
DARKTRACE
Dr. Erdal Ozkaya
CISO
XCITIUM
Nivedita Newar
Head of Cyber Security
UNSW
Emil Tan
Regional Advocate
CREST ASIA
Brandon Tan
Director Sales Engineering
FORCEPOINT
Serene Gay
Senior Director
EVERBRIDGE

back to top

Upcoming Activities/Events

Ongoing Activities

Date	Event	Organiser
Jan – Dec	Call for Female Mentors (Ladies in Cyber)	AiSP
Jan – Dec	Call for Volunteers (AiSP Members, Student Volunteers)	AiSP

Upcoming Events

Date	Event	Organiser
1 Nov	AiSP x MBOT Ladies in Cyber Webinar	AiSP & Partner
1 Nov	AiSP x PA x TrendMicro Scam Awareness Event with MOS Sun Xueling	AiSP & Partner
2 Nov	NTU Scantist Student Networking Event	Partner
2-4 Nov	Singapore FinTech Festival	Partner
9 Nov	Learning Journey to Trend Micro	AiSP & Partner
9 Nov	School Talk by Trend Micro for ITE East	AiSP & Partner
9 Nov	School Talk by Trend Micro for IHLs	AiSP & Partner
9 to 10 Nov	CDIC @ BITEC Bangkok Thailand	Partner
11 Nov	The Cybersecurity Awards 2022 Gala Dinner	AiSP
13 Nov	DFL Event @ Marsiling-Yew Tee CC	AiSP & Partner
13 Nov	DFL Event @ Tampines	AiSP & Partner
15 Nov	Ladies in Cyber Learning Journey to Schneider Electric	AiSP & Partner
16 Nov	SVRP 2022 Awards Ceremony	AiSP
17 Nov	Knowledge Series – DevSecOps	AiSP
23 to 24 Nov	South East Asia Cybersecurity Consortium (SEACC)	AiSP
30 Nov	SME Cybersecurity Conference 2022	AiSP
2 Dec	TCA2022 Judges Appreciation	AiSP
9 Dec	CTI SIG Networking	AiSP
12 – 15 Dec	Learning Journey to KL	AiSP & Partner
17 Dec	DFL in the Community at Taman Jurong CC	AiSP & Partner
18 Dec	DFL in the Community at Whampoa CC	AiSP & Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

Importance of Clear Visibility through the cloud

Cloud Security, what does it mean to different folks? Security for the cloud, security in the cloud, we are told don't get locked down into one Cloud Service Provider (CSP), but if you have many CSP's how do you manage the security consistently ?
Important reminder – CSPs are responsible for the security **OF** the cloud, but the customer of CSP (i.e. you) are responsible for the security **IN** your cloud. The CSPs have security tools but it's your responsibility to make them integrate and work seamlessly. These tools are at various stages of maturity and often do not work together seamlessly to provide you a context based risk picture of your cloud.

Tam wrote a great article previously (cloud securing strategies) and I thought of trying to expand a little further starting with -Visibility. It's a huge topic as it touches on all pillars of cloud security - Platform, Identity, Data and Workload security - so let me attempt to start the journey by asking some pertinent questions.

How is visibility affected : how much attention cloud security has garnered in the board room allowing more budget ? or is it enough damage by threat actors that we sit up and feel something needs to be done ? or perhaps enough coverage of a new buzzword in recent conferences or by different cloud security related organisations ? how far can we see and is the data in the vision sufficient enough for us to act responsibly ?

There are many important aspects you need to think of:

- You need to see all the things in the cloud and their configurations
  - What maturity level are they at
- You need visibility deeper into not only what your Identities are but:
  - What their entitlements are (effective permissions)
  - What data / sensitive resources they can access (risk)
  - What are they doing with that access (actions / incident)'
- You need visibility into data:
  - Where is all of your data
  - What is your data
  - Who / what has access to your data
  - Who / what are they doing with that access (actions / incident)
- Vulnerabilities
  - What your traditional tools are missing
  - Why are they missing stuff

Is context important when providing visibility ?

back to top

Let's look at something simple;vulnerabilities on workloads. How often are these workloads used, do they stay around long enough (ephemeral) to be visible to your scanning tool ?

Once you have the list of vulnerabilities (it can be a very long list), will it make sense to have further impact analysis on whether there are other amplifiers eg: who can access this workload (identities including Non Person) , public or private access (platform risks)even if it crosses multiple CSP's , have the permissions been used recently (if not , are they needed) , are there roles which can hop through assuming other roles (privilege escalation)?

Is there an attached storage with sensitive data(data classification) , is it encrypted (integration with vaults)? Finally, during this process is any residual data left with your vendor , increasing your supply chain risk ?

Gaining visibility into each of the areas is extremely important , as only then we can help to break the kill chain and improve our security step by step.

We are only scratching the surface here but it's important to scratch with the right vector (direction and force). We cannot solve what we cannot see , so the view must be complete across the path. Data should be presented in a consistent, clear and digestible manner.

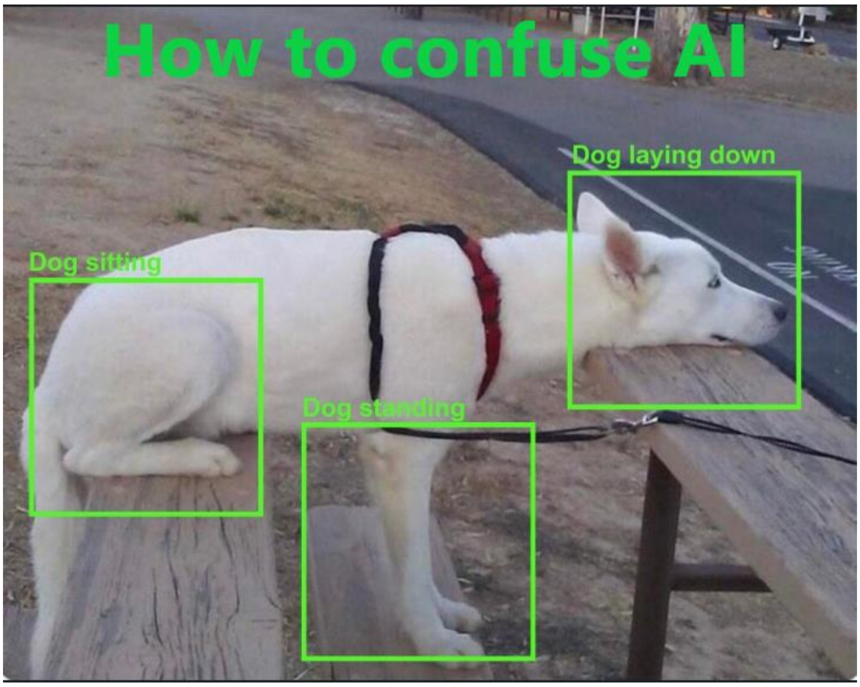
The environment must be continuously monitored and able to update itself with intelligent usable context, only then it can deliver a view that we can act on. We must then measure our progress to ensure we are making it more difficult for the threat actors.

