

## News & Update

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

## Contributed Contents

- Cloud Security SIG: The Rising Concern of Data Privacy Around the World
- CTI SIG: Rantings of a Cyber Security Analyst
- The IT Pro's Guide to OT/IoT Security
- The Cybersecurity Awards 2021 Winner – Ng Hoo Ming

## Professional Development

## Membership

## NEWS & UPDATE

### New Partners

AiSP would like to welcome AZ and Scantist as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.



### Continued Collaboration

AiSP would like to thank Institute of Technical Education (ITE) for their continued support in developing the cybersecurity landscape:



**Institute of Technical Education**

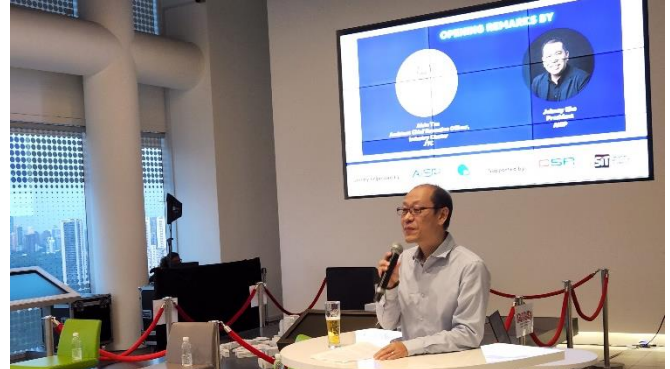
## News and Updates

### AiSP x CSA SG Cyber Leader x PDD Networking Event on 19 July

It was a great evening of networking and interaction at the AiSP x CSA SG Cyber Leader x PDD Networking Event on 19 July 2022 organised by AiSP and JTC.

More than 60 Cyber Leaders from AiSP Corporate Partners (CPP) came together and heard from our Speakers (Johnny Kho, Selwyn Scharnhorst, Steven Wong moderated by Sophia Ng) on the future of Cybersecurity in the region. Our leaders also had the opportunity to hear more on the plans of the Punggol Digital District through the networking.

AiSP would like to thank JTC for hosting us and Cyber Security Agency of Singapore - CSA and Singapore Institute of Technology for supporting the event and being part of the panel discussion.



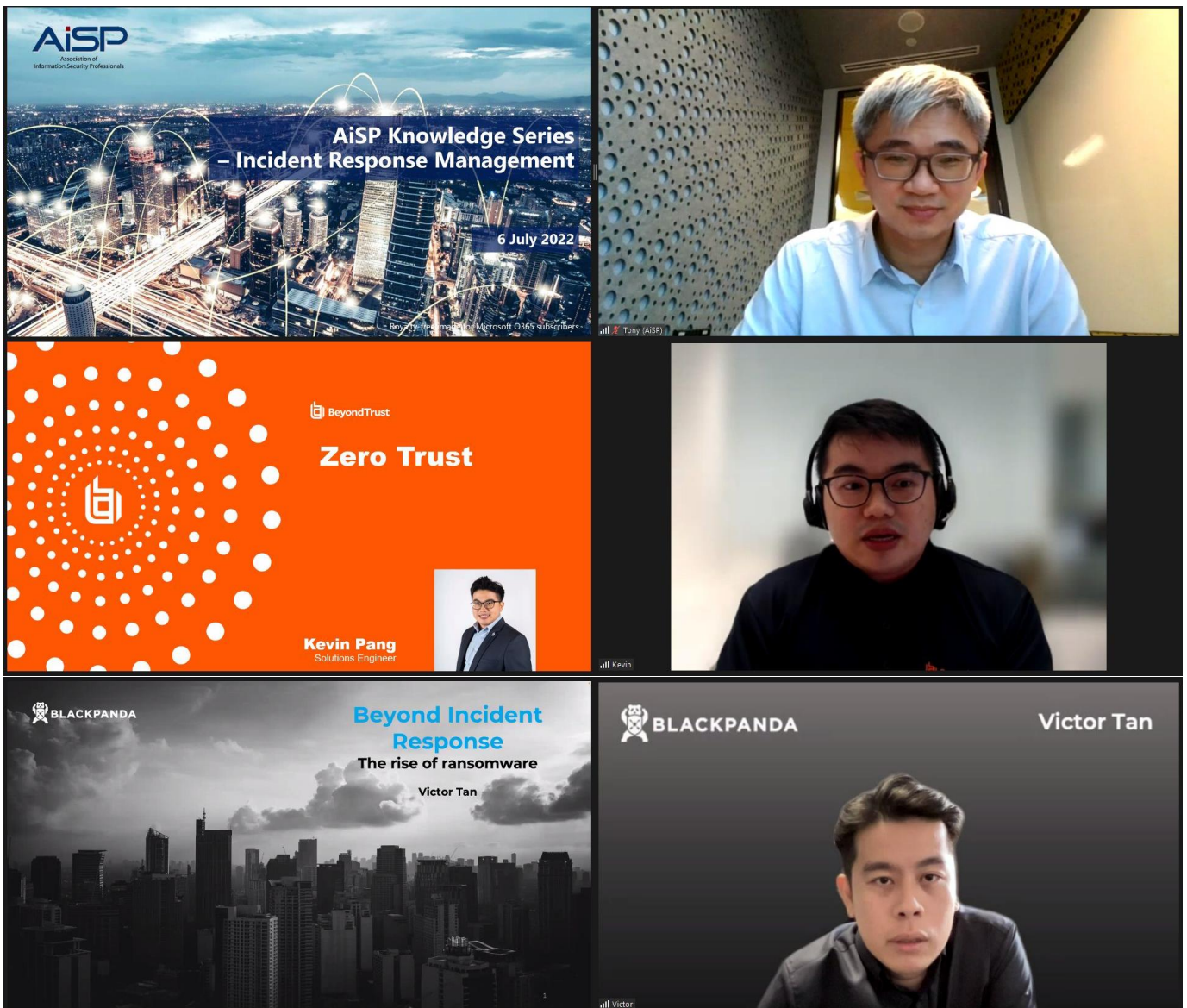
# Knowledge Series Events

## Incident Response Management on 6 July

As part of Digital for Life movement, AiSP is committed to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit.

