

News & Update

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

Contributed Contents

- IoT SIG: Can AI provide the Wide Angle Lens Needed to Stop Cyberattacks in IoT and Cloud?
- CTI SIG: Ratings of a Cyber Security Analyst
- Wissen: How DevSecOps Addresses DevOps Industry Problems? (ECDE)
- CSIT: Judging a book by its cover – Dissecting Malware Metadata for Insights
- Image Engine: Limited Time Access to Select GovWare 2022 Top Sessions
- Mimecast Connect: Work Protected, Together
- Globalsign: 2023 Cybersecurity Predictions in APAC
- Huawei: "Raising awareness on malware threats in cyberspace among SMEs and MNCs" – Highlights of the Malware Awareness event on 6 January 2023
- TCA 2022 Winner – Ms Soffenny Yap
- SVRP 2022 Winner – Gregory Choong

Professional Development

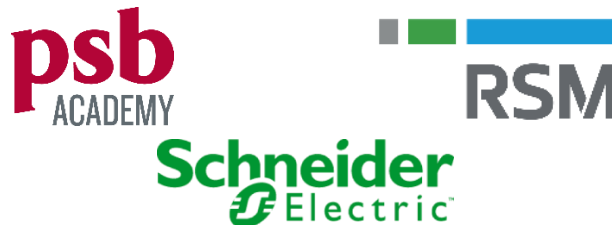
Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome PSB Academy, RSM Singapore and Schneider Electric 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 CSIT, Cyfirma, Mandiant, NetWitness and ThriveDx for their continued support in developing the cybersecurity landscape:



News & Updates

AiSP x CSCIS MOU Renewal on 20 January

On 20 January, AiSP did a MOU renewal signing with Centre for Strategic Cyberspace + International Studies (CSCIS). Through the MOU, AiSP will continue to work together with CSCIS such as collaborating with our special interest groups for Cloud Security, IoT and CTI and cross support each Association Events. Thank you everyone for taking time to join us at the occasion.




Annual General Meeting

AiSP cordially invites all AVIP, Fellows and Ordinary members to the Annual General Meeting which will be held on 30 March, 7pm. Details and agenda will be sent to all ordinary members in March.

AiSP
Advance Connect Excel

**ANNUAL
GENERAL
MEETING**

30 MARCH 2023 | 7PM

6 Raffles Blvd 
#03-308
Justco@Marina Square
Singapore 039594,
Event Space

**FOR AVIP, FELLOWS AND ORDINARY
MEMBERS ONLY**

We would appreciate if you could confirm your attendance [here](#) latest by **5:00 PM, 16 March 2023**

Knowledge Series Events

Software Security on 18 January

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.

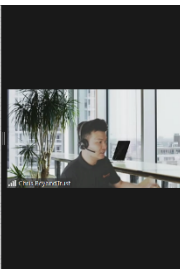
On 18 January, AiSP had our Knowledge Series focusing on Software Security. Our Corporate Partners, BeyondTrust and Parasoft shared insights on Software Security. Thank you Chris Lee and Steve Neo for sharing and AiSP Vice-President Tony Low for the opening address.

Challenges With Traditional Endpoint Security

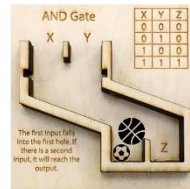
These factors leave organizations at risk of being 'left behind' when it comes to endpoint security:

- Continually evolving and more advanced cyber threats
- Increasingly complex and diverse endpoint environments
- Corporate misalignment of security technologies to threats
- Resource challenged IT and InfoSec teams that continue to be stretched thin

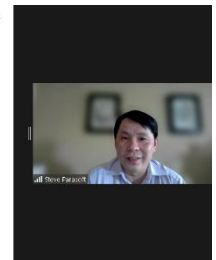
350,000 pieces of new malware are detected every day



Output of DevSecOps is TRUST



X is Application Security
Y is Application Quality
Z is Trust



Strategic Thrusts, that anchor our vision

Vision: A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem.
Mission: Pillar for the Information Security Profession and Professionals in Singapore

Strategic Goals	Achieved Sustainability	Increased Collaboration	Increased Recognition
	Advance	Connect	Excel
Strategic Thrusts	<ul style="list-style-type: none"> Innovation Knowledge Series Specialization Certifications Special Interest Groups 	<ul style="list-style-type: none"> Regional Ecosystem Local Ecosystem Corporate Partners Academics Partners Leaders in Cyber Cybersecurity Awareness & Advisory Program 	<ul style="list-style-type: none"> AISP Validated Security Professionals (AViSP) Cyber Security Awards Student Volunteer Recognition Program (SVP)

MEMBERS | CONNECT | EXCEL

Upcoming Knowledge Series

Data & Privacy on 22 February



AiSP Knowledge Series – Data & Privacy

Organised by



Supported by




In support of



DATA & PRIVACY

AiSP Knowledge Series

22 FEB 2023 | 3PM - 5PM

JUSTCO @ MARINA SQUARE

REGISTER NOW





Wong Onn Chee
Data & Privacy SIG
Lead
AiSP



Shaun Chen
Director, Sales
Engineering, APAC,
Thales CPL



Alvin Tan
Chief Marketing Officer
& Head of International
Operations, Straits
Interactive



Trina Swee
Data Protection Officer
Group Legal and
Compliance, DBS Bank



Dominic Ng
Manager, Data
Innovation &
Protection Group,
IMDA



Hoi Wai Khin
Data & Privacy SIG
Member, AiSP
TCA22 Winner
Leader Category

In this Knowledge Series, we are excited to have Thales and IMDA to share with us insights on Data & Privacy. 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.

Updates on Singapore’s Personal Data Protection Act
Speaker: Alvin Toh, Chief Marketing Officer & Head of International Operations, Straits Interactive

As businesses recover and ride on the accelerated wave of digitalisation, there is a growing awareness of the importance of data and the potential in harnessing these data for business insights, innovation and growth. Find out how the Enhanced PDPA strengthens personal data protection whilst enabling businesses to innovate in the data-fuelled environment, and how IMDA’s data protection initiatives can help your company strengthen consumer & regulator trust and increase your competitive advantage in the digital economy.

Ensuring Data Privacy in a Multi-Cloud Environment
Speaker: Shaun Chen, Director, Sales Engineering, APAC, Thales CPL

As more businesses today pivot towards a multi-cloud environment for flexibility, data security and privacy has become a crucial component. With proprietary information and sensitive data kept in cyberspace, organisations need to ensure their cloud environment is airtight right from the start.

Whatever your multi-cloud strategy is, the key lies in creating a trusted space where data is properly encrypted and authenticated. Beyond security, organisations should also maintain complete control and access over their own digital assets and operations without worrying about data breaches.

In this session, we'll explore the concerns around data privacy and digital sovereignty in a multi-cloud environment, both in the public and private sector, and how your organisation can implement the tools necessary to keep information secure.