Sukhdev Singh has an International & multicultural background across 24 years in Cyber Security. He has worked for a foreign public service , spoken at leading security conferences {RSA , HITB,IDC ,CII ID , VNCert, Govware} and was previously the X Force Spokesman for Asia Pacific. He has ACLP from IAL Singapore and is an experienced trainer across multiple security technologies and ISMS .His certifications include CISSP,CISM, CDPSE,CCSP,CEA. He currently leads the APJ business for Sonrai Security Inc. He volunteers in various capacities and is a SIG member of AISP

back to top

Article from Cyber Threat Intelligence SIG

Rantings of a Cyber Security Analyst



I recently saw someone post this and funny as it is, it does make sense. As a human, what would be your answer to this? How would you describe what is the dog doing?

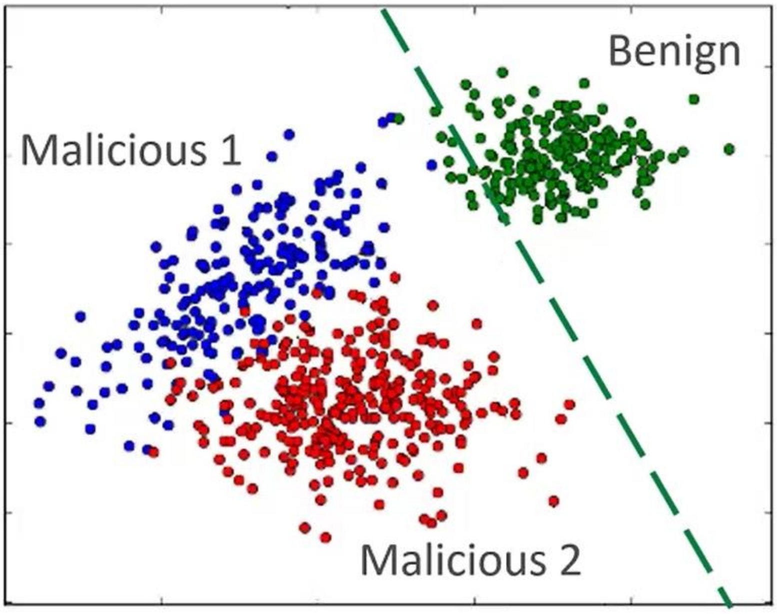
Till today, I still experience companies with misconceptions that Machine Learning solves ALL cyber security problems. I am not saying such technologies are useless; they do help a lot by doing pattern recognition and quick decision making based on known behaviours and other more time-consuming activities. In my opinion, Machine Learning is essential in today's threat landscape, but it does not completely eliminate threats. Look at all security vendors today and tell me which one does not use some form of Machine Learning? Look at the news and look at the companies that were reportedly breached. I am sure they use most of these vendors for their security.

As discussed in my previous write-up, cyber threats are growing because: -

- Businesses need to be online; more services are exposed on the internet.
- There will always be ways to exploit weakness on systems (vulnerabilities, human error, etc).
- Risk for cyber criminals is lower than physical crime (compared to physically breaking into a company).
- Unfortunately, cybercrime is profitable.

back to top

Machine learning requires some form modeling. By collecting samples and using algorithms to "train" the engines, security products can block new and unknown malicious threats.



However, like you and I in our daily lives, when we encounter issues, we will think of ways to overcome these difficulties to achieve our goals. Threat actors have a goal of breaching your environment. Just as we go about looking for solutions to overcome difficulties, so do threat actors.

Machine Learning cannot predict the future like a crystal ball. It is created by humans and needs to have "seen" examples of the data for reference. Threat actors know this and have ways to evade detections. In fact, threat actors also use Machine Learning, like automating the gathering of IT assets of the victim's environment.

I was asked about playbooks and felt there are misconceptions about them. Usually in Security Orchestration Automation & Response systems (SOAR), there are playbooks. Most come with pre-configured playbooks as recommendations. Playbooks are plans developed that outlines steps taken in the event of a security incident. They are not fixed and should be developed based on the needs and policies of the company. Questions like "please share your playbooks for comparison with another vendors'" does not make sense. They are guidelines and should be further developed by the organizations. If guidance is required, it should be a discussion between the company and security vendor to develop the playbooks that matches the policies and needs of the company. Unfortunately, SOAR with the playbooks can only automate responses which can be identified as true positive by the logics configured. As mentioned above, threat actors can and will use methods to evade or cause uncertainties which the automated solutions cannot make conclusive decisions. That is where alerting the security team comes in useful. The saying "It takes a thief to catch a thief" holds true.

back to top

For those interested in reading more about Machine Learning and AI, I recommend reading the articles by Alex Polyakov. His write-up on this topic is detailed and purely talks about AI concepts without the marketing fluff.
https://medium.com/towards-data-science/search?q=alex+polyakov

Harvey Goh is a cyber security specialist having been in the cyber security industry for over 15 years as technical personnel. Currently he is working as part of Sophos' Managed Threat Response team. He is also a member of AiSP CTI SIG, EXCO and volunteer at CSCIS CTI SIG.

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 Cloud Security Summit Sponsor, Cyber Security Agency of Singapore (CSA)

Securing the Cloud

As Singapore undergoes its Smart Nation initiative, we are increasingly adopting and embracing new technologies. Such technologies include 5G, Blockchain Technology, Artificial Intelligence and Quantum Computing. However, amidst the newfangled terminologies, we often forget the core of most of these new tech – that is none other than cloud computing.

For instance, 5G technology would most likely need a Central Cloud to form a backbone, whilst its fronthaul could use a real-time cloud for centralized processing. This is just one such example of cloud technologies being linked with many new and emerging technologies. Cloud computing offers cost savings, benefits from massive economies of scale, and allows increased speed and agility in deployment – all of which are crucial for deploying emerging technologies.

However, we cannot neglect the possible security risks of using cloud technologies. As we allow Cloud Service Providers (CSPs) to manage an increasing amount of infrastructure, we also expose ourselves to an increased attack surface. Access keys, for example, become another way for attackers to gain access to the cloud; the Capital One breach

back to top

is a clear example of that, whereby the attacker used stolen keys to steal the credentials of millions of customers.

While the benefits of cloud computing are numerous, there might also be certain challenges unique to cloud computing, spanning areas such as Security & Controls, Economics, and Geopolitics. From the domain of Security & Controls, some risks could include a lack of control over strategic data and operations, as they are managed by CSPs. From the domain of Geopolitics, we might be concerned about data sovereignty - where the data is stored, who has access to it, and whether there is a risk of foreign interference.

In short, as cloud computing becomes the dominant deployment choice for emerging technologies while on-premise servers take the backseat, we must also address the unique challenges we might face in cloud adoption. As time passes, securing the cloud will become increasingly important. After all, a chain is only as strong as its weakest link.

For any enquiries, please contact Mr Dennis Tay at Dennis_TAY@csa.gov.sg

Article from Cloud Security Summit Sponsor, ONESECURE

Being Proactive in Combating Phishing - Securing Stakeholders against Spoofing

The threat of phishing is ever-present today, with global trends observing that cybercriminals are increasing the use of spoofing to lure customers and employees to reveal sensitive information for threat actors to capitalise on. This is the case in Singapore as well - the annual Singapore Cyber Landscape report by the Cyber Security Agency of Singapore (CSA) noting that about 55,000 unique phishing URLs were hosted on Singapore infrastructure in 2021, a 17% increase over 2020's numbers.