On 6 July, AiSP was delighted to have our Corporate Partners, BeyondTrust & Blackpanda with us to support the event with the theme on Incident Response Management.

We would like to thank Mr Tony Low for giving the opening address and Mr Kevin Pang and Mr Victor Tan for sharing their insights at the webinar.





## Cyber Threat Intelligence on 20 July

As part of Digital for Life movement, we hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit.

On 20 July, we had our knowledge series focusing on Cyber Threat Intelligence where our Corporate Partner, IronNet & Micro Focus has shared insights on Cyber Threat Intelligence.



## Security Operation on 24 August



**AiSP Knowledge Series – Security Operations**

# AiSP Knowledge Series

## SECURITY OPERATIONS

24 Aug 2022 | Zoom | 3PM - 4.30PM



Haran Kumar  
Elastic  
Senior Solutions Architect



Sharat Nautiyal  
Vectra AI  
Security Architect

[REGISTER NOW →](#)



Organised by  
  
Supported by  
  
  
  
In support of  


In this Knowledge Series, we are excited to have Elastic and Vectra AI to share with us insights on Security Operations. 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.

**Security is a data challenge: Go beyond detections to continuous security monitoring with XDR**  
**Speaker:** Haran Kumar, Senior Solutions Architect, Elastic

A recent study, [Cybersecurity Solutions for Risker World](#), reveals how 1,200 organisations across 16 countries and 14 industries, with a combined cybersecurity spend of \$125.2 billion, are investing and expanding into advanced analytics with extended detection and response (XDR).

Modern SOC's need to address security as a data challenge, a risky landscape that has grown much more complex with the digital era. Join us in this session to learn about utilising a unified security ecosystem in addressing the threat landscape of unknown-unknowns through adoption of continuous security monitoring, and improved investigation and response times through security automations in SOC.

[back to top](#)

© 2008 – 2022 Association of Information Security Professionals. All rights reserved.

Page 5 of 45

Key takeaways include:

- The importance of continuous security monitoring and the need for data telemetries for limitless visibility.
- Evolution and adoption of extended and detection response (XDR) in modern SOC
- Adoption of dynamic analytics and automation to help detect today's and future attacks

**Enhance your Cyber and Cloud Security with Vectra AI**

**Speaker:** Sharat Nautiyal, Security Architect, Vectra AI

Supply chain attacks, ransomware, account compromises and data breaches are some of the many threats facing organisations today. And some can be nearly impossible to detect. Learn how with security-led AI, Vectra can identify threats and attacks before the damage is done. The sooner you identify a breach / attack the better you can protect your organisation.

Date: 24 August 2022, Wed

Time: 3PM – 4.30PM

Venue: Zoom

Registration: [https://us06web.zoom.us/webinar/register/6616589024995/WN\\_-uYWm8JZR8WDHHzh3p6hHw](https://us06web.zoom.us/webinar/register/6616589024995/WN_-uYWm8JZR8WDHHzh3p6hHw)

## Upcoming Knowledge Series

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its **Information Security Body of Knowledge 2.0** topics. Our scheduled topics for webinars in 2022 are as follows (*may be subjected to changes*),

1. Security Operation BOK Series, 24 Aug 22
2. Internet of Things BOK Series, 19 Oct 22
3. DevSecOps BOK Series, 16 Nov 22

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

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

# Cybersecurity Awareness & Advisory Programme (CAAP)

## Staying Cyber Safe with Cyber Trust & Cyber Essentials on 28 July

On 28 July, in collaboration with SCCCI, AiSP organised a webinar on Staying Cyber Safe with Cyber Trust & Cyber Essential.

We would like to thank Tony Low for giving the opening address and the following speakers for sharing insights with the participants: Ms Veronica Tan (Cyber Security Agency of Singapore (CSA)), Mr Balijit Singh (GIC), Mr Dave Gurbani (CyberSafe), Mr Kamal (TÜV SÜD) and Ms Alice (BSI).



## AiSP x SIAA - Automation, Robotics & IoT Security Workshop on 25 August




### AiSP x SIAA - Automation, Robotics & IoT Security Workshop

**REGISTER NOW!**

**AiSP x SIAA**  
Automation, Robotics & IoT Security Workshop

**THURSDAY**  
25 August, 2022

Organised by:






Speaker:  
**AFWAAN SIRAJ**  
Technical Solution Architect  
Cisco



Speaker:  
**JONATHAN CHIN**  
Business Development Manager, OT Cybersecurity  
Fortinet



Speaker:  
**DAREN TAY**  
Regional Technical Manager  
Nozomi Networks Asia Pacific

Supported by:






AiSP will be organising a Cybersecurity Awareness & Advisory Programme (CAAP) physical workshop together with the Singapore Industrial Automation Association (SIAA) to provide SIAA members knowledge on what solutions are available for securing their solutions in the area of Robotics, Automation and IoT.

This event aims to elevate cybersecurity awareness for SIAA members as an integral part of Singapore business fundamentals and establish a self-sustainable support ecosystem where businesses can raise their cyber resilience with the support of agencies, business associations, security communities and service providers.

**IT /OT convergence for Security in Enterprises**  
**Speaker:** Afwaan Siraj, Technical Solution Architect, Cisco

Focus on network security in industrial IoT. Understand the difference between IT Security and OT Security and how Cisco helps the enterprises to secure their networks in industrial environment.

**Building a Cyber Fortress for IoT**  
**Speaker:** Jonathan Chin, Business Development Manager, OT Cybersecurity, Fortinet



Businesses are expected to spend over \$1 trillion on Internet-of-Things (IoT) projects in 2023. To reap the potential benefits of IoT, businesses rely on an entire ecosystem of vendors and solutions to cover everything from the IoT devices' hardware and software, to connectivity, data storage and analysis, and more. This makes IoT a complex ecosystem that is difficult to realize, maintain, and manage.