Panel Discussion: DPTM - the Good, the Bad and the Future

Moderator: Wong Onn Chee, Data & Privacy SIG Lead, AiSP

Panellists:

Shaun Chen, Director, Sales Engineering, APAC, Thales CPL

Alvin Tan, Chief Marketing Officer & Head of International Operations, Straits Interactive

Trina Swee, Data Protection Officer, Group Legal and Compliance, DBS Bank

Dominic Ng, Manager, Data Innovation & Protection Group, IMDA

Hoi Wai Khin, Data & Privacy SIG Member, AiSP & TCA 22 Winner – Leader Category

DPTM - Data Protection Trust Mark - was launched by IMDA in 2019 and as of 6 Jan 2023, 135 entities are certified. A DPTM certification has the following benefits:

1. Demonstrate accountability to your customers, business partners and regulator that your organisation adopts responsible data protection practices to manage personal data.
2. Serve as a mitigating factor against enforcement action in the event of a data breach. In addition, under the PDPC's Active Enforcement Framework, the PDPC and/or the DPTM-certified organisation that is able to demonstrate accountable data protection practices, may initiate an undertaking process.

Come and hear from a DPTM organisation on their journey towards DPTM certification. And hear from other industry practitioners on what are the common areas to take note in your pursuit of DPTM. PDPC will also share with us on the future plans and directions for DPTM.

Date: 22 February 2023, Wednesday

Time: 3PM – 5PM

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

Registration: <https://forms.office.com/r/Nw8VU6LNQU>

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

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. Data & Privacy, 22 Feb
2. Cloud Security, 12 Apr
3. Cyber Defence, 25 May
4. Operations & Infrastructure Security, 19 Jul

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 2023 on 6 January

In collaboration with our Corporate Partners, Huawei Singapore, Cyber Security Agency of Singapore - CSA and Wizlynx group, AiSP organised the Malware Awareness 2023 where our speakers shared insights on Malware. AiSP would like to thank Mr Dennis Chan, Mr Yum Shoen Yih, Mr Jeffery Zhang and Mr Wong Yong Wah for sharing insights at the event.



A Practical Approach in Building Security Resilience in Zero Trust on 18 January

On 18 January, in collaboration with our Corporate Partner, Cisco, AiSP organised an event on "A Practical Approach in Building Security Resilience in Zero Trust". AiSP would like to thank Mr Koo Juan Huat, Mr Yum Shoen Yih, Mr Alan Goh, Mr Josh McCloud, Mr David Ong, Mr Chetan RaghuPrasad and Mr Jeff Yeo for sharing insights.



Student Volunteer Recognition Programme (SVRP)

School Talk at Bukit Panjang Government High School on 9 January

As part of Digital for Life Movement, AiSP conducted a school talk to more than 40 graduating students of Bukit Panjang Government High School. AiSP Secretary and SVRP Lead, Ms Soffenny Yap shared insights on Cybersecurity awareness and Careers Opportunities in Cybersecurity to the students.






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 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 for more details

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 more video content.



To find out more about the Digital for Life movement and how you can contribute, scan here.

Contact AiSP Secretariat at secretariat@aisp.sg to find out more on how you can be involved or if you have any queries.

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



Ladies in Cybersecurity



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.

Save the date

8 Mar 23: AiSP International Women Day Celebrations at SIT @ NYP.

18 Mar 23: AiSP Ladies in Cyber Symposium at Capital Tower Level 9

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

Internet of Things Networking + Lo Hei session on 31 January

On 31 January, Internet of Things Special Interest Group (SIG) had our networking + Lo hei session with our SIG members. AiSP would like to thank everyone who came down to join us for the session.

For more collaborations with our IoT SIG, please contact secretariat@aisp.sg



AiSP has set up four **Special Interest Groups (SIGs)** for active AiSP members to advance their knowledge and contribute to the ecosystem are:

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

We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together. If you are keen to be part of a SIG, please contact secretariat@aisp.sg



The Cybersecurity Awards



The Cybersecurity Awards 2023 nominations will start on 06 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) if your organisation would like to be our sponsors for The Cybersecurity Awards 2023! Limited sponsorship packages are available.

TCA2023 Sponsors & Partners



Organised by



Supported 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

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
3 Feb	CNY Lo Hei	AiSP
8 Feb	i-4 ASPAC Regional Meeting	Partner
12 Feb	Celebrate Digital festival for Nee Soon Link residents	AiSP & Partner
15 Feb	The Rise Of Ransomware Attacks: Protect, Defend, Respond	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
1-3 Mar	XCION in Bali	Partner
1 Mar	HPC Cybersecurity Workshop at SCA2023	Partner
2 Mar	Mimecast Connect Event	Partner
7 Mar	Event with YesWeHack	AiSP & Partner
8 Mar	International Women Day Celebration @ SIT@NYP	AiSP & Partner
9 Mar	Threats have evolved. So must your Privileged Access Management.	AiSP & Partner
11 Mar	Celebrate Digital @ Bukit Bangkit	AiSP & Partner

[back to top](#)

13-15 Mar	Inter Poly CTF	Partner
18 Mar	Ladies in Cyber Symposium	AiSP
30 Mar	Annual General Meeting	AiSP
30 Mar – 1 Apr	CYSummit	Partner

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

CONTRIBUTED CONTENTS

Article from IoT SIG



Can AI provide the Wide Angle Lens Needed to Stop Cyberattacks in IoT and Cloud?

Chris Fisher
Director, Security Engineering, Asia Pacific & Japan
Vectra AI Inc.

IoT has become a normal way of life for many people, we interact with these devices on a daily basis from doorbells to lights, cameras to building locks. IoT devices have become so prolific that most times we take them for granted. However, as commonplace as they've become, we've also seen the challenges in securing IoT devices—from massive armies of botnets used for DDOS activity, to being used for command and control in sophisticated attacks as a means to evade modern endpoint security controls. We have even seen some financial sectors suffer large data breaches where IoT offered a means to infiltrate the environment and exfiltrate data.

What makes IoT such a challenge to secure? Well, there are several factors at play ranging from hardware to network—and more importantly to cloud. Almost all IoT devices connect back to cloud services in some way, from consumer through to enterprise IoT devices—connecting to the cloud has become a vital means to operate. And similar to the security challenges present in OT networks, it is almost impossible to embed security agents within every IoT device. Additionally, these devices will typically run operating systems and software that is cheap to build, while tight margins can lead to solutions that run vulnerable code that is difficult to patch. Without the ability to place tight controls on the endpoint, we now look to network monitoring and cloud security to help close the gap.

[back to top](#)

Network monitoring within enterprise-grade IoT is an effective way to identify attacker behaviour, however, with all of these services connecting to cloud-based infrastructure—it is vital that we also secure the cloud as an attack surface. Cloud security is something that a lot of organisations have been grappling with as it's large, complex, and constantly changing. Adding to the complexity is that each provider does things a little different. And keep in mind that the cloud is made up of multiple core components—IaaS, PaaS and SaaS. IaaS lends itself to some of our traditional based security controls, SaaS is the newest category of security products, while PaaS is a key challenge as a large attack surface. Adding to this challenge is that we tend to look at all three in isolation from a security perspective, which can lead to blind spots that allow attackers to move laterally without detection. Effectively allowing attackers to move from IoT devices to the control plane of the cloud provider with almost no way to track lateral movement is a recipe for disaster.