A spate of phishing events caught the public's attention in 2021, particularly the high-profile scams involving OCBC bank where around 469 victims lost at least S$8.5 million after customers entered their credentials on fake bank websites. It was not just monetary gains that the threat actors were after. Sensitive and personal information were also targeted as social networking firms (e.g. Facebook, WhatsApp) and even the Ministry of Health (MOH) were spoofed taking advantage of the public's current interests such as a firm's privacy policy updates or COVID-19 news. Having a user's credentials allow for threat actors to act as the person, opening up access to the person's account and network - allowing for the installation of malware (in the case of organisation login details) or the amplification of phishing attempts.

back to top

These events prompted stakeholders in the Singapore landscape to act. The Singapore government and industry associations spearheaded a focus on the education of consumers on cybersecurity - a prominent example being the effort by the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) to include scam education alerts and quizzes upon customers logging in to their bank accounts online. While such efforts emphasise the shared responsibility of organisations and customers to protect against scams, ultimately the organisation has to lead in providing a safe environment for stakeholders to operate in.

Proactive steps taken by organisations to prevent phishing such as the standard to remove clickable links in correspondence with customers or having a system to scan for suspicious domains can go a long way to prevent attempts from reaching the end-user. Services such as **ONESECURE's Web Spoofing Detection** assists organisations to scan daily for active look-alike domains (a common method used by malicious actors to look legitimate) and monitor those domains for attempts to spoof the organisation (e.g. use of brand assets or change in website contents). A managed service takes the load off the organisation in scanning through thousands of domain permutations and the manual monitoring of suspicious websites. If a domain is noted to imitate the organisation, a takedown of the websites in question prevents the organisation's customers or employees from ever landing on those pages.

As long as phishing remains lucrative, the threats will not cease. It takes just one successful attempt for criminals to gain a foothold into stakeholders' accounts and networks. While education for consumers remains key, a proactive approach by organisations to close down on spoofing attempts ensures a safer environment for end-users. In this case, a strong prevention is better than working through a remediation.

About ONESECURE

ONESECURE is a cybersecurity company headquartered in Singapore, serving medium-to-large organisations regionally with a focus on value and an unwavering commitment for partners to have a complete and efficient security posture. The company provides a broad range of cybersecurity solutions for partners including: DDoS Protection, Security Operations Center (SOC), Security Information and Event Management (SIEM), Web Spoofing Detection, and Website Defacement Monitoring.

To find out more about ONESECURE and its services, do visit our website (onesecureasia.com) or get in touch with us via LinkedIn (ONESECURE Asia Pte Ltd). For questions, you may also email us at enquiries@onesecureasia.com.

back to top

Article from our Corporate Partner, Right-Hand Cybersecurity

How to Automate Your Cyber Awareness Program

Article contributed by Aaron Ang, Director of Education, Right-Hand Cybersecurity

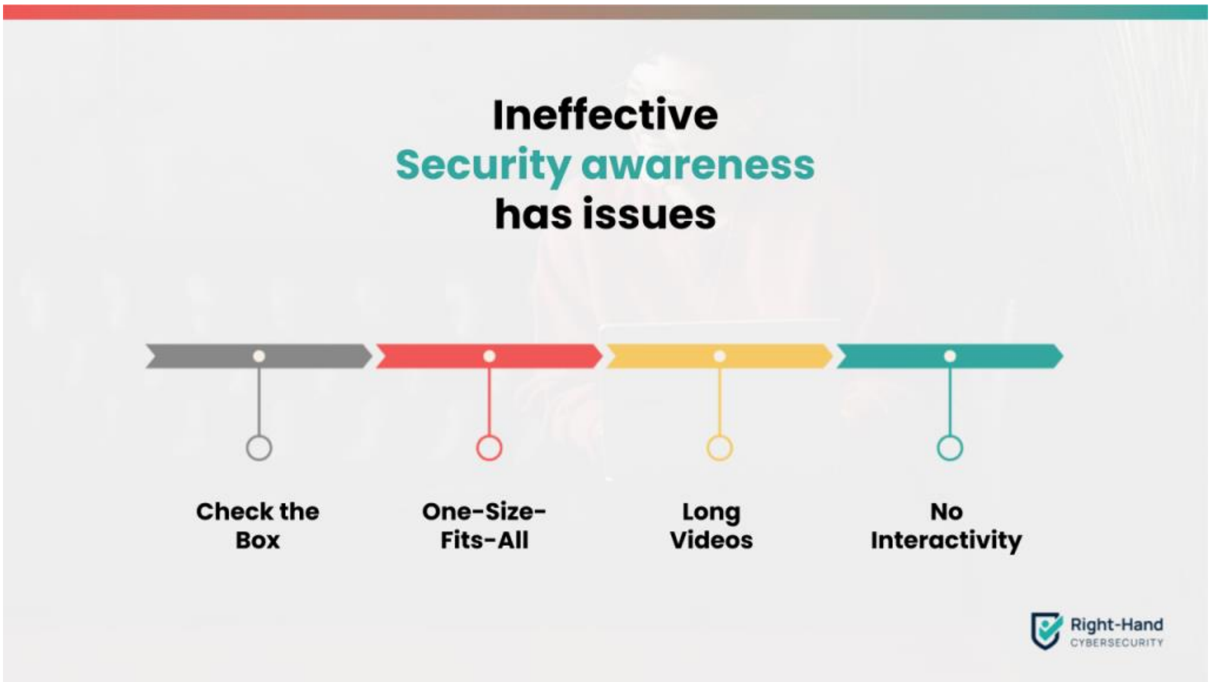
8 out of 10 cyber attacks start with a human being. That fact alone places Cyber Awareness in the center of cybersecurity discussions, not only in InfoSec departments but also in boardrooms.

However, it is easy to get Security Awareness programs wrong. Sometimes, it is a matter of limited budget, lack of knowledge of the full capability of a well-oiled program, lack of headcount to execute, or even the idea that Security awareness is just a compliance box to check.

In organizations where the importance of Cyber Awareness programs is acknowledged, the question is: how to optimize budgets and headcount and still create the security culture that improves organizational safety and resilience?

back to top

The problem: Ineffective Security Awareness



Current Security Awareness programs and solutions foster a one-size-fits-all culture. That means that all users are treated as if they were the same. And as we see in all successful learning apps (Duolingo, Elevate), users want to learn according to their schedules, lifestyles, and knowledge gaps.

So, treating everyone like they are in a production line, pretending your cybersecurity analyst has to go through the same phishing training content as your designer, is ineffective Security Awareness at play.
The one-size-fits-all spirit manifests itself in other aspects of training, such as

- **Format:** long, boring slides or videos that are often not updated for years and do not speak the language of your organization.
- **Lack of interactivity:** the users are passive spectators of the content, and interactivity is limited to a feedback form of a standard quiz that lacks knowledge of their vulnerabilities.
- **Check the box vibe:** training is measured in the presence and – best case scenario – whether the company was breached, but there's no apparent connection between user profiles and results.

And you'd think this "one-size-fits-all" mentality would make life easier for InfoSec teams. In reality, these solutions/programs take too much effort because they require manual labor to set up, onboard users, deploy training, and measure results.

back to top

The result? Ineffective Security awareness is **boring for employees and time-consuming for InfoSec teams**.

The Solution: Automated Cyber Awareness Programs

So, on the one hand, we have ineffective Security Awareness based on One-Size-Fits-All solutions, and on the other, we have the challenge of budget and headcount limitations that prevent InfoSec teams from creating more sophisticated, next-gen programs.