In this session, learn how you can adopt an integrated IoT strategy to protect against threats that target IoT ecosystem and still be empowered to deliver on the promise of IoT.

**Connecting the dots in OT Cybersecurity**

**Speaker: Daren Tay, Regional Technical Manager, Nozomi Networks Asia Pacific**

Connecting IT and OT can sometimes be challenging, but both teams know the importance of Cybersecurity. Join our session to find out why visibility is fundamentally imperative in addressing today's critical infrastructure and industrial networks cybersecurity challenges over safety concerns.



Date: 25 August, Thursday

Time: 2PM – 5PM

Venue: Singapore Industrial Automation Association

Registration: <https://forms.gle/LKhRQaNJtG6dT6Yx7>

## AiSP Cybersecurity Awareness E-Learning

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

### 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](mailto:secretariat@aisp.sg) if you have any queries.

### SME Cybersafe provides



Enhanced Security  
Awareness & Training



Cohesive Security  
& Knowledge Resources



Security Solutions &  
Services Support

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

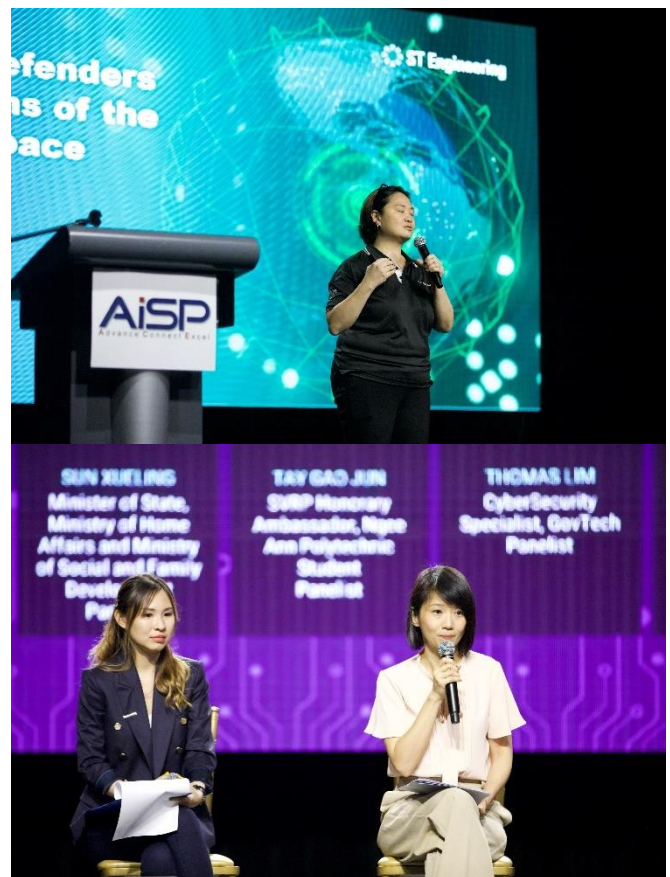
# Student Volunteer Recognition Programme (SVRP)

## AiSP Youth Symposium on 2 July

On 2 July, as part of Youth Day Celebrations, AiSP organised the inaugural AiSP Youth Symposium with various talks from company representatives. MOS Sun Xueling was the Guest of Honour for the event.

During the event, there was a panel discussion on our Youth in the Future moderated by AiSP EXCO member & SVRP lead Soffenny Yap, joined by MOS Sun Xueling, SVRP Honorary Ambassador Tay Gao Jun, GovTech Singapore Thomas Lim, Singapore Institute of Technology Raymond Chan and ST Engineering Cybersecurity Woo Lip Lim. It was an engaging and insightful session for the youths as they shared their perspectives from different walks of life.

A big thank you to our sponsors & supporting partners for making the event possible: Cyber Security Agency of Singapore (CSA), DBS Bank, GovTech Singapore, Huawei Singapore, IMDA Digital for Life Movement, National Trades Union Congress (NTUC) U Associate, Singapore Institute of Technology & ST Engineering Cybersecurity.







## Learning Journey to Singtel office on 4 July

As part of Youth Day Celebration, AiSP brought over 60 ITE West students to tour our Corporate Partner, Singtel office. They had the opportunity to visit the backend operations of Singtel and find out more about what each job entails. Thank you AiSP CPP, Fortinet for sponsoring the lunch for the students.



## Learning Journey to Acronis on 12 July

On 12 July, AiSP brought over 30 ITE West students on a learning journey to visit our corporate partner, Acronis office. It was an insightful day for the students as they get to ask first hand questions on the daily work of cybersecurity personnel.



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. Call for Nomination for Student Volunteer Recognition Programme has ended on 31 July 2022.

# AiSP Cyber Wellness Programme

Organised by:



Supported by:



In Support of:



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

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



---



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



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



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



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



**Want to know more about Information Security? Scan here for 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](mailto:secretariat@aisp.sg) to find out more on how you can be involved or if you have any queries.

Click [here](#) to find out more!



# Ladies in Cybersecurity



## Ladies Talk Cyber Series

For the Fourteenth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Su Mon Kywe, who is currently working as a security manager at the National Health Group (NHG).