To overcome the challenges presented by IoT and cloud, we need shift our thinking away from prevention and turn to detection. While we should still make entry as difficult as possible for attackers, prevention shouldn't come at the expense of detection. However, threat detection at this scale will require a modern approach. If we simply focus on vulnerabilities and malware, we will be forever playing catch up to the attackers. Instead, we need to focus higher up the value chain and look at the attacker behaviour. To identify behaviour, we need to look at solutions that will provide high-fidelity detections that leverage AI and machine learning to ensure signal clarity is provided without the false positives of signature-based detections. In addition, we need to look at solutions that will bring together all events on the network, IaaS, PaaS and SaaS environments so we can identify lateral movement without blind spots, but also ensure that these events are correlated and prioritised to the highest risk entities—be that user accounts, roles or hosts. Once this view achieved, then and only then will we be able to focus on how to detect, respond and most importantly—stop any attacks that enter or move across the environment.

For any further enquiries, please contact Ms Katherine Toh at ktoh@vectra.ai

Article from Cyber Threat Intelligence SIG

Rantings of a Cyber Security Analyst

It is 2023, a brand-new year. Firstly, I would like to wish everyone a successful year ahead and, hopefully, a year where everyone upgrades their security and is better protected.

Based on what I am seeing, the threat landscape for this year will be the same, with ransomware groups being the very active. This is unfortunate, as it is still a very effective attack with profitable gains and high success rates.

The general tactics are still the same, where threat actors search for exposed and vulnerable systems as their entry points. However, it is to be noted that the techniques have been refined, as threat actors use various hands-on keyboard methods, legitimate tools and even drivers signed with stolen, legitimate digital certificates. And they are really good at these, with comprehensive understanding of different command lines and actions that can be performed with this limited initial access.

Prior to the holiday season, I have been warning customers about signs of attempts to breach into public facing servers running vulnerable builds of MSSQL. Yes, the same threat that I have been talking about since 2022 July. There are even situations where I identified compromised administrator accounts using just the high-level telemetry data I have, without any access into complex XDR tools. It is unfortunate as the consoles of these customers actually provided this information and more. It is just because no one logged into these consoles to check.

Unfortunately, some of these warnings fell on deaf ears and eventually escalated into a ransomware attack.

There seems to be a failure to understand that even if the security solution blocks an exploitation attempt on a public facing server, there is still risk involved. Threat actors, as I have seen, are not that easily dissuaded by this. Even if the exploit failed, this informs the threat actor that there is a public facing server with MSSQL on it. The common next behaviors I see are attempts to directly log into the MSSQL service, through brute force of the "sa" account or attempting to identify other services that are open on the server, such as RDP. In this case here, I would say the vulnerability acted as a beacon for the threat actors, flagging out potential targets for them to poke around for weaknesses that they could exploit. A single password that "defends" against unauthorized entry is the weakest form of protection.

In a previous article, I mentioned about the concept of 5 Ws 1 H. This should be applied at this time. Questions on why is this server public facing, what services are accessible from public and so on. Identification of all these helps to identify the risks. Again, in most cases, the initial detections, even if mitigated by the security solution, that trigger should have already started an investigation.

My wish for 2023 would be for organisations to admit there is lacking in security knowledge and capabilities in majority of environments. Executive levels need to acknowledge there is a real need, regardless of company size, to incorporate some form of security expertise, not products, into their strategic planning.

IT staff need to acknowledge that they do not have the skillsets to protect the environment. Knowing how to install security products does not make anyone a security personnel.

Tough questions needs to be asked, such as what risks the company faces with these assets (There is no such thing as zero risk) and what are the strategies to reduce these risks.

Question if the team has any remediation plans for the various scenarios. It is fine to admit the lack of such capabilities, but it is important to acknowledge these gaps and for the executive leadership to allocate budgets to either hire such skillsets or have them outsourced.

The idea of "set and forget" security no longer applies. Adoption of AI helps to reduce the "heavy lifting" but is not a silver bullet against all forms of attacks. Security teams need to be updated on the latest trends of attacks and methods threat actors use to overcome security controls.

Have you heard of aswarpot.sys or mhyprot2.sys? How about Huorong Sword? These are legitimate drivers and software used by threat actors to disable existing security controls. We still see them in use, but they may get phased out by the adversaries as more methods of detecting these abused drivers and applications become available.

So, for 2023, the new year resolution for business executives should be to include security into their strategic business planning. For those who are keen and have strong interest in security, I encourage you to take up courses and read up more from open sources of attack trends and methods. Be curious and ask questions. This would be the perfect basis to start your journey as a security personnel.



Harvey Goh is a cyber security specialist having been in the cyber security industry for over 15 years as a technical personnel. Currently he is working as part of Sophos' Managed Detection & Response team and is a Certified Threat Intelligence Analyst. 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 Corporate Partner, Wissen International

How DevSecOps Addresses DevOps Industry Problems? (ECDE)

There are several inherent problems in the DevOps industry that need to be addressed. Automation has caused a massive skills gap, backlogs of work, and reliance on manual processes, especially in application security. DevSecOps is a solution to these problems. It incorporates security into the automated process, closes the skill gap, and eliminates the need for manual processes. This makes DevOps more efficient and secure, solving many of the industry's common problems.

What Is DevSecOps?

DevOps is a set of practices that combines software development (Dev) and information-technology operations (Ops) to shorten the time it takes to deliver applications and services. It aims at establishing a culture and environment where building, testing, and releasing software can happen rapidly, frequently, and more reliably.

The term DevSecOps refers to a type of DevOps that emphasizes security. In a DevSecOps model, security is integrated into every stage of the software development process, from coding and testing to deployment and operations. The goal is to make security an integral part of the culture and practice of DevOps rather than treating it as an afterthought.

What Are the Main Problems Faced by the DevOps Industry?

There are many problems that the DevOps industry is currently facing. Here are some of the most prominent:

- **Overcoming the dev versus ops mentality:** One of the main problems faced by the DevOps industry is the lack of understanding and cooperation between developers and operations teams. This can lead to siloed workflows, which often lead to delays and errors in delivering software updates.
- **Common understanding of Continuous Delivery practices:** Another problem faced by DevOps teams is a lack of common understanding of Continuous Delivery practices. This can lead to confusion and frustration when trying to implement or use these practices.
- **Moving from legacy infrastructure & architecture to microservices:** DevOps teams face another challenge: moving from legacy infrastructure and architecture to

microservices. This can be a difficult and time-consuming process, but it is necessary to improve efficiency and scale

- Implementing a test automation strategy: One of the most important aspects of DevOps is implementing a comprehensive test automation strategy. This can be difficult, but it is essential to ensure quality and avoid errors.
- Too much focus on tools: One of the final problems that DevOps teams face is a focus on too many tools. This can lead to confusion and a lack of productivity as teams try to use all the tools available instead of focusing on the task at hand. (Contino, 2017)

Why Security in DevOps Is Important

As DevOps gains popularity, more businesses are adopting the methodology to streamline their software development and delivery processes. However, many organizations fail to realize the importance of security during all stages of the DevOps lifecycle.

Security is often an afterthought in DevOps, but it is critical to consider security at every stage of the process, from planning and development through testing, delivery, and deployment. By incorporating security into all aspects of DevOps, businesses can improve their overall security posture and better protect their applications and data.

There are several reasons why security must be a priority in DevOps:

1. Rapid software development cycles can leave vulnerabilities unaddressed.
2. Automation can introduce new security risks.
3. Developers and operations teams must work together to address security concerns.
4. Good security practices can improve software quality.
5. Security must be part of the culture to be effective.