That's where automation comes to fill this gap.

Automated Cyber Awareness programs deliver four main benefits that turn Security Awareness from a box in cyber leaders' to-do lists into a resource that promotes real change and supports long-term behavior change and corporate security.

1. **Targeted training:** automation delivers the content each user needs. Each employee has a knowledge gap, a vulnerability that needs addressing. From an initial assessment and continuous reinforcement/validation, an automated Cyber Awareness program knows what users need to learn to fill these gaps. And training deployment happens individually without requiring InfoSec teams to set them up.
2. **Granular risk ratings:** automated training that knows users' vulnerabilities across different topics allows the creation of risk ratings for each one of them, for each user, for departments, branches, and the organization. This drill-down ability gives Cybersecurity leaders the power to mitigate human risk on all organizational levels and threat categories.
3. **Custom content:** training content that speaks the organization's language resonates with corporate culture and seamlessly integrates with the employees' routines has a much bigger success rate. Automation facilitates custom without stressing InfoSec teams with excessive labor.
4. **Simplified onboarding and deployment:** bringing users in and sending training campaigns when the programs focus on individuality may seem like a considerable effort, but automated cyber awareness is a significant help in that as well. SSO and other integrations eliminate the need for Infosec teams to do much more than just set up initial parameters.

How We Do It: Right-Hand's Ally Foundations

Our Cyber Awareness solution, Ally, provides organizations of all sizes and industries the ability to create this automated Security Awareness program through six core foundations.

back to top

Adaptive Learning

Like how an exercise app might assess your current health, Ally starts by learning about each user's current understanding of cybersecurity, digital safety, and the threat landscape. After establishing a benchmark, the system will operate autonomously and assign tailored content based on a user's knowledge gaps.

Mobility

Ally is compatible with any mobile or desktop device. It allows users to choose where they want to enjoy their learning experience, improving their chances of success in the Security Awareness program.

Real-World Scenarios

To drop the passive experience of slides and videos we described previously and to adapt to users' dynamic lifestyles, Ally delivers bite-sized scenarios and simulations based on real-life security experiences. The hands-on training will translate practice into long-lasting positive habits.

Gamification

Recognition, rewards, and competition are powerful learning drivers to drive motivation. Ally incorporates leaderboards to illustrate how users fare in comparison with their peers. That friendly competition pushes users to engage more with the content and retain the knowledge better. Badges and rewards are also a significant part of this mechanic, rewarding behavior and results.

Spaced Learning

The forgetting curve is real. Studies show that the degradation of knowledge is so deep that users remember roughly 20% of the training content after a month of learning. Spaced learning is built into Ally to automatically ensure users receive the training reinforcement they need when they need it the most.

Automation

With Ally, onboarding takes minutes. And once everything is ready, the ongoing training runs autonomously through a single pane of glass for admins and employees. With that, admins can pour more time into other critical security priorities and prevent employees from having significant distractions or deviation from their core job.

Interested to know more? Get in touch with Aaron at aaron.ang@right-hand.ai today!

back to top

About Aaron

Aaron is the Director of Education at Right-Hand Cybersecurity. He manages a team of cybersecurity content experts and developers in fulfilling the company's mission of making humans more defensible against cyber threats by helping clients build organizational cybersecurity culture.

Aaron holds the new Singapore Workforce Skills Qualification (WSQ) Advanced Certificate in Learning and Performance (ACLP), where he is certified to perform the role of a learning facilitator, assessor of SSG-funded certifiable courses, and also a learning solutionist to support the needs of enterprises and learners experiencing industry transformation.

In the early years of his cybersecurity career, Aaron was part of the Cyber Security Agency of Singapore (CSA), a government agency tasked with protecting Singapore's cyberspace. During his time at CSA, Aaron worked with veterans in the industry, both in the public and private sectors. Aaron is also passionate about helping to develop the next generation of cybersecurity leaders and has conducted cybersecurity training and workshops for many educational institutions and public agencies.

Aaron is a council member and the Chief Executive (Cyber Youth Collective) of Cyber Youth Singapore (CYS). CYS seeks to empower young Singaporeans to discover their passion for technology while providing them with opportunities to be innovative in giving back to the community.

Before his foray into cybersecurity, Aaron was an Education Officer at a local school before taking on an appointment as an Information Technology Consultant at the headquarters of the Ministry of Education, Singapore.

About Right-Hand Cybersecurity

Right-Hand was founded in 2019 by two Cybersecurity and EdTech experts and technology nerds, Theo Nasser and Uzair Ahmed.

During their time operating in the cybersecurity industry, Theo and Uzair observed clients from around the world invest millions of dollars in perimeter defense technology, but they were still becoming victims of data breaches. They realized what was missing – a technology platform that could help organizations shift their employee culture at the same rate as the evolving threat landscape.

Theo and Uzair have surrounded themselves with an incredible team, set of investors, advisors, and partners, and are working with clients across Asia-Pacific, North America, and Europe.
Right-Hand is a group of mission-oriented individuals driven to shift the power away from the adversary and back into the hands of businesses. And our journey has just begun!

back to top

Article from our Corporate Partner, Metasecurity

Log4j Vulnerability: Impacts on Network Security and How to Fix the Issue

A Log4j problem is a form of remote code execution vulnerability, a highly dangerous vulnerability that allows an attacker to install malware or ransomware on a target machine. The vulnerability was discovered in Log4j and can lead to the entire network penetration, the theft of critical information, and even the prospect of sabotage being carried out on the web.

The **log4j vulnerability** has been assigned the crucial rating and the maximum possible threat score **(10.0)** by the Common Vulnerability Scoring System **(CVSS),** the standard for quick evaluations of the severity of security flaws. This rating and score indicate that the vulnerability is extremely severe.

Summary of Log4j vulnerability

Log4j is a highly well-liked Java library that was first released in 2001 and is used by many programs to record activity and error messages. The principal method of attack involves sending messages to Log4j that tell the system to download and run malware from a remote site. This provides the attacker with additional access to the system of the victim.

Apache uses these descriptions to determine the severity of each vulnerability:

- **Critical:** 9.0 - 10.0
- **High:** 7.0 - 8.9
- **Moderate:** 4.0 - 6.9
- **Low:** 0.1 - 3.9

The most up-to-date, chronological list of Log4j CVEs is provided below:

CVE-2021-44228: The identity used to keep tabs on the first Log4j vulnerability.

CVE-2021-45046: Initial Log4j patch's tracking ID for a security flaw (version 2.15.0). Denial-of-service vulnerabilities in Apache 2.15.0 were discovered, as reported in the project's security warning. These vulnerabilities allowed attackers to create malicious input data using a JNDI query pattern.

CVE-2021-45105: The identifier used to keep tabs on the vulnerability fixed in Log4j 2.16.0's second patch, which, when exploited, may let attackers manipulate Thread Context Map data and trigger a denial of service via specially crafted string interpretation.

back to top

CVE-2021-44832: Name of the bug that affects all editions of Apache Log4j 2 (excluding 2.32 and 2.12.4). Due to this vulnerability, Remote Code Injection attacks are possible on all affected versions (RCE).

Log4j Impact on Network Security

The Log4j vulnerability may be exploited with minimal effort, but the repercussions can be devastating. For example, attackers might get access to networks and then sell that access to owners of ransomware programs.

