

## News & Update

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

## Contributed Contents

- D&P SIG: Accountability in Data Protection
- Xcellink: Xcellink Workforce Services
- Fortinet: Threat Predictions for 2023: New Attack Surfaces and Threats Emerge as Crime
- Yeswehack: How we help our clients step-by-step in their Bug Bounty program

## Professional Development

## Membership

# NEWS & UPDATE

## New Partners

AiSP would like to welcome ASUS, Armis, Detack, Fergus, Forescout, Grab, LearnCollab, SGS, Softscheck, Temasek, Tenable and Wissen as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

### New Corporate Partners



## Continued Collaboration

AiSP would like to thank Nanyang Polytechnic, Ngee Ann Polytechnic, Responsible Cyber, Singapore University of Social Sciences (SUSS) and ST Engineering for their continued support in developing the cybersecurity landscape:



## 2023 Welcome Message from AiSP President - Mr Johnny Kho



It has been an eventful year of 2022 for AiSP and AiSP has been fulfilling our mission of bolstering the development, increase and spread of information security knowledge and its related domains. I am glad to share with our members and friends on the iconic events that AiSP had embarked on

### **First Inaugural South East Asia Cybersecurity Consortium (SEACC) Forum**

AiSP has strengthened our collaboration into the South East Asia (SEA) region and gathered representatives from the various associations from Indonesia, Cambodia, Brunei, Malaysia, Myanmar, Thailand and Vietnam to sign a Memorandum of Understanding (MoU) at the inaugural South East Asia Cybersecurity Consortium Forum held on 23 November. AiSP is committed to grow the cybersecurity sector beyond Singapore and regionally with increased collaborations and activities with associations from the SEA region. We ended the year with WiSAP (Women in Security Alliance Philippines) signing an MoU with AiSP to join the SEACC partnership. We look forward to creating a stronger regional cybersecurity ecosystem with our SEACC partners!

### **Learning Journey to Kuala Lumpur with IHL students**

In the recent weeks, AiSP had brought IHL students to Kuala Lumpur, Malaysia to visit the government agencies, companies and universities for an immersive and interactive learning journey trip. In partnership with National Youth Council, AiSP led a team of youths abroad to learn more about the culture and working environment overseas for them to better appreciate our local ecosystem in Singapore. They visited technical universities, data centers, security operation centres and observed the daily activities in appreciation of the collective impact to the cybersecurity ecosystem. Students also had the opportunity to hear about the current job landscape in Malaysia from our Corporate Partner - Fortinet and understand more on the various certifications that were available to advance their knowledge on cybersecurity. There was also cultural exchange of information with the students studying in KL and it was a fruitful and enriching trip for them.

### **Engagement with the community through Digital for Life Initiative**

AiSP is not only concerned about the professionals but also the community as a whole and with the increase in scams, we recognized the importance to educate the public. Under the Digital for Life initiative, AiSP had went down to more than 10 different community centres to share with the senior citizens and general public about cybersecurity awareness. Since the Cyber Wellness Programme was launched, AiSP had reach out to more than 12,000 members of the Public to stay safe online. Our committee members has volunteered their personal time to give talks to the elderly on Cybersecurity Awareness in English and Mandarin. In recognition of our support and partnership, AiSP also received the token of appreciation at the 4 November partners appreciation dinner held by IMDA. With the increased awareness, it will help to create a safer cyberspace for everyone.

### **What to expect for 2023**

In addition, AiSP participated in major expo events such as GovWare 2022, Cyber Security World Summit, Singapore Fintech Festival where the team shared about AiSP membership and initiatives to the attendees. More international companies were aware of AiSP and more interesting collaborations can be expected in the coming year. For year 2023, we can look forward to another exciting year with more collaborations in the SEA region with our association partners, increased AiSP presence at international conferences and learning journey trips to our local companies and neighbouring countries. Increased engagement as well as recognition of the contributions of our Cyber Youths will be showcased in upcoming Regional Bug Bounty events, Student Volunteer Recognition Program (SVRP) and the Annual Youth Symposium. Thank you for journeying another year with AiSP!

# Knowledge Series Events

## Upcoming Knowledge Series

### Software Security on 18 Jan



**AiSP Knowledge Series – Software Security**

AiSP Knowledge Series  
**SOFTWARE SECURITY**  
18 Jan 23 | 3PM - 5PM | Zoom



**Chris Lee**  
Solutions Engineer,  
BeyondTrust



**Steve Neo**  
Regional Business  
Development Director  
Parasoft S.E. Asia



Organised by  
  
Association of  
Information Security Professionals

Supported by

  
  
  
In support of  


In this Knowledge Series, we are excited to have BeyondTrust and Parasoft to share with us insights on Software Security. 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.

**5 Critical Steps for Complete Endpoint Security**

Speaker: Chris Lee, Solutions Engineer, BeyondTrust

70% of successful breaches started at the endpoint in 2019. Since then, a global pandemic has caused a large-scale shift to remote work – a perfect storm for privilege abuse. As a result, malware has increased by 30,000%. This is especially concerning when many companies still rely on antivirus software (AV) or Endpoint Detection and Response solutions (EDR) alone to secure endpoints. In this visionary session, we will be highlighting which two overlooked steps can mitigate the 60% of modern threats that are missed by AV, and why the need for organizations to move from a reactive to a preventative approach is more important than ever.

**DevSecOps@Speed – Pitfalls to Avoid and Still get the job done Faster!**

Speaker: Steve Neo, Regional Business Development Director, Parasoft S.E. Asia

In the new era of Digital Factories, the impact of having their data hacked or held for ransom can be devastating. We are not new to security measures designed to enforce encryption and authentication. These protections are insufficient if the asset is not developed securely at every phase of its SDLC; starting from inception to maintenance and final retirement : what we called DevSecOps. Security coding analysis solutions exist to mitigate security issues, allowing you to integrate Security into your DevOps pipeline so that security is built right into your organization's build process. Higher quality, lower costs in testing and improvement in time-to-market have been reported by many organizations that have incorporated methodologies like Agile, Scrum, DevSecOps or CI/CD.

Putting things together is not without pitfalls! Join us to learn tips and tricks by top Digital Factories on how to DevSecOps@Speed.

Date: 18 January 2023, Wednesday

Time: 3PM – 5PM

Venue: Zoom

Registration:

[https://us06web.zoom.us/webinar/register/6816706716530/WN\\_I7ckc\\_StRTSQBoenguG3rA](https://us06web.zoom.us/webinar/register/6816706716530/WN_I7ckc_StRTSQBoenguG3rA)

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. Software Security, 18 Jan 23
2. Data & Privacy, 22 Feb 23

**Please let us know if your organisation is keen to provide speakers!** Please refer to our scheduled 2023 webinars in our [event calendar](#).

# Cybersecurity Awareness & Advisory Programme (CAAP)

## Malware Awareness Day on 6 Jan 23



**Malware Awareness 2023**  
Date/Time : 6th Jan 2023, 3pm  
Venue : Huawei Digi X Lab  
( refreshment provided )  
Registration contact : karen.ong@aisp.sg

 <b>Dennis Chan</b> AiSP Exco, Country Cybersecurity & Privacy Officer Huawei	 <b>Yum Shoen Yih</b> Cybersecurity Agency of Singapore	 <b>Wong Yong Wah</b> Cybersecurity Consultant wizlynx group	 <b>Jeffery Zhang</b> CTO Data Center and Storage Solution Sales Huawei
--	--	--	---

On this day we will like to honour 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, Wong Yong Wah from Wizlynx and Jeffery Zhang from Huawei.