Organizations prioritizing security in their DevOps initiatives will be better equipped to protect their applications and data from threats. By taking a comprehensive approach to security, businesses can improve their overall security posture and better defend against attacks.

How DevSecOps Can Address DevOps Industry Issues

As with any new and popular technology, there are always some bumps in the road. DevOps is no different.

Security is one of the biggest issues facing the DevOps industry today. With so much emphasis on speed and agility, security often gets left by the wayside. This can lead to critical vulnerabilities that hackers can exploit. By integrating security into the DevOps process, organizations can help ensure that their applications are secure from end to end.

There are many different ways to implement DevSecOps, but some common practices include security testing, automated security scanning, and secure code reviews. By

taking these steps, organizations can help ensure that their applications are secure and compliant with industry regulations.

If you're looking to get started with DevSecOps, you should keep a few things in mind.

- First, it's important to clearly understand the security risks your organization faces. Once you have a good grasp of the risks, you can start to put together a plan to mitigate them.
- Next, you need to choose the right tools and technologies for your organization. There are a number of different DevSecOps platforms and tools available, so it's important to select the ones that best fit your needs.
- Finally, you need to build a strong culture of security within your organization. This includes educating your team about DevSecOps and its importance, as well as creating policies and procedures that ensure everyone is working towards the same goal. (BeyondTrust, 2022)

By following these best practices, you can help your organization start on the path to DevSecOps success. Security has always been an afterthought in most organizations. With the increasing number of cyber-attacks, it has become more important than ever to have security integrated into all aspects of software development.

DevSecOps ensures that our applications are not only fast and reliable but also secure. The DevSecOps methodology has already been adopted by some of the largest companies in the world, and it will soon become the standard for software development across all industries.

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 for details!

Sources

BeyondTrust. (2022, September 22) DevOps Security Best Practices.

Www.beyondtrust.com. <https://www.beyondtrust.com/blog/entry/devops-security-best-practices>

Contino. (2017, February 13). 5 Challenges to DevOps Adoption and How to Overcome Them. Contino. <https://www.contino.io/insights/5-challenges-to-devops-adoption-and-how-to-overcome-them>

Article from our Corporate Partner, CSIT

Judging a book by its cover – Dissecting Malware Metadata for Insights

A book is made up of pages of information, and a book cover describes what the book is about. Similarly, malware contains information that is represented as bits and bytes, and akin to a book cover, metadata describes the contents of the malware. And just like books of the same series, a set of malware determined to have significant code overlaps is known as a malware family. As malware from the same family commonly share the same author, they may exhibit similar fragments of the author's techniques and quirks.

Unlike authors of books who identify themselves readily, malware authors do not typically identify themselves within the malware to avoid being pinpointed. Narrowing down the authorship of a malware helps analysts to derive strategic and operational insights. This allows us to better understand threat trends and develop techniques for thwarting future similar malware. This process of uncovering the provenance is called [Malware Authorship Attribution](#).

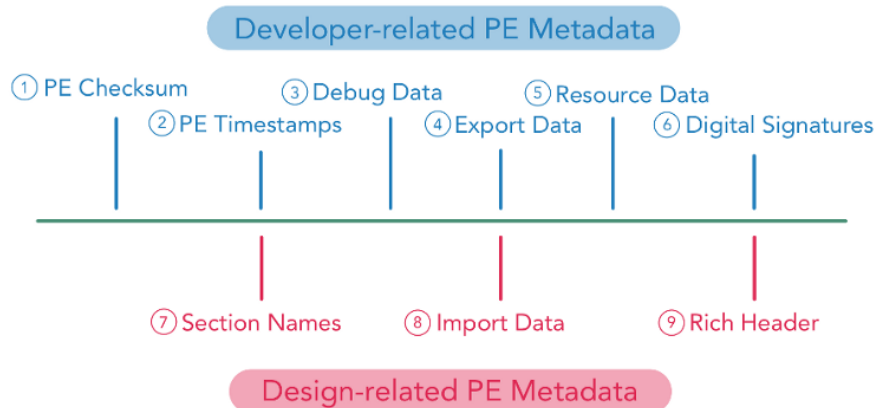
As part of our work in CSIT, we conduct continuous research to study state-of-the-art techniques used by threat actors and analyse malware to understand its evolution. This enables us to craft effective signatures against them and hypothesise the identification of threat actors.

Malware (PE) metadata – Looking at the “book cover” of a malware

Metadata is a static property, found in both Header and Sections of PE files, that can be analysed safely without executing the files. Traits found in PE Metadata can often be drawn upon to help analysts detect and attribute malware. But how?

Since humans are creatures of habit and habits tend to persist, unique styles and techniques of malware authors tend to exhibit themselves and persist in their malware. These patterns may appear in the metadata or the content of the malware. For this article, we will be focusing on the metadata. Malware metadata can be broadly categorised into two categories as follows:

1. **Developer-related PE metadata:** details that may reveal attributes of the author
2. **Design-related PE metadata:** intrinsic properties of the malware that contain traits of its code bases and development environments



Developer-related PE metadata can be understood as fragments of human (authors) habits or carelessness that can be regarded as “fingerprints” and author-specific malware traits. On the other hand, Design-related PE Metadata contains properties intrinsic to the design and the development environment of the malware that can be used to identify similar code bases, build environments, and even its family lineage. Hence, PE metadata is one type of information found in malware that can be valuable as analysts may be able to identify characteristics of the malware author and craft detection rules.

Let’s check out one of the more interesting PE Metadata from each category that help malware analysts derive meaningful insights from malware samples.

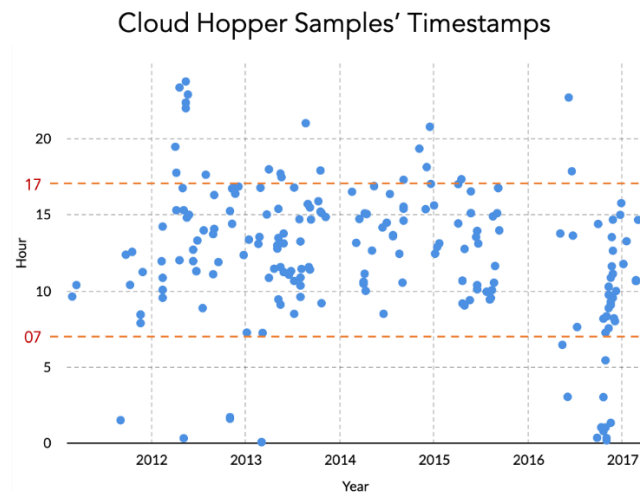
PE Timestamps – Are you in the zone?

Timestamps in PE files represent their (possible) compilation datetime. Analysts look for timestamps in the File Header and corroborate this information with the additional timestamps that can be found in several other directories in the PE file.

Malware authors may attempt to forge timestamps to hide the true creation date and time of the malware. While analysts may find it difficult to deduce the original timestamp from a forged one, we may still be able to find inconsistencies that suggest its invalidity.

Other than spotting such mistakes, timestamp values may reveal faint links to its author. Interestingly, malware authors do have work schedules, just like how some of us have a 9-to-5, 5-day work-week. This means that malware would likely be compiled at dates and times that correspond to the malware authors’ work periods.