The Log4j vulnerability can be exploited in other attacks to install Trojan malware, which can then trigger the install of an.exe file, which can, in turn, implement a crypto-miner or different types of malware on the targeted host to gain access to sensitive information and services.

Because Log4j is integrated into a wide variety of applications, Network Security, email services, cloud platforms, services, web applications, and enterprise software tools that are written in Java and used by organizations and individuals all over the world, the possible impact has the potential to affect millions of machines around the globe.

Attacks before the Log4j Fix was Released

Microsoft has updated the Log4j vulnerability advisory page on its website to include information on a ransomware operator (**DEV-0401**) headquartered in China. The operator is targeting systems that are accessible through the internet and spreading the **NightSky** malware.

According to the information provided, "Attackers started leveraging the **CVE-2021-44228** vulnerability in web computers running **VMware Horizon** as early as **January 4**." "**DEV-0401** has earlier deployed multiple ransomware households, including **AtomSilo**, **LockFile**, and **Rook**, and has likewise exploited web systems running combination of factors (**CVE-2021-26084**) and on-premises transfer servers (**CVE-2021-34473**)."

"**LockFile** is one of the ransomware families that **DEV-0401** has used in the past." According to the research conducted by Microsoft, it was found that the attackers were making use of command and control servers that forged legal domain names.

How to Fix the Log4j Vulnerability?

To make sure that your organizations and systems are protected from this dangerous vulnerability, implement the below steps;

Upgrade the Log4j Library to the latest version

Upgrading all instances of Log4j to the most recent version, which is now version 2.17.1, is the mitigating measure that is both the quickest and most effective at this time (download the latest Apache Log4j version here).

back to top

Log4j Vulnerability Scanner by UpGuard

The domain and IP scanner developed by UpGuard detects the CVE-2021-44228 affected entities automatically by sending a URL string 'HTTP GET request' to every IP address and domain.

A benign LDAP connection is established to confirm the Log4j library's vulnerabilities.

Update the System Properties of Java

Update Java system properties is a fix to the problem. If you cannot get the latest Log4j version, get in touch with the security teams to help you implement log4j2.formatMsgNoLookups and LOG4J_FORMAT_MSG_NO_LOOKUPS for versions 2.10 to 2.14.1.

Disable JNDI

This severe vulnerability is due mainly to an error in the **JNDI** Lookup plugin's architecture. It was recently uncovered that since its introduction in **2013**, the **JNDI** Lookup plugin allowed unparsed data to be passed to the Log4j library. This is why a single-string injection can trigger **CVE-2021-44228.**

Apache Log4j Questionnaire

Getting in touch with the vendors with the Apache Log4j Questionnaire will help the security team figure out all the affected systems with the vulnerability and devise the mitigating steps.

Multi-factor Authentication

Implementing multi-factor authentication and secure VPN policies can help you avoid vulnerability attacks. These VPN policies and authentication strategies make it almost impossible for the attacker to achieve network access through Log 4j vulnerability.

Update all Firewalls

Get all the latest Firewalls and update with the latest signatures and rules. Applying these patches will help stop the attackers from intruding on your privacy.

Huntress Vulnerability Tester

Using the Huntress scanning tool is a great way to keep an eye on the commonly used logging processes through APIs. It tells you if the data processing is affected by the Log4j vulnerability.
Download the Huntress Log4 Shell Vulnerability Tester source code here

Bottom Line

Log4j is a popular logging framework with several serious vulnerabilities. These vulnerabilities can be exploited to gain access to sensitive information or to perform denial of service attacks. While some workarounds can mitigate the risks posed by these vulnerabilities, the best solution is to follow the steps mentioned above.

For any enquiries, please contact Ms Tiffany Li at tiffanyli@metasec.one

back to top

Article from our Youth Symposium Sponsor, SIT

Competency-Based Education: A Novel Approach to Adult Learning

Ms Tammie Tham, Group Chief Executive Officer, Ensign InfoSecurity (left) and SIT President Prof Chua Kee Chaing (right) at the launch of the programme in 2021. (Photo: Singapore Institute of Technology)

At the Singapore Institute of Technology (SIT), a group of 14 adult learners taking classes in cyber security is also a test case of a progressive workplace learning model. The full-time employees from cybersecurity firm Ensign InfoSecurity are among the pioneers of a unique tie-up with SIT. The university is looking to pilot a curriculum centred around a competency-based learning approach.

By working closely with industry players, the programme upskills employees while acknowledging their competencies in the field. “We recognise their prior skills and knowledge and map them into university credits,” said **Associate Professor Goh Weihan** (left) from the Infocomm Technology cluster at SIT. He is part of the team that designed the programme.

Better yet, the programme avoids eating into learners’ personal time. “They study a few days and work a few days. We want to create a pathway that minimises disruptions to their work,” he added.

back to top

This differentiates it from most part-time degree programmes, where learners are usually not exempted from modules and have to attend classes and complete assignments on their own time.

In return, employers benefit from a highly skilled workforce capable of innovating their business to meet ever-evolving technological demands. Two full-time competency-based programmes in cybersecurity and land transportation, which adopt different approaches in delivering existing SIT degree programmes to various companies, were launched last year.

Carried out in partnership with Ensign, the competency-based programme in cybersecurity is fully sponsored by the company and enrolled employees are expected to remain with the company for the duration of the programme.

The competency-based pathway is a win-win strategy for employers and employees, said A/Prof Goh, as it bolsters companies' talent retention while allowing employees to fulfil their aspirations of owning a degree.

A Uniquely Designed Curriculum

SIT's Information and Communications Technology (ICT) (Information Security) undergraduate degree comprises 39 modules, including a capstone project, where learners are expected to engage in real-world computing and cybersecurity work.

While the competency-based programme with Ensign is based on this degree, it is also tailored to plug learners' skill or competency gaps rather than focus on relaying pure academic knowledge.

In the first eight months, learners study the fundamentals of computing full-time with SIT and are excused from work while receiving full pay. From the last trimester of Year 1 onwards, they spend two half-days a week at SIT and the rest of their time at work.

"We work closely with the company to ensure that the schedule suits everyone. The company has to be invested in the learning for us to provide the necessary support to the learners," said A/Prof Goh.
The programme does not require learners to take lessons for competencies they already know – a unique selling point of this pathway.

Drawing an analogy between competency-based learning and cooking, **Associate Professor Vivek Balachandran** (left), Programme Leader of SIT's ICT (Information Security), said: "If the module is on, say, the basics of cooking and the learner already knows how to marinate, he or she can choose to skip that lesson and move on to learning how to fry, for example."

back to top

He added: “This is a holistic approach in understanding what learners have done in their career and what certificates they have taken so that we can exempt them from certain assessments.”

If learners do not possess proof of such competencies, other methods are used to assess their knowledge. Some content, such as explaining various types of cyber attacks, is assessed via exams. Other content, like evaluating network security know-how, can be assessed only via hands-on practical work.

Under this provision, the learners from Ensign, whose experience in the field ranges from two to 16 years, can be exempted from up to four modules for a start. The number is set to rise as the university is looking to ramp up its competency-based assessment methods to allow learners to be exempted from more modules.

Key Learnings, One Year On

Scoping and selecting which undergraduate modules should be converted into competency-assessed modules has been a process of ongoing improvement for SIT and its partners.