Venue : Huawei Digi X Lab  
Date: 6th Jan 2023  
Time: 3pm - 5pm

Click [here](#) to register.

## A Practical Approach in Building Security Resilience in Zero Trust on 18 Jan

**AISP**  
Advance Connect Excel

### A PRACTICAL APPROACH IN BUILDING SECURITY RESILIENCE IN ZERO TRUST

18 January 2023 10.30AM to 12:00PM

Singapore Cisco Office, Building 80, Level 25,  
80 Pasir Panjang Road, Singapore 117372

Organised By

**AISP** **CISCO SECURE**

Register Now!

While many organizations strive to achieve zero trust in order to achieve cybersecurity resilience, this concept means different things to different organizations. Zero trust is not a product, but a mindset, a journey towards building better security resilience within an organization that includes a set of core capabilities and use cases.

The Zero Trust principles inspire a connected, cohesive, and holistic approach, one that requires a connected platform with capabilities such as NGFW, MFA, ZTNA, XDR, Segmentation, etc that work with one another in order to provide least privilege access yet maintain end-user experience.

This session aims to help organizations avoid confusion and develop a clear strategy about how to go about implementing a resilience zero trust security model and achieve their desired outcomes.

**Agenda:**

- 10.30AM Opening by Cisco
- 10.35AM Fireside Chat : Security Resilience in Zero Trust
- 11.00AM Cyber Threat Landscape by Talos
- 11:30AM Connect & Secure the Hybrid World with Cisco DUO
- 12.00PM Closing & Lunch

Date: 18 January 2023, Wednesday

Time: 10.30AM – 12.00PM

Venue: Singapore Cisco Office, Building 80, Level 25, 80 Pasir Panjang Road, Singapore 117372

[Register Here!](#)

# Student Volunteer Recognition Programme (SVRP)

## Learning Journey to Kuala Lumpur from 12 Dec to 15 Dec 2022

AiSP brought a total of 13 Youths to Kuala Lumpur (KL) for Learning Journey experience from 12 Dec 22 to 15 Dec 22 with the support of the National Youth Council, AiSP Corporate Partners and MOU Partners. We visited universities, companies and the government authority for an insightful learning experience on cybersecurity and discover KL on the cultural perspective . AiSP would like to take this opportunity to thank the universities, companies and government authority for hosting us.

### Day 1

First stop for the Learning Journey, our students visited the Tunku Abdul Rahman University of Management and Technology. Our IHL students had the opportunity to interact with the students and exchange their views on cybersecurity. They visited the Centre of Excellence Big Data Analytics and Artificial Intelligence (AI) where they saw the AI robots display and the PCs that costed the price of a car in Malaysia! The impressive display of the esports arena also caught their eyes and interest.







## Day 2

The students visited our Corporate Partner (CPP) Fortinet office in Malaysia for a morning of sharing and tour of their new office.



We also visited EC Council Global Sdn Bhd and tour the office and the Security Operations Centre (SOC) live at work. It was an inspiring and enriching time for our students as they had a deeper understanding on the importance of having the right skills being put to the right usage and also how they could contribute to the ecosystem positively.



### Day 3

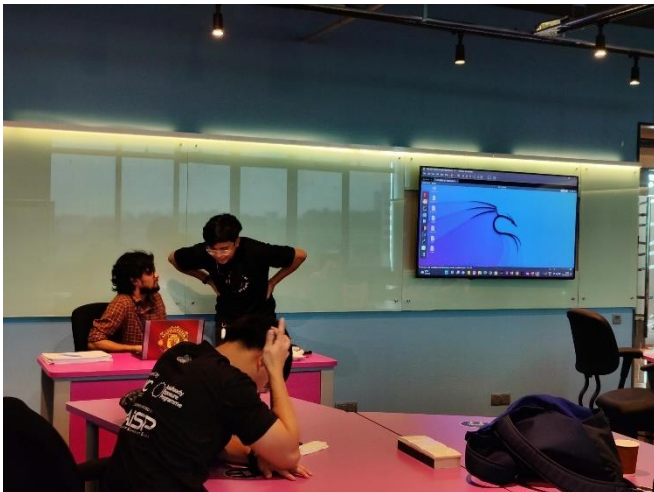
Day 3 of our Overseas Learning Journey and we visited Cybersecurity Malaysia for a morning of sharing and live gallery tour.



Next stop we visited Malaysia Board of Technologists (MBOT) at their office.



Our third stop for day 3 was to visit to Asia Pacific University of Technology & Innovation (APU), one of the Malaysia top 10 Universities. Our Youths get to participate in a mini cybersecurity workshop conducted by their lecturer. Thank you to the APU student ambassador for bringing us around your school and sharing with us what you do in school.





#### Day 4

Our last stop for the whole learning journey trip we visited to Time dot com Malaysia telecom service provider. Our Youths get to see the data center and learn about the daily operations there.







Nomination Period:  
1 Aug 2022 to 31 Jul 2023

# CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

Tier	Requirements
Bronze	Completion of one of three pillars or complete three of three pillars with minimum 50% attained hrs. + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Silver	Completion of two of three pillars + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Gold	Completion of all three pillars + Skills: 45 Hours or more + Events: 60 Hours or more + Leadership: 45 Hours or more



Scan the QR Code for the Nomination Form



**The SVRP comprises three broad pillars where IHL students can volunteer:**

- + Skills-based: E.g. Conduct cybersecurity workshops or develop related software
- + Events-based: E.g. Provide support at technology or cyber-related events
- + Leadership: E.g. Mentoring younger students and managing teams or projects

Visit [www.aisp.sg/svrp.html](http://www.aisp.sg/svrp.html) for more details



Nomination Period:  
1 Aug 2022 to 31 Jul 2023

# CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

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

Example A	Example C
+ Leadership: 10 Hours	+ Leadership: 0 Hour
+ Skill: 10 Hours	+ Skill: 36 Hours
+ Outreach: 10 Hours	+ Outreach: 0 Hour
Example B	Example D
+ Leadership: 0 Hour	+ Leadership: 0 Hour
+ Skill: 18 Hours	+ Skill: 0 Hour
+ Outreach: 18 Hours	+ Outreach: 42 Hours



Scan the QR Code for the Nomination Form

## The track for Secondary School and Pre-University students comprises three broad pillars where they can volunteer:

- + Leadership refers to how the volunteer leads a team to complete the voluntary activity.
- + Skill refers to how the volunteer applies his/her cybersecurity knowledge to others
- + Outreach refers to how the volunteer is involved in outreach efforts (social media, events) to increase cybersecurity awareness for the public.