### 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

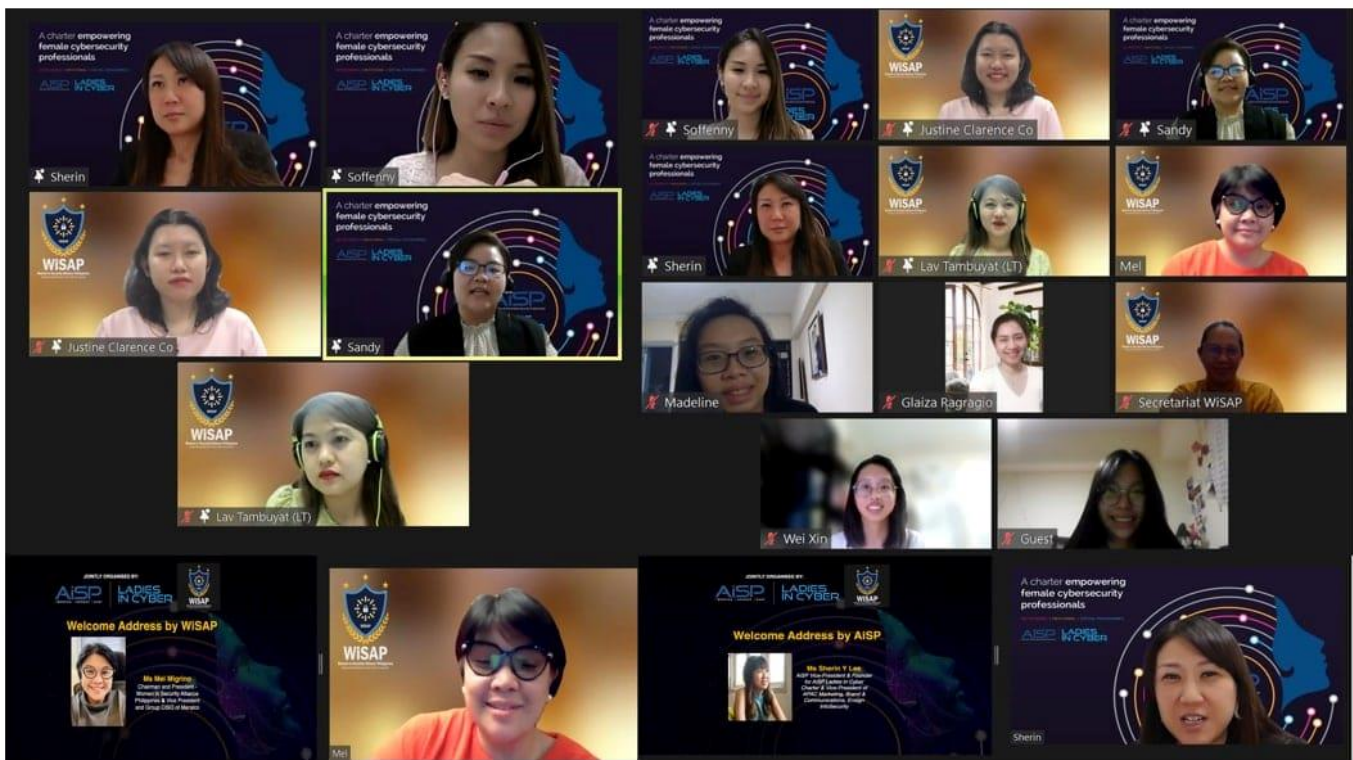
Su Mon is currently working as a security manager at the National Health Group (NHG). She liaised with cluster information security officers (CISOs) from hospitals, polyclinics, and pharmacies for various security initiatives, such as technical risk advisory, risk assessment, and application security training.

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



**AiSP x WiSAP Spill the Tea Webinar on 14 July**

AiSP held our first joint event with WiSAP (Women in Security Alliance Philippines) on 14 July with an evening of sharing at the AiSP x WiSAP Spill the Tea Session. It was our pleasure to have our panellists Ms Justine Co, Ms Sherin Y Lee, Ms Lav Tambuyat and Ms Sandy Cheong moderated by Ms Soffenny Yap. The panel shared on their personal experience in their daily jobs and how they are coping between their career and personal life. They also shared on what motivated them to stay in this industry and what are some of their biggest setbacks that they faced in their journey as well as what they hoped to achieve in the future.





## Upcoming Ladies in Cyber Events

### AiSP International Cyber Women's Day Celebration on 1 Sept

International Women in Cyber Day is a global movement of women and male advocates who recognize September 1st as a special day set aside to bring awareness to the challenges women face and celebrate women's achievements within the cybersecurity industry.

This year, AiSP will be doing a sharing on our past achievements and updates on our new programme. We will end the event with a networking and drinks (Free Flow of Beer & Red Wine). It will also be a night of networking and recruitment where every AiSP Female mentors can bring a female friend to join in the event too to know more about our programme.



JOINTLY ORGANISED BY:



Open to all Females only.

Please email to [secretariat@aisp.sg](mailto:secretariat@aisp.sg) if you are interested to join.

## Learning Journey to Ensign InfoSecurity on 6 Sept

As part of the International Cyber Women Day Celebrations 2022, AiSP will be organising a learning journey to Ensign InfoSecurity on 6 Sep 22 from 2pm to 5pm where we will invite about 50 to 70 female Youths (Subjected to COVID restrictions) from our Student Chapters to come together physically for a day of celebration, learning journey and visiting the Ops Centre at Ensign InfoSecurity and interacting with the working personnel at Ensign. Join us for an afternoon of enriching activities ranging from Dialogue Session with our Guest of Honour, Ms Gan Siow Huang, Minister of State in the Ministry of Education and Ministry of Manpower, Recruitment Talk, Internship Opportunities and visit to the Ops Centre. The event is open to all female students in tertiary level. Join MOS Gan, Ms cAsh Chng, Ministry CISO and Ms Sherin Y Lee at the event to hear what they have to share.