For instance, the knowledge that deals with theoretical understanding is highly dependent on exam-based assessments and challenging to map to competency-based ones. But modules with hands-on assessments and skills-based exercises can be easily done so.

“The experience of running this programme for about a year now has given us the insights to assess and convert relevant modules as we move forward,” said A/Prof Balachandran.

One new thing SIT lecturers have implemented is a checklist of competencies to help them assess their learners in a structured manner. Learners may be expected to produce supporting documents to qualify for exemptions, such as an endorsement from companies they have worked with on projects requiring those skills.

So far, SIT has effectively adapted the ICT (IS) programme according to the needs of cybersecurity professionals at Ensign.

Ms Chiam Joo Ting, Threat Hunter, Managed Security Services, Ensign InfoSecurity, shares, “Lifelong learning is indispensable. Being on this programme allows me to keep learning and be updated with the latest knowledge and skills that I can apply in my career.”
While the learners may aspire to achieve a credential at the end of their studies, the university hopes that they recognise that being able to apply what they learn immediately remains the key benefit of competency-based education.

back to top

Article from our Youth Symposium Sponsor, ST Engineering

Levelling the battlefield with Cyber as an Asymmetric Leverage

Goh Eng Choon, President for Cyber, ST Engineering

From sabotaging, stealing and destroying valuable enterprise data to crippling critical information infrastructure as the precursor to a conventional war, cyber attacks are harbingers of chaos to both nations and businesses.

But the dynamics in cyber warfare are different. Classical military theory often calls for a numerical superiority ratio of 3:1 to win a battle with good probability and acceptable risks. In cyber warfare, this rule is overturned as smaller actors have an asymmetric advantage.

Small but deadly

While cyber attacks may not result in high human casualties or physical destruction, we have witnessed their devastating effects – disrupting lives and crippling everything from satellite communications to energy-generating wind turbines.
Take cyber espionage as an example. At the corporate level, companies have been caught stealing information in deliberate attempts to erode the competitive edge of their competitors. At the national level, top secret military intelligence and aviation technologies have been leaked.

In an increasingly digital world, the convergence of digital networks and systems has resulted in a global spike in cyber attacks. In 2021 alone, governments worldwide saw an

back to top

18.9-fold increase in ransomware attacks, while healthcare institutions faced a 7.6-fold increase in similar breaches[1].

The asymmetric nature of such attacks means that it only takes a small team of very talented people with the know-how to cause catastrophic disruption. Given their power to wreak massive economic and social damage, cyber attacks could well be the new weapons of mass destruction in this digital age.

The Invisible Enemy

The threat is ever present. Some cooperatives may be passive, biding their time to steal information, while others are destructive and have the capabilities to cripple the operations of countries and organisations.
Cyber warfare, unlike physical combat and gunfights, can also be hard to spot. Stealth attacks make detection a challenge as we fight without full visibility and situational awareness. A lot of times, it can be difficult to trace or understand the extensiveness of the threat or damage. By the time companies or countries intervene, it can sometimes be too late.

As more interconnected systems come under perpetual attacks, the lines between peacetime and wartime cybersecurity are increasingly blurred. With no formal declaration of war – not to mention the difficulties of identifying the adversary – it is hard for countries to determine their defence readiness condition (DEFCON) state and ascertain when a skirmish becomes a full-fledged war.

No organisation should be a sitting duck, reacting only when the damage is done. All should maintain a proactive stance to mitigate and respond to such attacks. While investing in cyber defence is increasingly a priority among big corporate entities, many small and medium-sized enterprises (SMEs) still regard cybersecurity measures as cost drivers and tend to put them on the backburner. No surprise, then, that SMEs are the top targets of cyber criminals – they are three times more likely to be attacked than their larger peers[2].

A United Front

Given the volatile nature of cyber threats, every individual, organisation and country is crucial to keeping the cyber ecosystem secure. Here are three key areas to look into:

First, it is important to inculcate good cyber hygiene as everyone plays a role in cybersecurity. Sharing ways to stay cyber safe helps sharpen vigilance and ensure best practices – from exercising caution in the sharing of sensitive information to using certified cybersecurity products to better protect data.

[1] https://www.sonicwall.com/2022-cyber-threat-report/
[2] https://www.barracuda.com/spearphishing-vol7

back to top

Second, an organisation-wide mindset change is needed. Leaders must not regard cybersecurity as an afterthought or implement measures merely as a response to government legislation. Instead, cybersecurity should be seen as an enabler by providing greater value to its consumers.

Third, cyber diplomacy should be fostered among countries and industries. In this highly interconnected digital world, we would collectively benefit by building closer ties and being more open to sharing information. Many attackers are already sharing information and if organisations work in silos, they will be on the losing end. It is therefore important to create a safe platform where organisations and nations can come together to share their experiences and expertise in combating cyber threats.

Arming to disarm threats

Protecting cyberspace should not just be the leaders' job. Instead, guarding against asymmetric cyber attacks is the responsibility of everyone in an organisation.
To begin, organisations should work within a cyber-secure network. For instance, in this era of increased remote working, sensitive data in transit and at rest should always be strongly encrypted from one end to another. This way, even if it falls into the wrong hands, hackers will not be able to make sense of the data as it will take them many years to decrypt the information.

Encrypted information in transit must also be secured. Critical networks should be segregated from other networks to create additional layers of defence. Connecting to workplaces and high-security clearance sites through virtual private networks is one way to achieve this segregation. For sites which require an even higher level of security, cross-domain solutions allow for highly secured unidirectional communication and isolated networks across sites.

Defending critical infrastructures from cyber attacks takes more than just antivirus software. Having an advanced cybersecurity operations centre to monitor these systems and networks will enhance the detection and response capabilities so that threats can be blocked and eliminated in a timely manner.
Ultimately, building cybersecurity capabilities in people is paramount to levelling up an organisation's capabilities. We need to shift our paradigm from passive defence to active defence and from reactive to predictive to be able to guard against and prevent attacks. Cyber defenders must start moving away from conventional task-based cybersecurity analysis to adopt a holistic, pre-emptive and proactive approach that is enabled by automation, cyber threat intelligence, and comprehensive threat awareness. This allows cybersecurity defenders to detect anomalies, anticipate hackers' moves, and provide actionable insights for C-Suites and analysts to make informed decisions to combat cyber attacks. At the end of the day, we need to secure what matters and people will still be the last line of defence to ensure a safe cyber future.

back to top

About the Author

Goh Eng Choon is the President of the Cyber business area at ST Engineering, a global technology, defence and engineering group with a diverse portfolio of businesses across the aerospace, smart city, defence and public security segments. He is also an appointed member of the Cybersecurity Advisory Group, a panel of eminent cybersecurity experts whose expertise may be tapped for cybersecurity issues or cyber threats that confront Singapore.

Eng Choon can be reached at our company website https://www.stengg.com/cybersecurity.

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

The content and information provided in the document do not constitute the opinions and views of the Association of Information Security Professionals. AiSP remains neutral to the products and/or services listed in the document.

back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

BECOME THE CYBER SECURITY LEADER OF TOMORROW

- Bachelor of Science in Cyber Security
- Master of Science in Cyber Security
- Graduation Certifications Programs
- Non-Degree (Short-term) Programs

ADMISSIONS OPEN 2023

Accepting Applications for January Term 2023

APPLY NOW

Hi, did you know ...