Visit [www.aisp.sg/svrp.html](http://www.aisp.sg/svrp.html) for more details

# AiSP Cyber Wellness Programme

<p>Organised by:</p> 	<p>Supported by:</p> 	<p>In Support of:</p> 
<p>The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."</p>		
<p>Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website (<a href="https://www.aisp.sg/aispcyberwellness">https://www.aisp.sg/aispcyberwellness</a>) to get updates on the latest Cyber tips, Cyber news, activities, quiz and game happenings related to Cyber. Scan the QR Code to find out more.</p>		
		
		
<p>Scan here for some tips on how to stay safe online and protect yourself from scams</p>	<p>Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship &amp; Ethics.</p>	
		
<p>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.</p>	<p>Scan here if you are looking for activities / events to participate in for knowledge exchange / networking / get to know more people / stay protected &amp; helping others.</p>	
		
<p>Want to know more about Information Security? Scan here for some career advice on Information Security.</p>	<p>To find out more about the Digital for Life movement and how you can contribute, scan here.</p>	
<p>Contact AiSP Secretariat at <a href="mailto:secretariat@aisp.sg">secretariat@aisp.sg</a> to find out more on how you can be involved or if you have any queries.</p>		

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

## Ladies in Cybersecurity



AiSP will be celebrating the 5 years anniversary of the AiSP Ladies in Cyber Charter in 2023. We will be having a series of activities in 2023 from our quarterly learning journey to our International Women Day celebrations to our annual Ladies in Cyber Symposium and our International Cyber Women Day celebrations. We will also be organizing a 5 year anniversary dinner in Q3 of 2023. This is in addition to the school talks and mentoring programme that we have currently.

The AiSP Ladies in Cyber Bear Mascot and Mentor Booklet will also be launched as part of the 5 year anniversary in 2023. AiSP Ladies in Cyber Charter hoped to reach out to as many females and share with them the journey in Cybersecurity.

Interested to be part of the AiSP Ladies in Cyber Charter or how you can be involved in the AiSP Ladies in Cyber mentoring programme or school talk? Contact the AiSP Secretariat at [secretariat@aisp.sg](mailto:secretariat@aisp.sg).

Follow our AiSP Social Media to stay updated on our Ladies in Cyber Anniversary Programme. We looked forward to having you to be part of our milestone and celebration.





## 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)

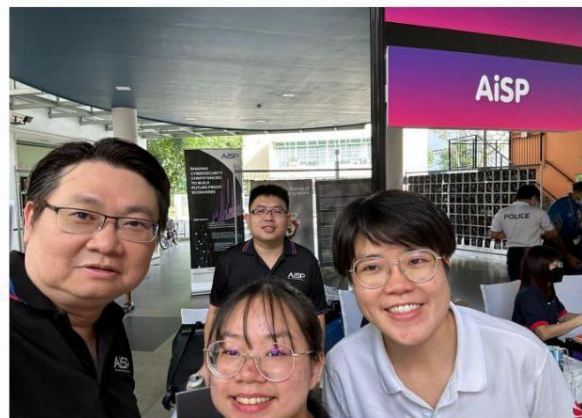


# Digital for Life

## Celebrate Digital @ Taman Jurong on 17 Dec

As part of the Digital for Life Movement, AiSP was at the Celebrate Digital @ Taman Jurong with our Corporate Partner - Huawei Singapore where we setup a booth to share with the public on how to stay safe online and beware of scams.

Thank you to our AiSP EXCO Dennis Chan for taking time off to share with more than 30 elderly on 网络安全人人有责.



## Whampoa CC Digital Carnival on 18 Dec

As part of the Digital for Life Movement, AiSP was at the Whampoa CC Digital Carnival with our Corporate Partner - RSM Singapore where we setup a booth to share with the public on how to stay safe online and beware of scams. Thank you Senior Minister of State, Mr Heng Chee How for visiting our booth. Our TCA2022 Leaders Award Winner, Mr Hoi Wai Khin also did a sharing and skit on online scams.



## The Cybersecurity Awards



**TCA 2022** has concluded on 11 November 2022. The Cybersecurity Awards 2023 nominations will start on 01 February 2023.

### 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)

Please email us ([secretariat@aisp.sg](mailto:secretariat@aisp.sg)) if your organisation would like to be our sponsors for The Cybersecurity Awards 2023! Limited sponsorship packages are available.

**TCA2023 Sponsors & Partners**

Organised by



Supporting Associations



Platinum Sponsors



Gold Sponsors



Silver Sponsors



# CREST

## **CREST launches the CREST Defensible Penetration Testing standard, CREST OWASP Verification Standard (OVS), and the CREST Skilled Persons Register**

### CREST Defensible Penetration Test

The Defensible Penetration Testing standard was published in July after input and feedback from CREST companies and members of the buying community. Thanks to everyone who contributed to this standard. CREST plans to continually promote it as an exemplar of how a Penetration Test should be scoped, delivered, and signed off.

The standard reduces the information gap between buyers and service providers. It gives clear guidance on the importance of accredited organisations and skilled and competent individuals. CREST recommends that all members leverage the standard to demonstrate the benefits of being CREST accredited when bidding for sales opportunities.

### **CREST OWASP Verification Standard (OVS)**

CREST has also launched the OWASP Verification Standard (OVS). This new program is designed to provide higher levels of assurance to organisations that utilise mobile and web-based applications.

The standard leverages ASVS and MASVS from OWASP and is designed to build more consistent and scalable assessment approaches for global organisations. CREST engaged with governments, regulators, and digital marketplace operators to better understand the need for AppSec standards.

OVS provides a pathway for ensuring that applications are assessed with a consistent methodology and deliver a consistent series of reports that can be ingested and analysed at scale. The CREST OVS program demonstrates strong collaboration with OWASP. Collectively, the program is intended to stimulate a step change in security assessment standards.

### **CREST Skilled Persons Register**

Both CREST OVS and the Defensible Penetration Testing standard embrace the concept of accredited organisations and skilled and competent individuals. Both of these programs show strong enrolment in the CREST Skilled Persons Register.

The register requires individuals to share details of their skills, competencies and experience and sign up for a code of conduct. Once submitted, this validates the application by generating a unique CREST ID for the individual. We expect CREST IDs to become increasingly common indicators of skills, competence, and professional standards.

These three initiatives are all core to the updated vision we published early this year.

We will continually pursue programs that build trust in the digital world by raising professional standards. In addition, each of these activities will help deliver measurable quality assurance for the global cybersecurity industry. We hope our members will embrace them and use them to differentiate themselves positively when conducting work across the globe.



Rowland Johnson, President of CREST  
 Visit [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
5-6 Jan	SINCON	Partner
6 Jan	Malware Awareness Day	AiSP & Partner
9 Jan	School talk at Bukit Panjang Government School	AiSP & Partner
12 Jan	Vietnam Retail Banking Forum 2022	Partner
18 Jan	A Practical Approach in Building Security Resilience in Zero Trust	AiSP & Partner
18 Jan	AiSP Knowledge Series – Software Security	AiSP & Partner
20 Jan	AiSP x CSCIS MOU Renewal	AiSP & Partner
3 Feb	CNY Lo Hei	AiSP
12 Feb	Celebrate Digital festival for Nee Soon Link residents	AiSP & Partner
16 Feb	CISO Malaysia	Partner
20-22 Feb	CISO Sydney	Partner
21-24 Feb	Cyber Security For Financial Service Asia	Partner
22 Feb	Data & Privacy Knowledge Series	AiSP & Partner

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

# CONTRIBUTED CONTENTS

## Article from Data & Privacy SIG

### Accountability in Data Protection

Since the Personal Data Protection Act (PDPA) 2012 has moved its emphasis from the 10 Obligations<sup>1</sup> to organisations' accountability in 2021, organisations that have yet to have a data protection management programme in place may not have considered how accountability is linked to self-governance on data protection compliance.