With a substantial number of samples, we may be able to make some interesting observations. Statistical methods can be applied to determine the malware authors’ patterns of life. Malware families from the [Cloud Hopper](#) campaign is one such example.



Probable Cloud Hopper authors' work schedules

From the illustration above, we can deduce that most Cloud Hopper samples statistically have compilation timestamps between 7:14am and 5:03pm. By observing which time zones they fall under, we may be one step closer to understanding the operation times of the authors. But be aware: even though PE timestamps is a valuable forensic artifact, they can also be forged with ease. Thus, it needs to be corroborated with other PE metadata.

Rich Header – The “Rich”-est information indeed!

The Rich Header has been part of the PE file format since the release of Visual Studio 1997 SP3. It contains information such as the compiler, linker, imports that were used in the compilation, and a brief description of the overall structure of the PE file. However, till today, no introduction or documentation has been released by Microsoft, and it remains a mystery “treasure box”. In an extracted RICH header, information such as

1. Estimated number of files and imports that were used in the development project;
2. Indication of the existence of data directories in the PE file – Export and Resource
3. Derivation of the most “probable” compilation timestamp, inferred by comparing the release dates of the compiler and linker

Hence, the Rich Header entries, when placed together, can be considered relatively unique to a project as they can remain unchanged for weeks or even months throughout its development cycle. [An extensive research study by SANS](#) examined the effectiveness of using Rich header for malware detection and linking. In the paper, two PE files with identical or similar Rich Header entries (plausibly different versions of the same project) can be identified to be built from the same environment.

While it is possible to modify a Rich Header, it is much more difficult to forge a realistic one and still maintain consistency with other parts of the PE metadata. This difficulty can be seen in one of the “[most deceptive hacks in history](#)”, the [Olympic Destroyer](#) case in 2018, where the Rich Header was deliberately modified to mask its provenance and cause misattribution. In the article, analysts could determine that the malware was built using Visual Studio 6.0 from its Rich header. However, when the information was compared

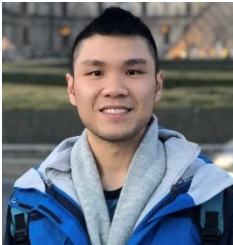
against the other parts of the PE file, it appeared to be importing functions from a library (mscoree.dll) that did not even exist at that point in time!

The Rich Header forgery ultimately resulted in an inconsistency between the Rich Header and the other components of the malware. This triggered the suspicions of analysts, who went on to expose the malware author's intent of imitating other threat groups' samples. Indeed, the act of modifying the Rich Header convincingly is not easy, and may instead become an indicator used to reveal the malware's true colours. Hence, looking out for such inconsistencies can potentially assist us in performing attribution more accurately.

Conclusion

Today, malware metadata remains as one of the keys in helping analysts derive meaningful insights. At CSIT, we have developed in-house malware analysis systems to harness malware metadata as an analytical pivot to cluster malware campaigns and families in understanding malware evolution, crafting detection rules and correlating malware of the same families. This is just a quick introduction into the exciting adventure of malware metadata analysis. We caught a glimpse of how the insights from PE metadata can help us detect malware, attribute to its source, and understand its evolution. If you are keen to find out more about metadata insights and the application of machine learning techniques to cluster malware at scale, you can visit the full article at our CSIT Tech Blog: [Part 1 – Dissecting Malware Metadata for insights](#) and [Part 2 – Analysing Malware Metadata at Scale](#).

For further enquiries, we can be reached at connect@csit.gov.sg.



Chase Tiong is a cybersecurity engineer at CSIT. He designs and implements creative solutions to counter sophisticated cyber threats and collaborate with cross-domain experts to strengthen the security of digital systems.

Article from our Corporate Partner, Image Engine

Limited Time Access to Select GovWare 2022 Top Sessions

The graphic features the GovWare logo in the top left corner. The main text reads: "LIMITED TIME ONLY! ACCESS EXPERT-LED CONTENT FROM SOME OF GOVWARE 2022'S TOP SESSIONS ON-DEMAND". Below this, it says: "Sign up for your complimentary access and watch these select sessions online anytime, anywhere! Only until 28 February 2023." A blue button at the bottom left says "GET ACCESS NOW". On the right, under the heading "Hear from these speakers and more!", there are four speaker portraits with their names and titles: Bryan Palma (Chief Executive Officer, Trellix), Juliette Wilcox CMG (Cyber Security Ambassador, UK Defence and Security Exports, Department for International Trade), Goh Eng Choon (President, Cyber, ST Engineering), and John Suffolk (President and Global Cyber Security & Privacy Officer, Huawei).

Don't miss out on this opportunity to learn from cybersecurity experts and leaders and stay ahead in the field! From now until 28 February 2023, we are offering exclusive on-demand access to some of the top keynotes and track sessions from the recent GovWare Conference and Exhibition. Over 10,000 attendees from across 65 countries have garnered new insights and ideas to enhance their strategies for the new year. You can too! **[Sign up now here](#)** to get your complimentary access.

Article from our Corporate Partner, Mimecast

Mimecast Connect: Work Protected, Together



We are excited to announce that Mimecast APAC Connect is coming to Singapore for the first time in early 2023! Live and in-person, as well as a live-stream option. With more reasons than ever to lock it into your calendar right now.

<https://mimecastconnect2023.splashthat.com/AiSP>

Article from our SEACC Sponsor, Globalsign

2023 Cybersecurity Predictions in APAC



APAC has become a focus of cyberattacks in recent years. While cybersecurity technologies are continuously upgrading, cyberattacks are also becoming more prevalent in the region. In fact, [IBM and Checkpoint have reported that APAC has experienced the most cyberattacks in both 2021 and 2022](#), attributed to the rapid digitalisation in the region combined with the low cybersecurity awareness and regulations present.

What is in store for 2023? [Our experts predict seven \(7\) emerging trends:](#)

1. Growth in digital signatures expected with eIDAS 2.0 (electronic Identification, Authentication, and Trust Services)
2. New regulations and legislations to emerge, such as PSD3 (Third Payment Services Directive)
3. Email remains strong as ever
4. Perception of the CA (Certificate Authority) market to change
5. A renewed focus on identity authentication
6. Deployment of MFA (Multi-Factor Authentication) to grow
7. Adoption of automated tools to rise

1. Growth in digital signatures expected with eIDAS 2.0

The global [digital signature](#) market is growing at a staggering rate and as more conversations evolve around the potential changes [eIDAS](#) 2.0 could bring to the market, the momentum is only going to grow.

The prevalence of remote work coupled with the globalisation of business processes has increased the need for document security. Nowadays, documents are being transmitted online or through cloud-based systems, exposing information to the risk of potential breaches. The eIDAS regulation aims to reduce this risk through setting authentication requirements.

Since it was established in 2014, eIDAS has set a common framework for identity verification in the European digital space. With the evolving market and advancing business processes, eIDAS 2.0 was developed with hopes to create the means for a unified and secure identification service that can offer authentication through certification schemes. The new regulation will also expand authentication in all public and business services. Hence, [the need for certificate-based authentication through digital signatures will grow](#).