The Knowledge Review Magazine recognized EC-Council University in the annual listing of

"The 20 Most Valuable Online Colleges in America,"

Graduate and Undergraduate Programs in Cyber Security

EC-Council University is a premier institution of higher learning that specializes in cybersecurity technologies, enabling its graduates to obtain advanced cyber skillsets.

Our unique programs allow our graduates to lead their peers to strategically and effectively manage cybersecurity risks in their organizations.

Hi, did you know ...

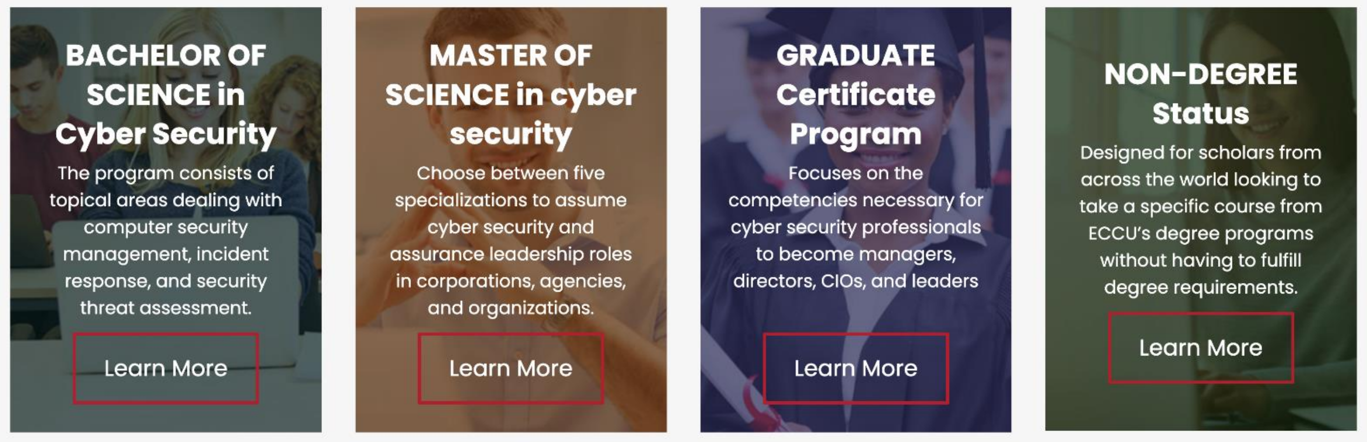
back to top

EC-Council University has been ranked in the **"The Top 45 Online Master's in Internet Security Degree Programs"** by Intelligent.com, highlighting our high standards of quality postsecondary education.

And...

Credit exemptions also applicable for relevant courses if you are holding EC-Council professional certifications like CEH, CND, CHFI, etc.

Come learn at ECCU. Your gateway to a great career in Cybersecurity!



BACHELOR OF SCIENCE in Cyber Security

The program consists of topical areas dealing with computer security management, incident response, and security threat assessment.

Learn More

MASTER OF SCIENCE in cyber security

Choose between five specializations to assume cyber security and assurance leadership roles in corporations, agencies, and organizations.

Learn More

GRADUATE Certificate Program

Focuses on the competencies necessary for cyber security professionals to become managers, directors, CIOs, and leaders

Learn More

NON-DEGREE Status

Designed for scholars from across the world looking to take a specific course from ECCU's degree programs without having to fulfill degree requirements.

Learn More

Special discount available for AiSP members, email aisp@wissen-intl.com for details!

Advertisements placed on the AiSP website is in no way intended as endorsements of the advertised products and services. No endorsement of any advertisement is intended or implied by AiSP.

Listing of Courses by ALC Council

alc
ADVANCE YOUR CYBER CAREER
with world-class certification training
CISM® • CRISC® • CISA® • CGEIT®
SABSA® • NIST® • CISSP® • CCSP®

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.

back to top

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

Advertisements placed on the AiSP website is in no way intended as endorsements of the advertised products and services. No endorsement of any advertisement is intended or implied by AiSP.

Qualified Information Security Professional (QISP®) Course

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP)
- 5 DAYS-
$840*
~~$2800~~
*70% funding for Singaporeans 40 and above.
50% funding for all Singaporeans below 40 & all PRs.
Call us: +65 8839 0071
Email us: training@opusit.com.sg
AiSP Advance Connect Excel
OPUS ACADEMY

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

back to top

COURSE DETAILS

2022 and 2023 Course dates can be found on https://www.aisp.sg/qisp_training.html
Time: 9am-6pm
Fees: $2,800 (before GST)*
**10% off for AiSP Members @ $2,520 (before GST)*
***Utap funding is available for NTUC Member**
*** SSG Funding is available!**

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***.

Program Partner

Transformists NETWORK

Delivery Partners

Ai Network 360

OPUS ACADEMY

NETASSIST

back to top

Cybersecurity Essentials Course

STEPPING UP ON INFORMATION SECURITY
AiSP Advance Connect Excel
CYBERSECURITY ESSENTIALS COURSE
SSG FUNDING IS AVAILABLE

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

back to top

- Cloud Computing
- Cybersecurity Operations

COURSE DETAILS

Training dates for year 2022 and 2023 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**
*** SSG Funding is available!**