Accountability is a fundamental principle of the PDPA, where organisations must take responsibility for the personal data under their care<sup>2</sup>, through a structured approach<sup>3</sup>:

1. Ensure staff's practices are in compliance with organisation's policies and procedures for data protection and PDPA compliance,
2. Ensure organisation's PDPA compliance measures are available to customers who entrusted with their personal data,
3. Ensure organisation is able to cooperate with regulatory authorities on complaints, investigation and data breaches.

### What does it mean to organisations that have yet to set up a data protection management system (DPMS)?

While the Personal Data Protection Commission has advocated organisations to have a data protection management programme in place, my view is a system rather than a programme would be more valuable to organisations. Systems require organisations to monitor their effectiveness, enable scalability and ensure sustainability. It is not meaningful for organisations to implement a programme or a system if they are not able to dedicate resources to protect their customers' personal data.

#### 1. Ensure staff's practices are in compliance with organisation's policies and procedures for data protection and PDPA compliance

One school of thought that organisations' documentation of implemented policies and procedures demonstrate their data protection efforts. Documentation requires sustained efforts; if this fundamental is not in place, it is uncertain how the organisations have proper measures in place to protect personal data. However, it is not uncommon for companies not to have such documentation in place. This may arise from the company's standpoint that it is not a significant business risk based on the PDPA penalties and the (low) likelihood of data breach being revealed publicly. After all, the

---

<sup>1</sup> Including Transparency Obligation

<sup>2</sup> Please see Part 3 of the PDPA 2012: <https://sso.agc.gov.sg/Act/PDPA2012#P1III->

<sup>3</sup><https://www.pdpc.gov.sg/accountability#:~:text=Accountability%20Principle,under%20their%20possession%20or%20control>

regulator's investigation streamed from customer's complaint or if a data breach was made known.

PDPA compliance would not be taken seriously by companies that fulfil statutory requirements on paper, i.e., appoint a data protection officer (DPO), and put up a data protection statement in their website. When customers read the statement that is titled as policy, it functions more as a statement as how the company's policy would be implemented and enforced are not revealed. The appointed DPO may not have received company's support to be proficient in PDPA compliance, let alone data protection for company's clients.

Policies and procedures are a means to an end, as the focus is to ensure employees' behaviours and practices are in compliance with organisation's directions on data protection. This sets organisations that are committed to ensure data protection apart from those that prefer 'paper' compliance.

There are various means to ensure compliant practices, one common way is to have mandatory regular training for all employees in the organisation, not limiting to selected few. While not all staff may handle personal data in their areas of work, it is important to build an organisational culture where everyone understands the importance of data protection and how they can play their part. The management is ultimately accountable for the company's data protection, not the DPO. It is evident that when management does not support data protection, cracks can be seen in daily operational practices. It just takes one mistake to cause a data breach.

## **2. Ensure organisation's PDPA compliance measures are available to customers who entrusted with their personal data**

In addition to their commitment on data protection in their policies, organisations have to be open on their compliance measures to customers who have the right to ask. Compliance measures are not restricted to customers only as it should cover employees' personal data as well. The measures would generally include,

- The organisation's approach to protect personal data including not to over retain personal data,
- Its promise to notify affected individuals promptly on data breach so that the individuals can minimise potential harm arising from the data leak; and,
- Implemented policies are relevant to the prevailing laws, societal norms and stakeholders' expectations, as a way to endear trust.

A thought leader shared the data breach notification in the General Data Protection Regulation underlines a principle where customers and the public would hold controllers (or organisations in PDPA) accountable to make things right after a data breach. This is more effective than regulator's penalty alone. The same can be said for PDPA'S Mandatory Data Breach Notification Obligation (MDBNO) and how organisations should be transparent in disclosing their breaches to affected individuals, even if the impact is lower than stipulated criteria of MDBNO.



Savvy consumers should be aware that there is a trade-off between convenience and security when it comes to the use of personal data. Also, if it sounds too good to be true, it is likely is. When individuals pay a low fee for a service or product, individuals have to be clear on their risk appetite in disclosing personal data, contact details and financial information to third parties – given that proper security requires resources.

### **3. Ensure organisation is able to cooperate with regulatory authorities on complaints, investigation and data breaches**

If organisations are motivated to avoid the financial penalties for PDPA infringement, they would want to cooperate with the authorities on complaints, investigation and data breaches as a baseline requirement. However, organisations that have yet to grasp the accountability principle would be challenged to fully support the authorities with proper documentation and relevant evidence on their data protection measures. Organisations that value their reputation seriously, would tend to monitor complaints received on possible PDPA infringement or privacy concerns. Having a process to manage complaints and feedback while ensuring confidentiality requires due care and consideration by the management. It would not be appropriate to use the same customer feedback channel for data breach incident management, if the incident would be investigated by the same staff who caused the breach. The timeline should be in accordance to the MDBNO, and to ensure proper records on management's decision not to report the incident to PDPC and risk assessment on impact to affected individuals. The data breach report should be direct to management, thus there is expectation that the organisation's DPO has direct access to the Chief Executive Officer or equivalent and there should not be a conflict of interest for DPO carrying out his or her job objectively.

The Personal Data Protection Commission (PDPC) advocates complaints to be resolved by the organisations, thus it is important for the latter to have a systematic complaint and incident management process for potential PDPA infringement. Complaints that are resolved timely with affected individuals should be made known to the PDPC voluntarily, for transparency and to avoid potential future dispute with affected individuals. My personal view is organisations that chose to admit their mistakes and rectify them timely, would be more committed to prevent infringements and breaches. Consumers who value their privacy and PDPA rights should be wary on organisations that misuse personal data on purpose or repetitively.

#### **Accountability matters**

As a good practice to strengthen its data protection competencies, the organisation could demonstrate accountability by establishing a structure for governance and risks assessments, by developing management policies and practices for the handling of personal data, and by establishing processes to operationalise the policies and practices. This is a compelling value proposition to customers, partners and employees. The most powerful persuasion for organisations to be accountable for data protection is when customers speak with their purchasing power. When customers paid for a product or service, they did not agree to sacrifice their privacy and be affected by possible

impersonation or scams. Organisations that demonstrate accountability would go a much longer way in cementing their legacies and public trust.

*Contributed by Yvonne Wong, Co-opted Committee Member, EXCO, Association of Information Security Professionals (AiSP)*



[Bio]

Yvonne is currently a Co-opted Committee Member, EXCO, in AiSP. She is volunteering in the Cyber Threat Intelligence Special Interest Group (SIG), and Data and Privacy SIG, and is a Fellow in Information Privacy with International Association of Privacy Professionals. Yvonne has been a practitioner, consultant and trainer for Governance, Risk and Compliance (GRC) since 2015. She is presently the Senior Manager in the Yishun Health Data Protection Office.