The details for the event are as follow:

Date: 6 Sep 22 (Tue)

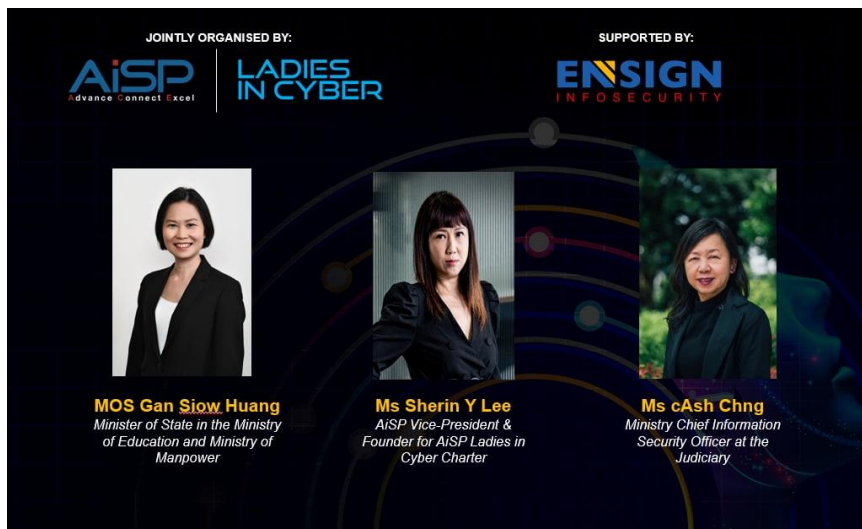
Time: 2pm to 5pm

Venue: Ensign InfoSecurity (Singapore) Pte Ltd located at 30A Kallang Pl, #08-01, Singapore 339213

Dress code: Smart Casual

Guest of Honour: Ms Gan Siow Huang, Minister of State in the Ministry of Education and Ministry of Manpower

\*Light Refreshments will be provided at the event



Open to Female students only. Register [here](#) by 12 Aug 22 or scan the QR code below.



## 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](mailto:secretariat@aisp.sg)



# The Cybersecurity Awards



**Thank you for all your nominations  
TCA 2022 Call for Nominations has ended on 1 July.**

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



Organised by



Supported by



Supporting Associations



Community Partner



Supporting Organisation



Platinum Sponsors



Gold Sponsors



Silver Sponsors



Visit [www.thecybersecurityawards.sg](http://www.thecybersecurityawards.sg) for more information.



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

Professionals

1. Hall of Fame
2. Leader
3. Professional

Enterprises

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

Students

4. Students

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

## Digital for Life

### Skills for Good Festival 2022 at Toa Payoh Hub on 23 – 24 July

As part of Digital for Life movement, we hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 23 and 24 July, AiSP and our Corporate Partner – Acronis were at Toa Payoh HDB Hub for the Skills For Good Festival 2022. Acronis provided free onsite installation of Cyber Protection software on mobile phones. On 23 July, AiSP Vice- President Sherin Y Lee & Co-Lead for Cyber Wellness Faith Chng shared on the different Cybersecurity Career and their journey in Cyber for Women. AiSP Vice- President Tony Low was present on 24 July as he shared on the importance of Cybersecurity Awareness and Advisory Programme (CAAP).

The event was a great platform to gain insights on industry trends and jobs in Singapore's key growth areas – the Digital, Green and Care economies - and pick up skills for the good of self, for community and for life.





## CREST

### An update from CREST

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

#### An evolved identity

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

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

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

## **Exam updates in 2022**

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

## **Improved pathways into CREST**

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

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

## **Evolving accreditation process**

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

## **A consistent international governance structure**

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

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



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

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

Visit our website for further news and updates: [www.crest-approved.org](http://www.crest-approved.org)

## Upcoming Activities/Events

### Ongoing Activities

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

### Upcoming Events

Date	Event	Organiser
4 Aug	LawSoc Cybersecurity Conference	AiSP & Partner
15 Aug	School Talk at Victoria School	AiSP & Partner
22 Aug	AiSP x CSA Joint Event with AVIP Members with CE CSA	AiSP & Partner
24 Aug	<u>Knowledge Series – Security Operations</u>	AiSP & Partner
25 Aug	IASA BITAS Conference 2022	Partner
25 Aug	<u>AiSP x SIAA - Automation, Robotics &amp; IoT Security Workshop</u>	AiSP & Partner
29 Aug – 1 Sept	Virtual AppSec APAC 2022	Partner
30 Aug	Learning Journey for Anderson Secondary to Cisco	AiSP & Partner
30 Aug	<u>Making Zero Trust A Reality</u>	Partner
31 Aug	Cybersecurity Innovation Day 2022 by CSA	Partner
1 Sept	AiSP International Cyber Women's Day Celebrations 2022	AiSP
6 Sept	<u>AiSP Ladies in Cyber Learning Journey to Ensign</u>	AiSP & Partner
6 Sept	PDD Connect Smartness Event	Partner
6- 7 Sept	Identity Week Asia	Partner
13 Sept	Cyber Leaders Series	AiSP
13 – 14 Sept	SMEICC Conference Series	Partner
14 Sept	Identity & Access Management BOK Series	AiSP

[back to top](#)



15 Sept	GTACS 2022	Partner
26 Sept	Cloud Security Summit	AiSP

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

# CONTRIBUTED CONTENTS

## Article from Data & Privacy SIG

### The Rising Concern of Data Privacy Around the World

For a long time, organisations large and small have been collecting data from their customers without their complete knowledge and consent. Since the true purpose of such data collection is kept hidden from consumers and tucked deep inside the terms and conditions, many consumers click the “agree to terms and conditions” check box without understanding its impact. They have handed over so much of their information to companies without even realising it.

User data has a huge market value, resulting in companies pooling and selling the personal data of individuals on a large scale. Websites all over the world collect and store this data in many forms:

- Personal data, including an individual's name, gender, IP address, and location
- Engagement data, such as text messages, emails, mobile apps, and social media pages
- Behavioral data, in the likes of purchase history, visits to certain areas and product usage information
- Behavioral data metrics, as in consumer satisfaction, purchase criteria, and product desirability

Global tech giants have been found to keep more information about users than what they require, and they often claim to use this data to personalise content and improve the user experience. However, the fact is that these companies sell this data to advertisers, publishers, and other third parties.

For instance, ad performance with respect to a particular user is shared with advertisers, who then customise their ads based on the user's behavior to hyper-target them for conversion. Users' location information is also commonly shared and used to display personalised local ads. In response, many data subject request have made attempts to erase their digital footprints and secure their personal information that's available online because of privacy concerns.

Typically, data refers distinct pieces of information, usually formatted and stored in a way that is concordant with a specific purpose whereas data privacy refers to protecting data in terms of data collection, use, and disclosure.