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

Transformists NETWORK

Delivery Partners

Ai Network 360

OPUS ACADEMY

NETASSIST

back to top

MEMBERSHIP

AiSP Membership

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

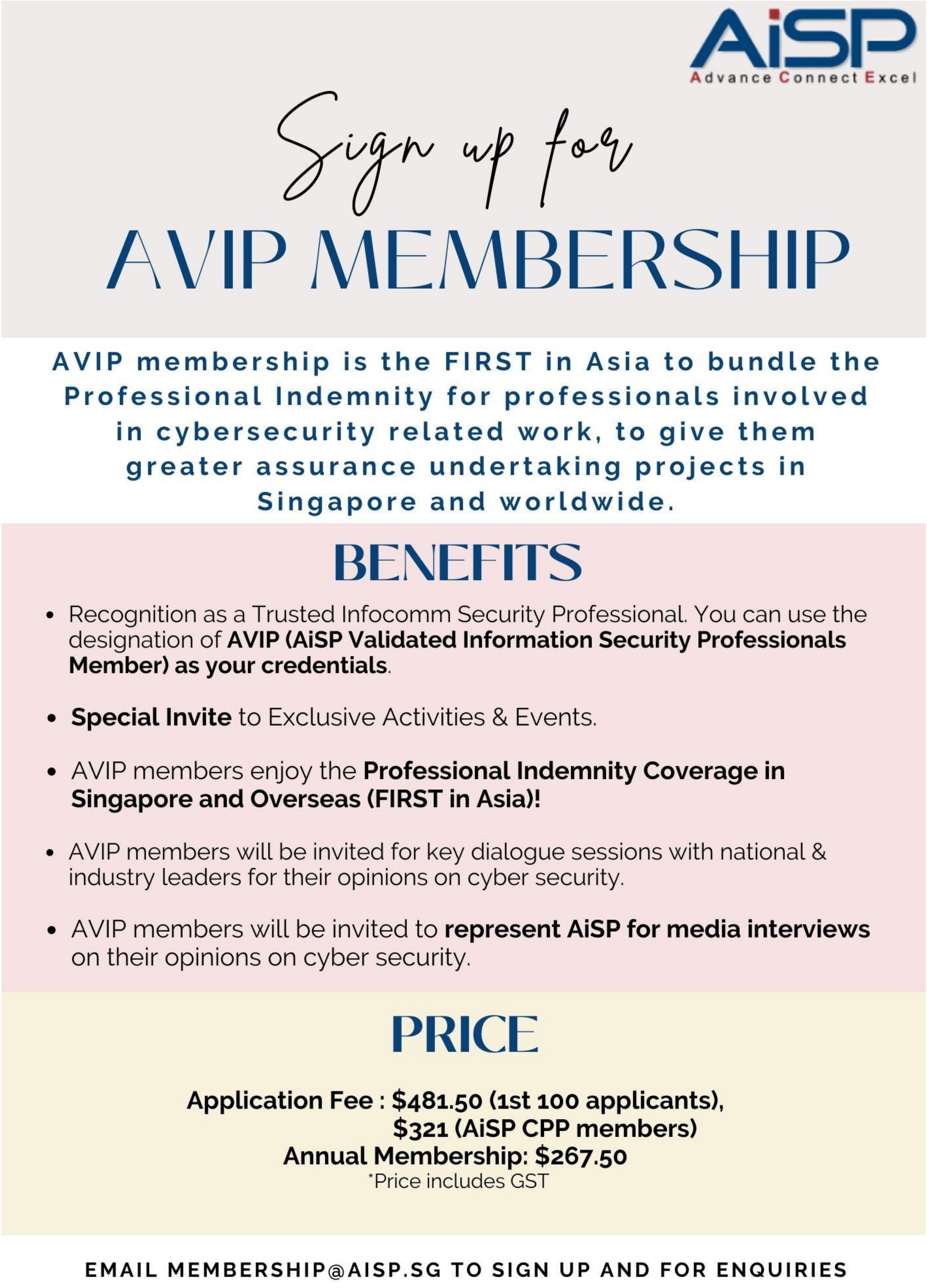
Complimentary Affiliate Membership for NTUC Members
AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2021 to 2022) from 1 Sept 2021 to 31 Dec 2022. The aim is for NTUC members to understand and know more about information security and Singapore's 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.

back to top



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

Application Fee : $481.50 (1st 100 applicants),
$321 (AiSP CPP members)
Annual Membership: $267.50
*Price includes GST

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

back to top

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

ABPGROUP
Acronis
AZ ASIA-PACIFIC
BCG
BD
BeyondTrust
BitCyber Securing Your Business
BLACKPANDA
Checkmarx
CISCO
CSA SINGAPORE
CSIT Centre for Strategic Infocomm Technologies
CYCOGNITO
CYFIRMA DECODING THREATS
DBS
elastic
ENSIGN INFOSECURITY
ExtraHop

back to top

FORTINET

GlobalSign by GMO

GOVTECH SINGAPORE

HUAWEI CLOUD
Grow with Intelligence

image engine

無限

INSIGHTZ TECHNOLOGY

IronNet

IT SEC ASIA

kaspersky

KROLL

Lookout

MANDIANT

METASECURITY

MICRO FOCUS

mimecast

YANG PERTAMA DAN UTAMA
MINDEF SINGAPORE

NETWITNESS
An RSA Business

NOZOMI NETWORKS

NUMEN

ONESECURE

RAJAH & TANN CYBERSECURITY

Recorded Future

Responsible Cyber

Right-Hand CYBERSECURITY

SAVIYNT

SCANTIST

SECURECRAFT

SecurID
An RSA Business

Singtel

STARHUB

ST Engineering

back to top

ThriveDX Formerly Cybint

TREND MICRO

VECTRA

wizlynx group

xcellink.pte.ltd. completing your technology chain

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

AiSP Academic Partners

ITE Institute of Technical Education

NYP NANYANG THE INNOVATIVE POLYTECHNIC

NGEE ANN POLYTECHNIC

NUS National University of Singapore

REPUBLIC POLYTECHNIC DISCOVER. TRANSFORM. ACHIEVE

SiT SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SMU SINGAPORE MANAGEMENT UNIVERSITY

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek POLYTECHNIC

back to top

Our Story…

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

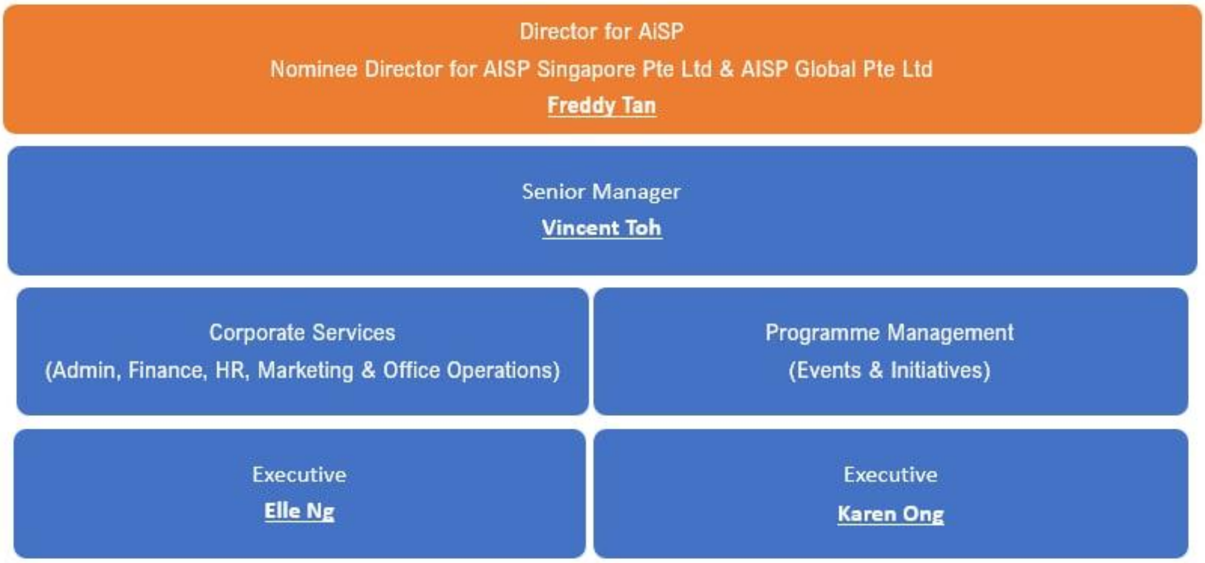
We believe that through promoting the development, increase and spread of cybersecurity knowledge, and any related subject, we help shape more resilient economies.

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

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

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

About Secretariat



Director for AiSP
Nominee Director for AISP Singapore Pte Ltd & AISP Global Pte Ltd
Freddy Tan

Senior Manager
Vincent Toh

Corporate Services
(Admin, Finance, HR, Marketing & Office Operations)

Programme Management
(Events & Initiatives)

Executive
Elle Ng

Executive
Karen Ong

AiSP
Advance Connect Excel

🌐 www.AiSP.sg
✉ secretariat@aisp.sg
☎ +65 8878 5686
📍 6 Raffles Boulevard, JustCo, Marina Square, #03-308,
Singapore 039594
Please email us for any enquiries.

back to top