## Article from SME Conference Sponsor, Xcellink

**xcellink.pte.ltd.**

*completing your technology chain*

### **Xcellink Workforce Services:**

Established in 1995, Xcellink more than 2 decades of Enterprise ICT Operation management experience and capabilities development, as a trusted vendor partner to high-growth global companies, established local enterprises and government-linked corporation. We support organisation with recruitment, managed operations and IT outsourcing services within the technology and infocomm sector.

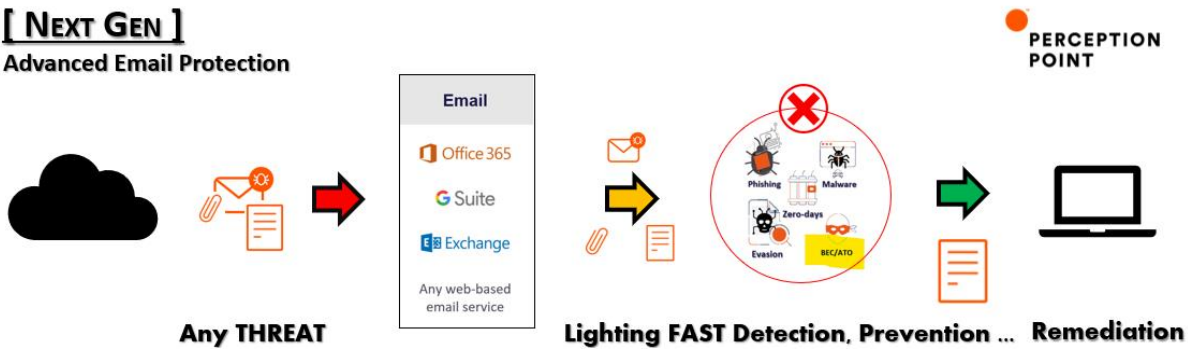
Xcellink is excited to have Perception Point as part of our Cybersecurity Solutions Partner. Their solutions provide effective and holistic threat prevention for our customers' business email platform. Its unique 7 detection layers provide a comprehensive prevention, detection and remediation of threats across emails and cloud collaboration channels. Perception Point's Advanced Email Security Solution is the next-gen email

[back to top](#)

security software that prevents APTs, phishing, malware, ATO, impersonation, and BEC attacks with the speed, scale, and agility of the cloud.

**[ NEXT GEN ]**

**Advanced Email Protection**



**Perception Point Researchers Discover “Phishing in Motion” Video Scam**

Blog post: <https://perception-point.io/blog/perception-point-researchers-discover-phishing-in-motion-video-scam/>

The team researchers discover a 2-step phishing campaign that utilizes a video to execute its payload.

**How the Phishing campaign works**

This attack appeared in an email sent to a client. However, due to the content of the email, the message was flagged by our advanced threat detection platform and never made it to the client’s inbox. It was analyzed by the Perception Point Incident Response team, who reported that the email contained a fake invoice seemingly delivered via Egress, a British company that provides email security services like encryption and, ironically, anti-phishing software. \*Note how the email body also contains the sender’s signature, alluding to an external account takeover (ATO), but more on that later.

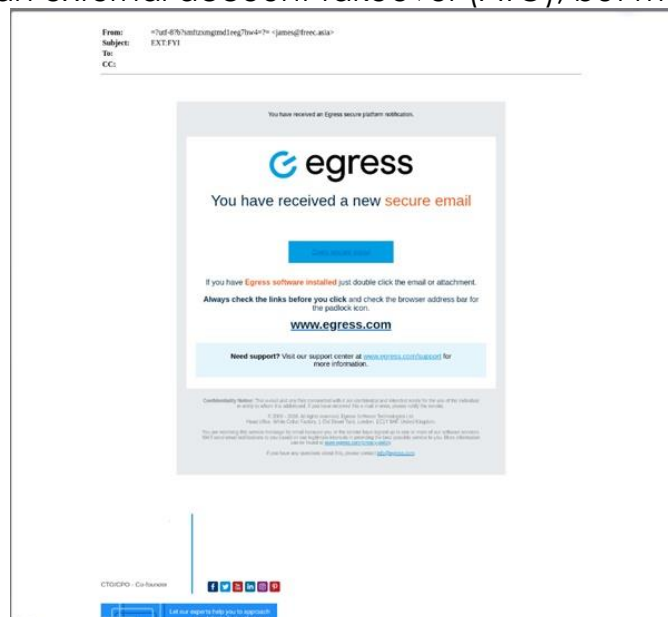


Figure 1: The phishing email

When you click on the invoice, it leads to Powtoon's website, a platform that allows people to share visual content. A site like this is ideal for cyber attackers, as using a legitimate platform to execute their malicious payload increases an attack's "legitimacy". Here, the attacker uploaded a video that reveals the malicious payload – a link to a malicious site – when played.

This is a 2-step phishing attack, meaning that the attacker prompts the user to click on a button or link within the initial web page in order to redirect them to the malicious site. It is on this secondary site that the attacker attempts to steal the user's credentials.

### A phishy and tricky attack

While this may seem like an obscure phishing attack that surely no user would fall for, the attacker employs a series of tricks to increase the attack's success rate:

*The fake invoice originates from a "legitimate email account," which was actually compromised, and appears to be using an email encryption service (Egress). The message contains the company's logo and assures the recipient that they "have received a secure email" (Figure 1).*

The first malicious payload is a clickable link within a video hosted on a legitimate platform, Powtoon.

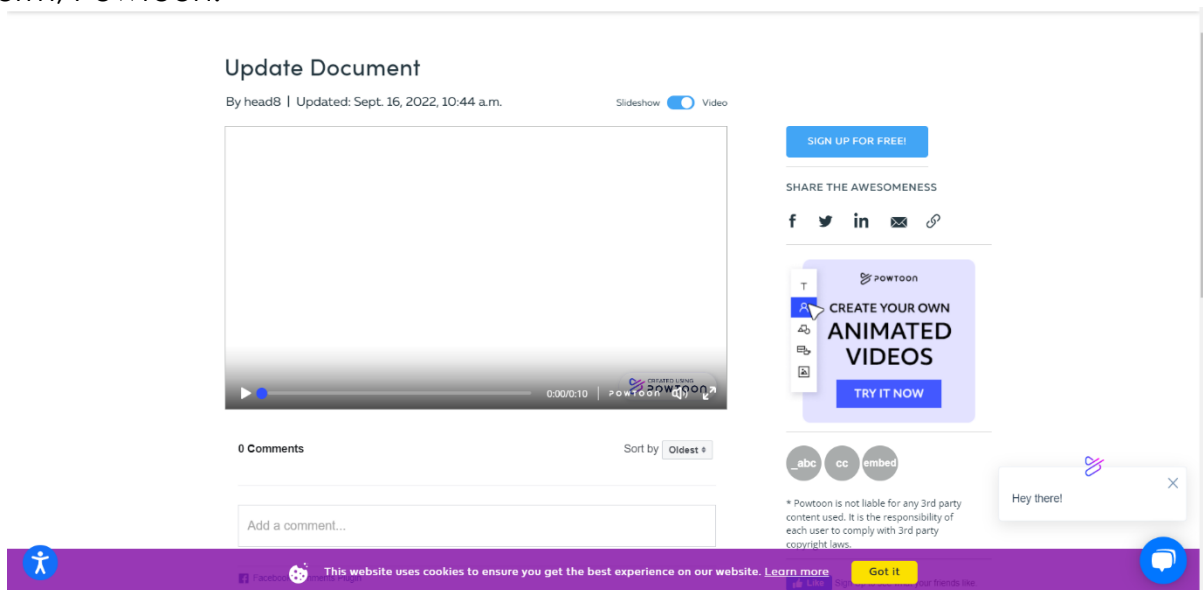


Figure 2: The video hosted on Powtoon – which has since been removed by Powtoon, after they were made aware of the attack

When played, the video displays an Outlook logo (a known brand), and prompts the user to click, to view the document.