Despite being an EU regulation, eIDAS 2.0 also has a significant impact in APAC. As European countries adopt more stringent policies surrounding authentication, APAC countries handling cross-border documents are also expected to comply with the regulation. As a result, increased demand for digital signatures as one of the most secure means to authenticate one's identity follows.

2. New regulations and legislations to emerge



Digital connection in APAC is stronger than ever. In 2020, Global System for Mobile Communications Association (GSMA) reported that more than 1.2 billion people in APAC are connected to the internet, with the number of mobile phone users consistently rising. Similarly, the Internet of Things (IoT) market in the region is significantly expanding - projected to reach US\$14.7 billion in 2027. This growth is driven by the increasing connectivity and smart automation. It is in line with Industry 4.0, which is the fourth wave associated with “automation, data exchange, digital technology, artificial intelligence (AI) and machine learning, and the Internet of Things (IoT).”

For APAC, Industry 4.0 is characterised by the creation of new industries, rise of smart devices, and the growing demand for industrial robotics that call for new regulations and legislations around the use and security of these devices. Governments have started rolling out guidelines on this phenomenon. For instance, [Singapore has issued improved rules about labeling](#). The legislation focuses on multi-level labeling schemes for IoT devices to improve security. Threat sharing in the IoT space is also becoming a trend for the region, hence the need to coordinate with the rest of the world to monitor and prepare for threats, while also enhancing risk analysing capabilities.

3. Email remains strong as ever

"Email will be gone in the next five years," said our expert [Andreas Brix](#) in 2018. True enough, there have been changes in the way we communicate, with messaging services and apps simply proliferating further in the business world. But where does this leave email?

It turns out there are at least [4 billion daily email users](#). After 50 years of usage, we head into 2023 with electronic mail staying strong as one of the few communication standards for reliably exchanging information worldwide.

As most transactions and communications in APAC are predicted to happen through email, organisations must strengthen security measures in sending and receiving emails. The use of Secure/Multipurpose Internet Mail Extensions (S/MIME) will help APAC businesses ensure the security of this communication channel through encryption and digital signature technologies. S/MIME guarantees that information in any email exchange is not compromised through transmission, while also authenticating the identity of the sender, the non-repudiation of the signature, and the integrity of sensitive data.

4. Perception of the CA market to change



We mentioned at the very beginning of this article that conversations around cybersecurity were intensifying. In years past, organisations would implement rudimentary security software that required little oversight. Today, the situation is vastly different.

In 2023, we can expect to see a two-fold increase in security awareness, as well as products utilising Public Key Infrastructure (PKI) as well as the broad-based cloud security. This surge is especially imminent in developing markets like APAC and African countries as compared to their Western counterparts.

Given the increase in internet attacks in APAC, coupled with the continuous growth and depth of internet services, the region is forecasted to exhibit the [highest Compound Annual Growth Rate \(CAGR\) in the CA market for the period 2020-2030](#). Many companies, especially those in ecommerce and financial technology, will obtain digital certificates from CAs to meet the growing demand for online security. As a future-proof CA,

GlobalSign commits to constantly investing in different technologies and infrastructure. Our latest 7.5 version of Auto Enrollment Gateway (AEG) is one such platform which boasts improved capability beyond the automated feature of enrollment, provision, and installation of certificates - providing identity for an organisation's plethora of devices.

5. A renewed focus on identity authentication



Identity security is known to be the cornerstone of the new digital economy, especially for APAC countries. As the region continues to invest in technology and innovation for industries like ecommerce and fintech, it is unsurprising that Southeast Asia's internet economy is expected to reach US\$1 trillion by 2030. While the era of digitalisation presents various opportunities for business expansion and improvement, there remains to be a huge risk in terms of data security. New identity-related threats come into play, together with the unprecedented growth of devices that need to be authenticated.

The need to keep up with the trend of digitalisation and the continuous rise of internet services for APAC's growing economy puts a renewed focus on identity authentication. APAC's identity verification and authentication markets are forecasted to grow with a [CAGR of 16.6% for the period 2021-2028](#), setting a record high for the region. Subregions like ASEAN and ANZ have also exhibited an increased demand for both on-premises and cloud-based identity verification, recognising the need for more stringent security measures for their systems.

For example, in Australia, verification regulations need to be complied with before a customer can gain access to financial products and services. Other businesses also require ID verification to reduce fraudulent activity and protect privacy and personal information. The same is true for New Zealand where identity authentication is required through the RealMe project that proves someone's identity online. ASEAN countries have also put in place regulations related to identity authentication and other internet security rules for businesses. Aside from the requirement to authenticate, focus is also put on the convenience of verifying identity via biometric and certificate-based authentication.

6. Deployment of MFA to grow

With cyberattacks getting stronger, the traditional methods of authentication can be at risk. Hackers may be able to breach through its preliminary levels, increasing the threats of sensitive data leakage and the exposure of personal information. In a survey conducted by ZDNet, [46% of responding individuals and companies from APAC](#) stated that they shared more data and personal information in 2022 than previous years. At the same time, 74% of respondents perceived data leakage as a main security threat to their organisations, posing various financial and reputational risks.

This finding reinforces the growing trend of multifactor authentication for website or system access, leveraging multiple levels of identity establishment and permission verification. MFA ensures that users are who they say they are through two or more mechanisms, significantly reducing the risk of data breaches. Given its enhanced security features, deployment of MFA is expected to grow in APAC over the next few years, meeting the demands for improved identity verification and data security.

7. Adoption of automated tools to rise

Digitalisation of businesses and economic processes is at a faster pace in APAC than any other part of the globe, according to the [Think Tank KAS](#). APAC businesses continue to invest in technological advancement, leading the way in areas like financial technology, e-health, and autonomous driving. These advancements come hand in hand with the increased adoption of automated tools.

At same time, The Market Data Centre predicts that the industrial automation market will grow at a [CAGR of 12.1% from the period 2022-2030](#), mainly attributed to the digitalisation of industries in China and India and driven by the creation of new businesses throughout the region. The digital transformation in APAC presents a vast opportunity for companies offering automation products that can be proven effective to aid the rapid growth of digital industries. Due to the proliferation of new threats, organisations will want to future-proof their systems by seeking out opportunities for automation support. Among the [processes and tools that will make use of automation](#) include threat detection response, vulnerability management, compliance, Artificial Intelligence (AI) and machine learning tools, cloud security tools, and IoT security tools. Automated tools reduce the workload on cybersecurity professionals, allowing them to focus on more complex tasks and respond more quickly to threats. They also improve the efficiency and effectiveness of an organisation's cybersecurity efforts by continuously monitoring networks and systems for signs of security breaches or vulnerabilities.

Keeping Up with the Changes

2023 certainly looks very much like a year of change, with accelerating momentum, for cybersecurity. With new technologies, regulations, and advancements, it is important your business has the confidence in your Certificate Authority (CA) to ensure that your organisation is compliant. At GlobalSign, we can help your business to automate, manage, and integrate PKI. Contact us today.