The aim is to secure multiple types of data, like first-party data (information that brands and creators collect directly from their consumers), second-party data (information acquired from the company that collected it), and third-party data (information purchased from other sources, ideally including data from different sources aggregated in one place).

As consumers become more knowledgeable about their data rights and how their data is used, they will demand that it be protected and secured. An increasing number of consumers have expressed concerns about the way their personal information is used by companies. With rising concern from the general population over the misuse and abuse of data, there is a need for global data regulations that focus on strengthening consumer privacy and data protection.

Over the last few years, data misuse has extended far beyond creepy advertisements that target individual customers. The increased focus on privacy concerns is driven by the numerous cybersecurity attacks that have led to massive breaches of personal data. Data breaches cost organisations time, money and more importantly, reputation. This loss happens in the form of data loss, which can be compensated to some extent, and through irreversible damage to their reputation, which eventually leads to the loss of customers. Customer loyalty is almost impossible to regain.

The global rise in ransomware attacks is a major source of concern for businesses. According to Security Brief Asia, 65% of Singapore organisations were hit by ransomware attacks in 2021, more than twice the number from the previous year (25%). 64% of attacks resulted in data being encrypted, a considerable increase from the 49% that was reported by respondents in Singapore in 2020<sup>1</sup>. Organisations in Singapore that are hit by a ransomware attack are paying an average of around S\$1.5 million.<sup>2</sup>

Thus, many governments are starting to regulate data collection and management by companies. With privacy being declared a fundamental right by the United Nations Universal Declaration of Human Rights, there is an immediate obligation to preserve privacy rights.

### **Data Privacy Regulations: The Impact on Business**

Data privacy regulations enable businesses to optimise their data handling practices and ease cross border digital transactions. However, they require businesses to strengthen their data management technologies in order to build strong digital capabilities. The core idea is to create compliant, efficient business models that protect customers' data privacy.

---

<sup>1</sup> <https://securitybrief.asia/story/ransomware-hits-65-of-organisations-in-singapore>

<sup>2</sup> <https://www.businesstimes.com.sg/technology/singapore-companies-pay-average-s15m-after-ransomware-attack-report>

There are two major changes businesses can expect as a result of data privacy regulations. First, privacy will become a fundamental expectation among customers. Second, transparency in privacy policies will no longer be optional. As consumers become more aware about data policies and with governments enforcing privacy requirements, companies are learning that implementing data privacy policies can create a business advantage by keeping them ahead of the curve.

On the other hand, from a business standpoint, the cost of compliance will shoot up since organisations might have to allocate separate staff and financial resources just to keep up with these regulations. With high noncompliance penalties and the potential risk of losing their brand value, organisations will be forced to pay to achieve compliance. The other impact on businesses is overregulation of policies. Customers become burdened by endless consent forms for every data process, taking away the ease of use of online platforms.

Through widespread implementation of regulations across the globe, businesses are at risk of noncompliance and increased investment. Many frameworks are being developed to help businesses find the right combination of optimal investment and compliance with regulations. Gartner's data security governance framework<sup>3</sup> describes how businesses can meet legal requirements while dealing with consumer data.

The framework suggests the following steps:

- Identify and discern the type of data that is impacted by data privacy compliance regulations.
- Develop privacy impact assessments for data protection and administer these periodically while keeping all business stakeholders involved.
- Configure technology controls to minimise risk to an acceptable level.
- Review security policies methodically and whenever business risks change.

The common misconception about data privacy regulations is that they only impact the legal department. That said, the point often missed is that everyone who works with data in a company must be aware of the regulations and stay compliant. Many experts studying these regulations propose that this has less to do with data management and more to do with change management processes. Businesses need to rethink and restructure the way they handle customer data. The better approach to integrating these privacy regulations into a business is to implement change management.

The proposal is such that investing in analytics and automation technologies should be any company's first step towards building a robust, compliant system that ensures adherence to most if not all privacy regulations. Most data privacy laws mention the customers' access rights, which essentially means that a customer can at any time ask for a copy of all the data that is being gathered on them, or for their data to be deleted.

---

<sup>3</sup> <https://www.gartner.com/en/documents/3978381>

Businesses will need digital, automated solutions to comply with these requests efficiently. For example, forms that autofill necessary details, desktop guidance tools, or virtual assistants will make the process faster with minimal manual effort. This will in turn reduce the possibility of mishandling data.

The constant shift of data privacy laws will only become more rigorous with time. The ideal step for any business to take would be to voluntarily comply with all the privacy laws in the locations where their businesses operate. Furthermore, countries and states affected indirectly by their businesses must also be taken into consideration as regulations like how the PDPA/GDPR require. In order to avoid or reduce exorbitant fines, operational interruptions, and the loss of customers, the sooner businesses plan and comply with these laws, the more successful they will be for all stakeholders.

### Author Bio



*Cecil Su currently leads various engagement teams on diversified advisory, security testing and threat intelligence projects across vertical industries for a mid-tier firm. Cecil has been a cybersecurity practitioner, consultant and advisor since the mid 2000s. He is a Fellow of the Association of Information Security Professionals (AiSP) and is involved in a wide range of cybersecurity initiatives in Singapore and globally.*

## Article from Cyber Threat Intelligence SIG

### Rantings of a Cyber Security Analyst

Disclaimer, for any marketing people reading this article, please note I am not specifically targeting anyone. These are just my personal views and I hope to shed some light, which I hope would make everyone's cyber security journey better.

AI, Machine Learning, Automation... the list of trend words goes on. I am not a salesperson, have never seen myself as one. As a technical person, all I want is a feasible solution to solve problems. Often, we hear lots of buzz words and how they can magically prevent attacks. The continuous write ups about how Product A can stop ransomware.

Are they lying? No. I genuinely believe every vendor has come up with unique ways to identify behaviours of a ransomware. Mind you, this is no easy feat as encryption is a legitimate process. Think of device encryption, encrypting your own files for secure



storage or transmission. Ransomware behaves the same way and to identify which is legitimate and which is not poses a tough challenge.