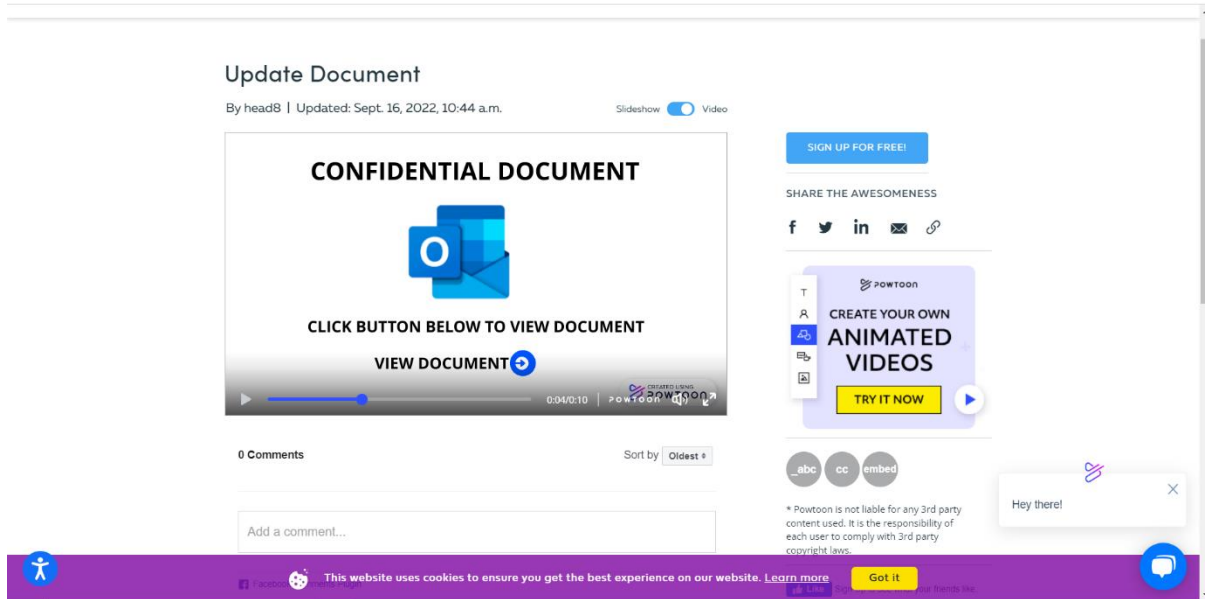


Figure 3: The Outlook logo in the video

When the user click's the second malicious payload (the malicious site that steals the users credentials) appears as an extremely accurate, spoofed Microsoft login page.

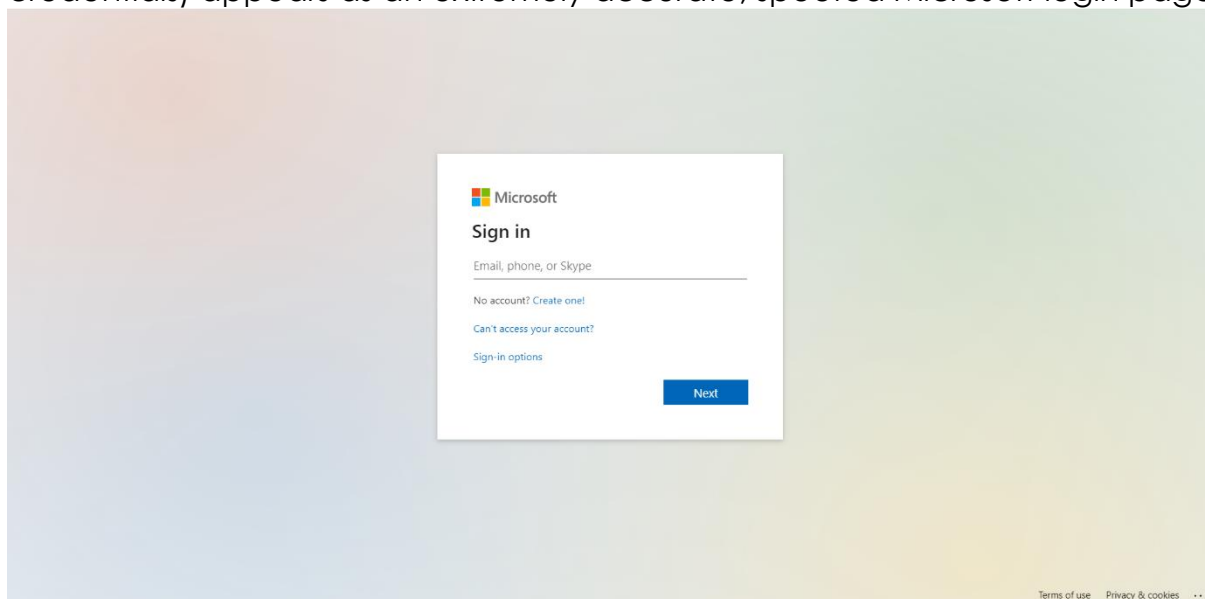


Figure 4: Spoofed Microsoft login page

Perhaps most importantly, the sender of the email is an actual person whose account had been recently compromised and taken over. From our experience, 2-step phishing attacks usually come from actual email accounts that have been compromised. It is clear that this an ATO because 1) the original email body contains the sender vendor's signature and 2) it passes SPF and is sent from Microsoft. Because 2-step phishing attacks are typically sent by compromised accounts makes this type of phishing attack all the more dangerous, especially if the recipient knows and trusts the sender.

### The bottom line

This a highly sophisticated phishing attack that involves multiple steps, ATO, video and a phishing site. Due to a similar attack that had used video to deliver a payload, and was analyzed by our IR team, threat intelligence powered the system's prevention of this attack from reaching the user's inbox.

**Remember: attackers leave patterns.** Our platform has the ability to detect those patterns and implement new detection rules based on them very quickly. Typically, however, there isn't a need to create new rules. Even when attackers sample a new technique (like using video as their payload), some part of the attack will contain a pattern our system already recognizes as malicious and knows how to prevent.

If you are interested to know more on either our workforce services or the advanced email protection solutions, we would be more than happy to drop by your office or arrange a Teams call with you to share further.

Our email contact is [xplore@xcellinkgroup.com](mailto:xplore@xcellinkgroup.com)

## Article from our SME Conference Sponsor, Fortinet

### Threat Predictions for 2023: New Attack Surfaces and Threats Emerge as Crime as Cybercrime Expands

By [FortiGuard Labs](#) | November 07, 2022

While "less is more" may be the strategy behind consolidating networks and security, "more is more" seems to be the mantra cybercriminals continue to live by.