[Discover Our Solutions](#)

Article from our SEACC Sponsor, Huawei

“Raising awareness on malware threats in cyberspace among SMEs and MNCs” – Highlights of the Malware Awareness event on 6 January 2023



On 6 January 2023, Huawei held its Malware Awareness x AISP seminar, titled “Raising awareness on malware threats in cyberspace among SMEs and MNCs organisations.” The event brought together a group of cybersecurity professionals including **Mr Dennis Chan**, AISP Exco, Country Cybersecurity & Privacy Officer of Huawei International; **Mr Yum Shoen Yih**, Director of Cybersecurity Programme Centre, Cyber Security Agency of Singapore (CSA); **Mr Wong Yong Wah**, Cybersecurity Consultant, wizlynx group, and **Mr Jeffery Zhang**, CTO of Data Center and Storage Solution Sales, Huawei Singapore Enterprise Business.

The prevalence of malware attacks such as ransomware have continued to rise due to constantly evolving and elaborate phishing scams, in an attempt to stay ahead of law enforcement. During the event, the speakers shared the principle of zero trust as a mindset, while emphasising the importance of a practical approach when building cyber resilience. The journey towards cyber resilience within an organisation involves many factors - putting together a core cybersecurity framework, equipping an organisation with cybersecurity software, and education on cybersecurity related matters, among others. Participants also had the chance to network with industry experts and exchange views with other similar-minded peers.

The event began with speeches from four speakers who shared their unique perspectives and recommendations on how technology such as Huawei’s Ransomware Storage Solution can provide ransomware countermeasures, as well as essential requirements to mitigate cybersecurity risks in our local communities.

[back to top](#)

1.1 Opening Speech – Malware Awareness

Speaker: Mr Dennis Chan, AISP Exco, Country Cybersecurity & Privacy Officer, Huawei International

Giving the opening address for the event, Mr Chan shared about how Huawei labs have benefitted SMEs and the overall technology landscape through the use of Huawei AI and cloud innovation. He also gave a brief overview on AISP and what the organisation does, with support from the Cyber Security Agency Singapore.

Mr Chan reiterated that in alignment with Singapore's initiatives to tackle rising ransomware attacks, AISP aims to empower organisations to develop their own safe cyberspace. He also emphasised the need to raise awareness of cybersecurity issues in SMEs and MNCs.

"It's important that we rope in more cybersecurity professionals or like-minded peers from our local communities to create awareness and mutual rapport to provide assistance or support, be it organisations, industry peers." said Mr Chan.

1.2 What is malware?

Speaker: Mr Yum Shoen Yih, Director of Cybersecurity Programme Centre, Cyber Security Agency of Singapore (CSA)

Adding on to what Mr Chan shared in his opening speech, Mr Yum shared about CSA's advanced security solution, which is able to cover a wide range of cybersecurity threats, including malware. He spoke about the CSA's pivot towards implementing a cyber resilient approach – "Zero Trust" when it comes to staying safe online. He further elaborated on the cybersecurity risk management framework - seven key steps for users to be safe online and future proof an organisation's cyber defences. These steps are:

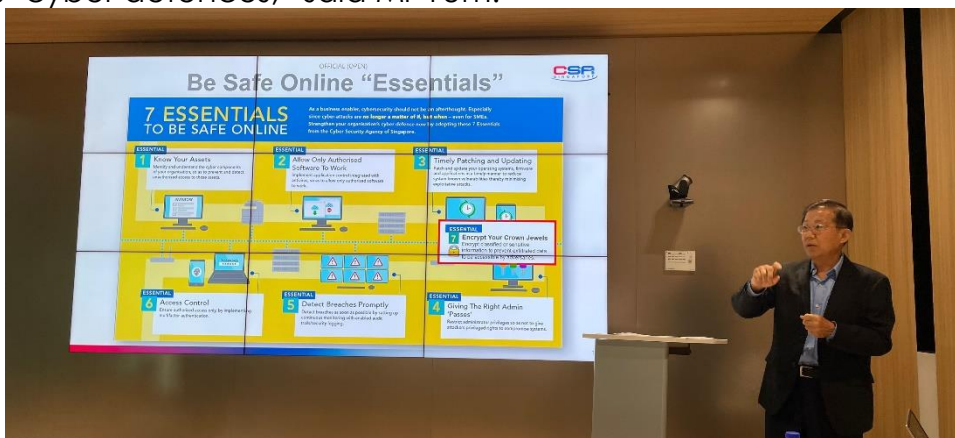
1. Know Your Assets – Identify and understand the cyber components of your organisation, so as to prevent and detect unauthorised access to those assets.
2. Allow Only Authorised Software to Work – Implement application control integrated with antivirus, so as to allow only authorised software to work.
3. Timely Patching and Updating – Patch and update your operating systems, firmware, and applications in a timely manner to reduce system known vulnerabilities, minimising exploitative attacks.
4. Giving the Right Admin 'Passes' – Restrict administrator privileges so as to not give attackers privileged rights to compromise systems.
5. Detect Breaches Promptly – Detect breaches as soon as possible by setting up continuous monitoring with enabled audit trails/security logging.
6. Access Control – Ensure authorised access only by implementing multifactor authentication.
7. Encrypt Your crown Jewels – Encrypt classified or sensitive information to prevent exfiltrated data from being accessible by adversaries.

Sharing the latest statistics from the Singapore Cyber Landscape Report, Mr Yum highlighted that cyber threats such as ransomware and malware still loom over the years

despite large amounts of funding poured into developing sophisticated cybersecurity software. He underlined that phishing scams are the main cyberattack technique to gain access to an organisation's security endpoint or credentials. Mr Yum spoke about how CSA has been overseeing cybersecurity strategy, requirements, and user-friendly practices to tackle the ever-evolving global cybersecurity attacks and detect breaches of protections under the NICE cybersecurity framework.

Mr Yum further shared CSA's stance on cybersecurity - that it inherently is not a technical problem at its core. He stated that the only reason for the existence of cybersecurity is to combat adversaries who wish to compromise a company's systems, and that the best way to do so is through the utilisation of military doctrine - knowing yourself and your enemies. To facilitate this, he touched on the collaboration between NUS and local companies on the development of the AI Malware Analysis, for more effective detection of new and unknown malware. Highlighting steps which companies can take to ensure their cybersecurity, Mr Yum also shared about the two-tiered Singapore Cyber Essential Mark, which aims to enable organisations to prioritise cybersecurity measures required to safeguard themselves from common cyberattacks.

"Cybersecurity is a team sport, be it by yourself or your organisation would not have the capability to tackle cyber threats altogether, this is why the Cyber Security Agency (CSA) brought together three local companies to develop a technology solution to strengthen organisations' cyber defences," said Mr Yum.