So why do I bring up this topic you may ask? I have seen many cases of companies being hit with ransomware and their immediate thought is that the product has failed them. I have even encountered a company that has changed their endpoint security vendor three times over a course of a few years, each due to a ransomware attack.

I am sure the conversation went like this: -

**Local IT Team:** We got hit with ransomware, Product A failed us! They told us they can prevent ransomware attacks!

**Product B Sales:** Our product can protect you against ransomware! (Pulls out Gartner and some other research article to back their claims).

**Local IT Team:** Ok, let's change to Product B.

\*Few months or years later, another ransomware incident occurs\*

**Local IT Team:** Product B failed us! They said they can prevent ransomware attacks!

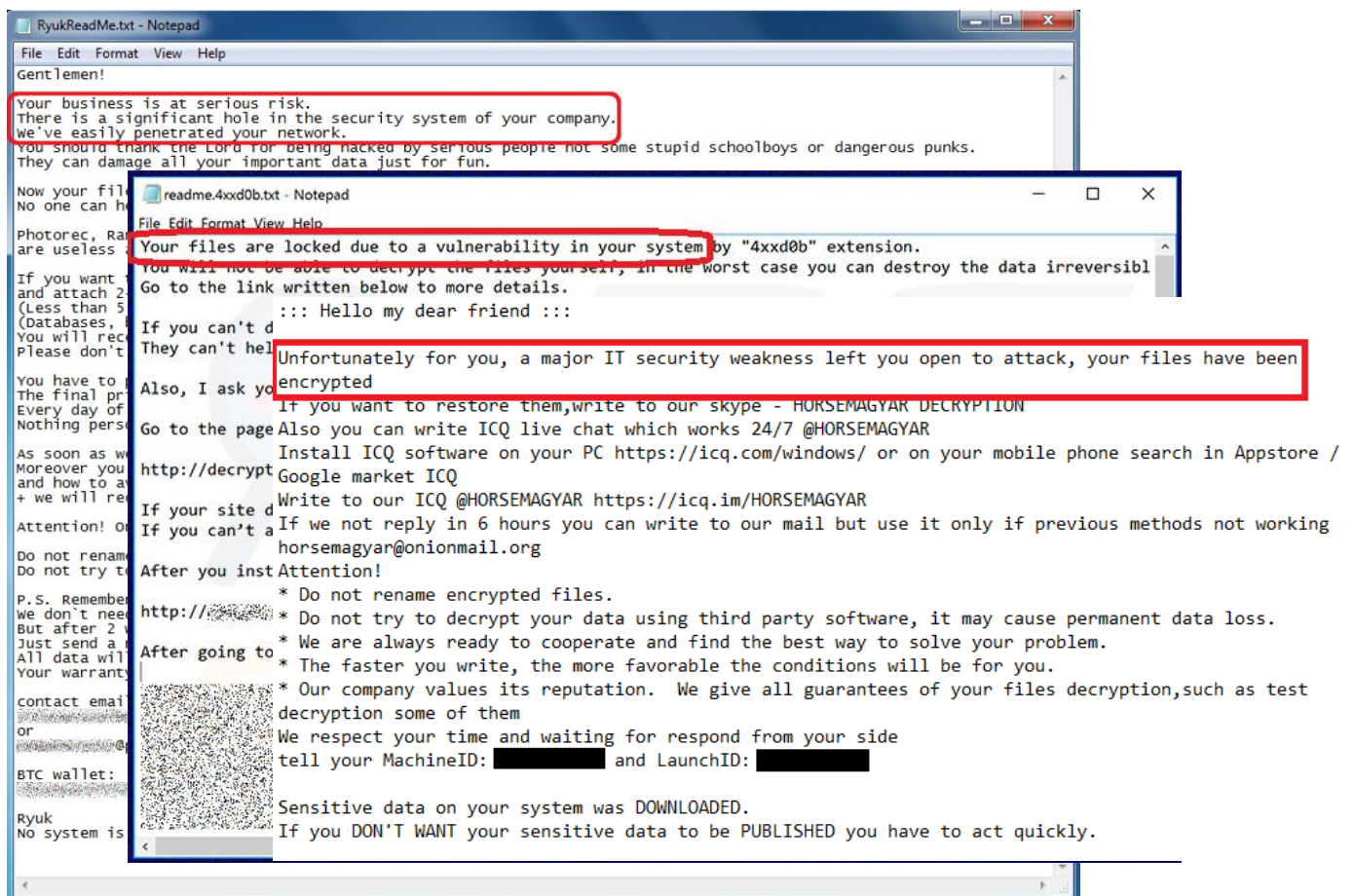
**Product C Sales:** We have the best ransomware protection in the market! (Again, pulls out Gartner and other research articles)

**\*The cycle continues\***

Now, is it true that all products failed? Did all the marketing, research articles lie to us? Being a threat analyst, I looked at these attacks and find that in most cases, these products will block the payloads used by the threat actor. So how, you may ask, did the ransomware still occur?

One important thing that I feel all these hype about ransomware attacks failed to talk about is that these are humans that have trained themselves to overcome security controls in as short amount of time as possible.

It is no longer a case of someone within the office accidentally clicking on a link or downloading a file. We are at an age where threat actors are putting in effort to understand how different OS works, what tools are available to them, how to obtain access and privileges. Noticed I never mentioned anything about improving their ransomware payload. These skills allow them to quickly identify security gaps, granting them permissions to shut off or overcome security products, or find a machine that has weaker controls. Some of these groups even proudly advertise they are testing your security controls.



I am not advocating ransomware groups, but those who got breached needs to acknowledge the truth in the highlighted statement above. Bear in mind, they referenced security system, not a specific product.

In a ransomware attack, I would like to say the ransomware is the end result, but it is the breach we should be concern about. Everyone seems to be so focused on the end result of seeing encrypted files that many failed to even consider breach prevention or detection. It just so happens that having the end result of ransomware draws the most profit for the threat groups now, but with a breach of an environment, the threat actor is free to do anything they wish.