And as we look at our threat predictions for 2023 and beyond, there is "more" at every turn. As cybercrime converges with advanced persistent threat methods, cybercriminals are finding ways to weaponize new technologies at scale to enable more disruption and destruction.

As a result, the most troubling trend we've observed across the cyber landscape this year that we anticipate will continue into the future—is that threats of all kinds are becoming increasingly ubiquitous.

From [Ransomware-as-a-Service \(RaaS\)](#) to new attacks on nontraditional targets like edge devices and virtual cities, the growing volume and variety of increasingly sophisticated cyberthreats will surely keep security teams on their toes in 2023 and beyond.

## How Our 2022 Predictions Fared (and will Evolve)

Last year we made numerous predictions about how the threat landscape would evolve—from attackers spending more effort on pre-attack activities to an increasing number of attack attempts impacting Operational Technology (OT). Unfortunately, many of those predictions did show promise. Lets look at what is coming up to help CISOs and security leaders prepare in advance.

## New Threat Trends in 2023 and Beyond

It's not surprising that cyber adversaries will continue to rely on tried-and-true attack tactics, particularly those that are easy to execute and help them achieve a quick payday. However, FortiGuard Labs predicts that several distinct new attack trends will emerge in 2023.

Here's a glimpse of several attack developments we'll be watching for in the next year:

**The Explosive Growth of CaaS:** Given cybercriminals' success with RaaS, we predict that a growing number of additional attack vectors will be made available as a service through the dark web. In addition to the sale of ransomware and other Malware-as-a-Service offerings, we'll also start to see new a-la-carte criminal solutions.

**Money Laundering Meets Machine Learning:** We also expect that money laundering will get a boost from automation. Setting up money mule recruitment campaigns has historically been a time-consuming process. We anticipate that cybercriminals will start using machine learning (ML) for recruitment targeting, helping them to identify potential mules better while reducing the time it takes to find these recruits. Over the longer term, we expect that Money Laundering-as-a-Service (LaaS) is also on the horizon, which could quickly become part of the growing CaaS portfolio.

**Deep Web Destinations Welcome a Wave Cybercrime:** And while newer online destinations like virtual cities that take advantage of augmented reality (AR), virtual reality (VR), and mixed reality (MR) technologies open a world of possibilities for users, they also open the door to an unprecedented increase in cybercrime. From virtual goods and assets that can easily be stolen to potential biometric hacking, we expect this attack surface will result in a new wave of cybercrime.

**Wipers Become Rampant:** We've already witnessed the alarming growth in the prevalence of wiper malware, but we don't expect attackers to stop there. Beyond the existing reality of threat actors combining a computer worm with wiper malware, and even ransomware for maximum impact, the concern going forward is the commoditization of wiper malware for cybercriminals. Malware that may have been developed and deployed by nation-state actors could be picked up and re-used by criminal groups and used throughout the CaaS model. Given its broader availability

combined with the right exploit, wiper malware could cause massive destruction in a short period of time given the organized nature of cybercrime today.

## Protecting Your Organization Against the Evolving Threat Landscape

While keeping up with the volume and velocity of threats can often feel like an uphill battle, the good news is that most of the tactics they're using to execute these attacks are familiar, which better positions security teams to protect against them.

Understanding the lifecycle of an attack can go a long way in helping you protect your networks—the [MITRE ATT&CK framework](#) is an excellent resource. Implementing network segmentation is also critical in protecting your organization against cybercriminals. Segmentation improves security by preventing attacks from spreading across a network and infiltrating unprotected devices. In the event of an attack, segmentation also ensures that malware can't spread into your other systems.

"Consolidation and integration into a single cybersecurity platform is crucial, especially considering the increasing ubiquity of all types of threats today, no matter your industry or the size of your organization."

Yet the most important action you can take to enhance your organization's security posture is to adopt a broad, integrated, and automated cybersecurity mesh platform. Cybersecurity defenses have traditionally been deployed one solution at a time, usually in response to an emerging challenge. But a collection of point solutions simply doesn't work in today's growing threat landscape. Consolidation and integration into a single cybersecurity platform is crucial, especially considering the increasing ubiquity of all types of threats today, no matter the industry or the size of an organization.

Using an [inline sandbox service](#) is a good starting point to protect against sophisticated ransomware and wiper malware threats. It allows real-time protection against evolving attacks because it can ensure only benign files will be delivered to endpoints if integrated with a cybersecurity platform.

Looking outside an organization for clues about future attack methods will be more important than ever, to help prepare before attacks take place. [DRP services](#) are critical for external threat surface assessments, to find and remediate security issues, and to help gain contextual insights on current and imminent threats before an attack takes place.

[Download a copy of our full predictions report for 2023.](#)

[Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.](#) [Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda \(TAA\), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program.](#)



# Article from our Corporate Partner, Yeswehack

## How we help our clients step-by-step in their Bug Bounty program

A Bug Bounty program is a crowdsourced security testing initiative that rewards ethical hackers for identifying and reporting a vulnerability in an organisation's websites, mobile applications, infrastructure and connected devices, all within a set of defined scopes and rules. In contrast to traditional security testing methods such as pentest where you are limited by the pentester's skills, it is a more holistic approach since it allows an organisation to access thousands of ethical hackers and take advantage of an unlimited pool of skills to strengthen its security testing capability.

The use of Bug Bounty programs has become commonplace around the world today, with governments and enterprises running their own programs or partnering with Bug Bounty platforms. As a global Bug Bounty platform, YesWeHack is often asked about how an organisation can set up a Bug Bounty program and how we can help and support this intricate process. For more insights, we sat down with Selim Jaafar, the Head of Customer Success at YesWeHack, to discuss how to implement a Bug Bounty program and the best practices to adopt.

Could you please explain to us quickly your role within YesWeHack?

My role is to ensure the success of our clients' Bug Bounty journey, which of course involves some technical, functional, organisational and human aspects. My team bring our expertise and experience to our clients – they often need advice and support when it comes to implementing and deploying their Bug Bounty programs.

Organisations typically have little experience and feedback on the practice of Bug Bounty. By contrast, we benefit from the experience and feedback of hundreds of organisations, with varying programs, goals, approaches and budgets. It's then easy to identify and anticipate potential pitfalls, as well as to share best practices and help clients project themselves in the Bug Bounty world. We are also close to the hunters' community, so we can answer various questions about their ethics, way of working or how to interact and collaborate with them within a Bug Bounty framework.

Also, launching a Bug Bounty program through the YesWeHack platform allows you to take advantage of a rich set of features, integrations with third-party systems, indicators and other tools at your disposal. Helping clients get to grips with the platform, get the most out of it and make the process more efficient, is naturally an essential part of our job. As such, it is necessary to question ourselves and to collect the feedback and wishes of our clients, always to improve and better meet their needs.

Simply put, our role is to allow clients, with a given budget and limited resources, to get the most out of their Bug Bounty experience while avoiding missteps. Achieving this

[back to top](#)

requires constant support: onboard clients on the platform and familiarise them with the model, then launch their first program, make it evolve, animate it and deploy Bug Bounty on a larger scale, step by step, in the long run.

Ultimately, our goal would be to help clients enable Bug Bounty adoption within their organisation.