Shoen Yih's photo

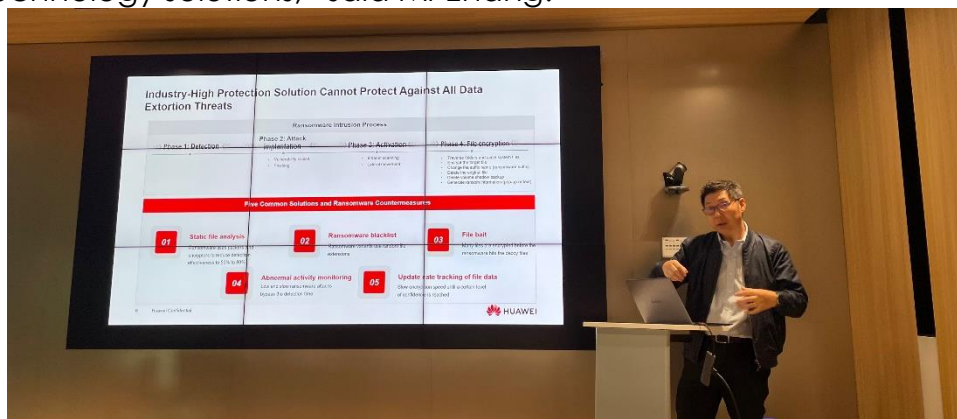
1.3 Huawei Storage Solution with Ransomware Demands

Speaker: Mr Jeffery Zhang, CTO of Data Center and Storage Solution Sales, Huawei Singapore Enterprise Business

Moving on to measures that organisations can take to secure themselves from cyberattacks, Mr Zhang shared about the focus on the efficiency of storage solutions – whether physical or on the cloud – to secure data against ransomware or other cyberattacks. Further sharing about the common solutions and countermeasures to tackle cyber threats from a technical perspective, he underlined that ransomware attacks are always evolving to encrypt valuable data, citing examples of recent global ransomware attacks and threat statistics.

He also spoke about Huawei's unique Ransomware Storage Solution as a last line of defence against cyber-attacks, touching on its key features such as dual protection storage, encryption, air gap, secure snapshot, and WORM, which provides data anti-tampering, security detection, and secure recovery. He also emphasised the importance of encryption for end-to-end transmission to prevent data leaks.

“With the four key technologies, we have different solutions coming into place. When businesses are affected by ransomware attacks; it does not have the bandwidth for ample recovery time. However, Huawei’s holistic solution can restore data and reduce recovery time. With that, Huawei is the best choice to counter ransomware attacks with our unique technology solutions,” said Mr Zhang.



Jeffery's photo

1.4 Victim Perspective of Ransomware Attack

Mr Wong Yong Wah, Cybersecurity Consultant, wizlynx group

As the final speaker for the event, Mr Wong began his speech by sharing a video focusing on the victim's perspective when encountering a ransomware attack. He also reiterated the point shared by CSA Director Mr Yum, that phishing still is the most effective cyberattack technique, further expounding on a Zero Trust approach to protect oneself from ransomware attacks.

Giving participants a breakdown of what happens during a ransomware attack, Mr Wong described how a ransomware attack encrypts files and data from a user's software system, and what happens when a user decides to give in to ransomware demands. He also shared examples of ransomware attacks and how to manage ransomware infections during the aftermath.

“When a victim such as organisations or businesses encounters a ransomware attack, thousands of computer systems are compromised. Victims are likely to be targeted for repeated ransomware attacks due to poor cybersecurity management or lingering vulnerabilities, often by the same attacker,” said Mr Wong.



Yong Wah's photo

For further enquiries, please contact Ms Angus Cheng at angus.cheng@huawei.com

Article from our TCA 2022 Winner, Ms Soffenny Yap



Never have I thought or could have imagined that I will be able to stand alongside with 7 other industry professionals to receive The Cybersecurity Awards 2022.

Connecting back the dots, never would I had imagined that the path I chose was so meaningful. Not for the better of myself or anything to do with this award but how it has helped people and companies aware of what cybersecurity is and how crucial it has taken place in our daily lives, made me realized that it was worth every effort of my 8 years of cybersecurity path.

[back to top](#)

The summary above would not be possible for a working mother like myself without the support and guidance that I have received from my family, friends, colleagues, and association members.

This award would not be possible without the help of all the mentors and cyber security veterans who have not only provided me guidance but also the opportunity and platform to give back to the society on what I have learnt. Being a non technical cybersecurity professional, I was able to help, relate and translate technical jargons to simple terms to my families, friends, public and students that I have presented to.

Personally, this award signifies a remarkable milestone for my career and inspires me to reach for greater heights in future. Through this award, I hope to inspire more youth and women to come forth and join me - to continue my/this journey of making cybersecurity complex, simple.

Lastly, I would hereby like to take this opportunity to thank the Cyber Security Agency (CSA), Association of information security professionals, organising committee and panel of judges, and the Singapore cybersecurity professional community (CSCIS and SCS CS Chapter) for the recognition.



Reflection from our SVRP 2022 Winner, Gregory Choong



I am grateful and honoured to have received the AiSP SVRP Gold Award. As the President of NYP InfoSec, I have several opportunities to contribute to the cybersecurity ecosystem - planning workshops, events, competitions and more. Volunteering in the area of cybersecurity has been fulfilling. I have also grown my expertise in cybersecurity. Moving forward, I will continue to volunteer and contribute to the cybersecurity ecosystem.

~ Gregory Choong, Nanyang Polytechnic

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, each containing a padlock icon. The text is arranged as follows: 'E|CDE' with 'EC-Council Certified DevSecOps Engineer' below it in the top left; 'EC-Council' in the top right; 'DEVSECOPS IMPROVES SECURITY, QUALITY AND RESILIENCE.' in large, bold, red and white letters in the center; 'Build Secure Applications Rapidly. Be a DevSecOps professional Today' in white below the main headline; a white box containing 'Build & Deploy Secure Applications with ECDE' and a red button with 'Get Certified' at the bottom.

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 for details!

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.

[back to top](#)

Upcoming Training Dates

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

Special Offers.

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

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

Thank you.

The ALC team



ALC Training Pte Ltd

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

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

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

Qualified Information Security Professional (QISP®) Course

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP)
- 5 DAYS -

\$840*

~~**\$2800**~~

*70% funding for Singaporeans 40 and above.
50% funding for all Singaporeans below 40 & all PRs.

Call us: +65 8839 0071
Email us: training@opusit.com.sg

AiSP Advance Connect Excel

OPUS ACADEMY

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

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

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

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

COURSE DETAILS

2023 Course dates can be found on https://www.aisp.sg/qisp_training.html

Time: 9am-6pm

Fees: \$2,800 (before GST)*

*10% off for AiSP Members @ \$2,520 (before GST)

*Utap funding is available for NTUC Member

* SSG Funding is available!

TARGET AUDIENCE

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

COURSE CRITERIA

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

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

For registration or any enquiries, you may contact us via email at secretariat@aisp.sg or Telegram at **@AiSP_SG**.

Program Partner



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 2023 can be found on https://www.aisp.sg/cyberessentials_training.html

Time: 9am-6pm

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

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

***Utap funding is available for NTUC Member**

*** SSG Funding is available!**

TARGET AUDIENCE

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

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

Program Partner



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: 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.

CPP Membership



Join our Corporate Partner Programme
for exclusive benefits and partnership with AiSP!

Contact AiSP Secretariat for the benefits and corporate
pricing at secretariat@aisp.sg

For any enquiries, please contact secretariat@aisp.sg

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.



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

[back to top](#)

Membership Renewal

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

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

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

For more updates or details about the memberships, please visit www.aisp.sg/membership.html

AiSP Corporate Partners



Acronis







YES WE H/CK

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

AiSP Academic Partners



Our Story...

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

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

Our Vision

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

Our Mission

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

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

AiSP Secretariat Team



Vincent Toh
Associate Director



Elle Ng
Senior Executive



Karen Ong
Executive



Jennifer Goh
Finance & Human
Resource Officer



www.AiSP.sg



secretariat@aisp.sg



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



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

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