You can buy the best gate, marketed as being hard to cut though with saws or any other tools, with a lock that has been advertised as unpickable but left a key hidden under the floor mat for convenience. If your house gets broken into because someone saw you place the key there, would you say the lock or gate failed you?

So, the answer is no, the marketing and sales did not lie to you, they just answered the specific question of "Can your product prevent ransomware" which they are not wrong for answering yes.

Maybe it is time the security teams step up to design and determine the requirements to secure their networks and not just follow trends and asking vague requirements.

### Author Bio



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 our CPP Partner, Nozomi Networks

### **The IT Pro's Guide to OT/IoT Security**

Learn how to manage the unique security challenges of critical infrastructure and industrial operations, including IT, OT and IoT devices & networks.

<https://info.nozominetworks.com/learning-guide-ot-iot-security-lp-0>

# Article from The Cybersecurity Awards 2021 Winner – Ng Hoo Ming



I'm truthfully honoured and grateful to be awarded with the Hall of Fame award 2021 by the AiSP. It came as a pleasant surprise. It wasn't the aim that I hankered for my professional career objective. Let me take this opportunity to express my heartfelt gratitude to the committee for your kind recommendation and awarded me with this prestigious accolade. I would also like to thank the Bosses, Colleagues and Industrial partners for your trusts and support rendered to me throughout my 30 over years of career in the cyber security field, without that I would have given up long ago in this challenging task.

Why I ended up spending my entire professional life in the cyber security field? I was by training a software engineer in the 80s. There wasn't security per se at that time. I recalled after my study, I was posted to the Ministry of Home Affairs as a research and development engineer to develop secure solutions to protect Government's secret data. It was a very technically challenging and fulfilling role, as there wasn't anyone assuming this critical role in the Government. I derived much satisfaction when you see your solutions being deployed successfully Government wide supporting the day-to-day secure computing needs at the national level and created many first in Singapore if not industry security solutions. It was this reason that sustains my strong commitment to continue pursuing a career in the cyber security field.

[back to top](#)



Besides the many security solutions that I had developed, there were other related works throughout my career that I have the opportunity to contribute to in making Singapore's cyber space more secure. When I was appointed as the Director in charge of the newly formed Singapore Infocomms Technology Security Authority (SITSA) in 2009. I have established the national incident reporting framework to facilitate the proper handling of cyber incidents at the national level to deal with major threats to national security which include cyber-terrorism and cyber espionage. I have also spearheaded the development of a cyber security readiness maturity index to guide the critical information infrastructure sectors in their effort to better improving their cyber security posture systematically. Another major work undertaken by me was to help the Cyber Security Agency, when it was established in 2015, to develop its operation capability.

In my final remarks to everyone there. To be respected in this field or equally in other profession, it is paramount to have "Professional Integrity". Without that you would not be able to garner the respect of others. Be a "TRUE CONSULTANT" not a "CON" "SUL" "TANT".

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

# PROFESSIONAL DEVELOPMENT

## Listing of Courses by Wissen International



**Ready to Crack the Toughest Cyber Challenges?**

**CyberQ**  
Fully Cloud Orchestrated Military-Grade Cyber Range

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

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

Vulnerability research techniques covered:

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

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

**SPECIAL PRICE \$112 FOR AISP MEMBERS**  
EMAIL [AISP@WISSEN-INTL.COM](mailto:AISP@WISSEN-INTL.COM) NOW!

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

Ready to crack the toughest cyber challenges?

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

Enjoy a special price of \$112 for AiSP members, please email [aisp@wissen-intl.com](mailto:aisp@wissen-intl.com) now!

## Listing of Courses by ALC Council



### Stand out from the crowd

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

We offer the most in-demand cyber certifications including:

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

### The right training makes all the difference

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

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

## AiSP Member Pricing – 15% discount

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

## Upcoming Training Dates

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

## Special Offers.

We periodically have special unpublished offers. Please contact us [aisp@alctraining.com.sg](mailto: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](mailto: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](mailto:learn@alctraining.com.sg) | [www.alctraining.com.sg](http://www.alctraining.com.sg)



# Qualified Information Security Professional (QISP®) Course



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

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

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

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

## COURSE DETAILS

2022 Course dates can be found on [https://www.aisp.sg/qisp\\_training.html](https://www.aisp.sg/qisp_training.html)

Time: 9am-6pm

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

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

\*Utap funding is available for NTUC Member

\* 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](mailto:secretariat@aisp.sg) or Telegram at **@AiSP\_SG**.

Program Partner



Delivery Partners



# Cybersecurity Essentials Course



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

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

## **Course Objectives**

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

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

- Cloud Computing
- Cybersecurity Operations

## COURSE DETAILS

Training dates for year 2022 can be found on [https://www.aisp.sg/cyberessentials\\_training.html](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](mailto:secretariat@aisp.sg) to register your interest.

Program Partner



Delivery Partners





# MEMBERSHIP

## AiSP Membership

### **Complimentary Affiliate Membership for Full-time Students in APP Organisations**

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

### **Complimentary Affiliate Membership for NTUC Members**

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2021 to 2022) from 1 Sept 2021 to 31 Dec 2022. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. [This does not include Plus! card holder \(black-coloured card\), please clarify with NTUC on your eligibility.](#)

On [membership application](#), please do not email your personal data to us via email if your information or attachment is not password-protected. Please send us your password via [Telegram](#) (@AiSP\_SG).

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

### **AVIP Membership**

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

Sign up for  
**AVIP MEMBERSHIP**

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

## **BENEFITS**

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

## **PRICE**

**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](mailto: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](http://www.aisp.sg/membership.html)

## AiSP Corporate Partners



Acronis



[back to top](#)



Lookout®





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

## AiSP Academic Partners



## Our Story...

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

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

### Our Vision

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

### Our Mission

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

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



 [www.AiSP.sg](http://www.AiSP.sg)

 [secretariat@aisp.sg](mailto:secretariat@aisp.sg)

 +65 8878 5686

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

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