Can you explain the main steps before the launch of a Bug Bounty program?

**1 - List the scope(s) that should be tested in the first place.** Suppose it's your first Bug Bounty program. In that case, there is a balance to find: large enough to be interesting and produce concrete results, but small enough to remain manageable. Some will prefer to test their "crown jewels" applications first while others are testing some less sensitive scopes. There is no such thing as a wrong choice here; it depends on your security objectives and resources and what you are trying to prove or improve through these first iterations.

**2 - Define and prepare testing conditions.** Black-box or Grey-box? On a production environment or a dedicated environment? How could hunters get access to the scopes? These kinds of topics often come with challenges that you'd better identify at the early stages of your project.

**Pro tip:** the more latitude you'll give to hunters, the more committed they will be, and the more exhaustive and interesting the results will be.

**3 - Delimit budget and set priorities.** The higher the budget, the better the results will be, of course. Still, you could deliver value with a minimal budget, as long as you set your priorities and focus on what matters most, either in terms of scope or type of vulnerabilities.

**4 - Identify stakeholders, distribute roles and define responsibilities.** Bug Bounty programs often involve a broad set of actors and stakeholders—mostly Devs, Secs and Ops. Make sure to identify all those with a direct role in the program and grant them the appropriate access within the platform, and thus, technically enforce roles and responsibilities for better reports management. On the other hand, it's never too soon to inform other interested parties of the upcoming Bug Bounty program and live testings.

**5 - Draft your program.** It is in the definition of your program that your means, your objectives and your constraints will crystallise, through the scopes, rewards and rules that you will set up.

**And that's it. Time for the program to go live!**

**Pro tip:** Avoid Fridays when launching a new program, if you want to enjoy your weekend.  
In your experience, what should be avoided when drafting a program?

**Ambiguity is your worst enemy.** Pay attention to how you define the scope, the qualifying vulnerabilities and the eligibility rules of your program. When doing so, don't leave too much room for interpretation (on both sides, i.e. hunters and program managers) as it could be frustrating, misleading or counter-productive if not well-bounded.

Once your objectives are clearly identified, program drafting should be a transposition of those, in terms of:

- **Scope:** what should be tested
- **Rules:** what can be done and what not while testing the scopes
- **Rewards:** what could one expect when submitting a valid in-scope report

On top of this, you may add some details about how the application works and how hunters should proceed to get onboard on the program (accounts creation, testing environment, etc.). Anything that could help hunters to work for you correctly to get the expected results, no less.

Do not overlook the details. That is why we systematically review all program creations and updates to ensure that the description meets the client's objectives and expectations. Just as we regularly enrich our program creation form and templates to guide clients through these decisive steps.

Now that the program is up and running, how do you ensure it runs smoothly?

Well, most of the job is on the hunters' side – identify vulnerabilities, and on the clients' side – fix those. But as we were saying above, we do offer personalised support to our clients, and it comes with regular status meetings, to check up on:

- Internal teams workload: how comfortable are you with the current flow of reports?
- Results vs Objectives: how relevant and useful were the last reports received?
- Opportunities for step-up or improvement: do you want to go one step further? Do you want to put more focus on one aspect?

Depending on the client's feedback and expectations, we can make some suggestions and recommendations, on where to lead the program:

- Invite more hunters
- Introduce new scopes
- Switch from black-box to grey-box
- Increase the reward grid
- “wait and see”.

At all times, we must ensure that the program remains under control (on budget, workload, fix backlog, etc.) while delivering value and meaningful results.

To maintain the program's appeal to hunters, what are the best practices?

Rather than listing what could go wrong or what to avoid, we emphasise on what to do to get the odds on your side:

- **Be fair:** try to adopt the hunters' point of view and keep in mind the time, skills and efforts they put in while working with you. Make a good-faith effort to understand and apply best practices when it comes to handling hunters' reports (e.g. is it really a duplicate?). Being fair does not mean being overly generous; it just means being fair.
- **Be transparent:** it applies to many situations and topics. Bug Bounty is a collaborative approach—the more information you share with hunters, the more involved they will be. For instance, when lowering the impact of a vulnerability, you

might have some very good reasons to do so, that the hunter will only understand if you explain those, even briefly.

- **Be interactive:** once again, that's inherent to the collaborative model: direct interactions will often help you get to the bottom of it. If not sure about your understanding of a vulnerability's impact, or its technical implications, feel free to ask. Knowledge sharing is part of the hunters' DNA.
- **Be creative:** in your rules, your tone or by setting up new challenges within the program itself; there are many ways to differentiate or to experiment through Bug Bounty.
- **Be thankful:** it's a common thing to think that hunters are only interested in bounties. Let's be honest, it's a great motivation and a legitimate expectation, considering the work and efforts. But in the long run, hunters will tend to focus on programs where they feel appreciated and useful. It's a matter of human interactions after all.

And more importantly, be cool, Bug Bounty is mostly fun!

Want to find out more about Bug Bounty and how to leverage it effectively to prevent cyber threats for your organisation? Do not hesitate to contact YesWeHack at [contact@yeswehack.com](mailto:contact@yeswehack.com) to speak to our Bug Bounty expert today!

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.*

# PROFESSIONAL DEVELOPMENT

## Listing of Courses by Wissen International

The graphic features a dark background with a person's hands typing on a laptop. Overlaid on the laptop are glowing blue wireframe boxes containing padlock icons, symbolizing security. The text is arranged in a clean, modern layout with a mix of red and white colors.

**ECDE**  
EC-Council Certified DevSecOps Engineer

**EC-Council**

**DEVSECOPS  
IMPROVES  
SECURITY,  
QUALITY AND  
RESILIENCE.**

**Build Secure  
Applications Rapidly.  
Be a DevSecOps  
professional Today**

Build & Deploy Secure  
Applications with ECDE

**Get Certified**

Become experts at building applications with both speed and security with the **EC-Council Certified DevSecOps Engineer (E|CDE) program**.

This lab-based program teaches candidates to excel with practical knowledge.

Learn to address cloud security issues and fix them directly at the source, identify security vulnerabilities at different stages of the development cycle and become proficient in leveraging innovative tools in both on-premises and cloud-native environments.

**Build your #DevSecOps career today!**

**Special discount available for AiSP members, email [aisp@wissen-intl.com](mailto:aisp@wissen-intl.com) for details!**

[back to top](#)

## 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)

*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



## COURSE DETAILS

2022 and 2023 Course dates can be found on [https://www.aisp.sg/qisp\\_training.html](https://www.aisp.sg/qisp_training.html)

Time: 9am-6pm

Fees: \$2,800 (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](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 and 2023 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: 2022 to 2023) from 1 Jan 2023 to 31 Dec 2023. 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.

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 : \$486.00 (1st 100 applicants),  
\$324 (AiSP CPP members)**

**Annual Membership: \$270.00**

\*Price includes GST

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

### Your AiSP Membership Account

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

### Membership Renewal

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







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.

## AiSP Secretariat Team



Vincent Toh  
Associate Director



Elle Ng  
Senior Executive



Karen Ong  
Executive



Jennifer Goh  
Finance & Human  
Resource Officer



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



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



+65 8878 5686 (Office Hours from 9am to 5pm)



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

Please [email](#) us for any enquiries.