News & Update
- Knowledge Series
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Special Interest Groups
- The Cybersecurity Awards
- Digital for Life
- Regionalisation
- CAAP
- AVIP
- Corporate Partner Events
- Upcoming Events

Contributed Contents
- Data & Privacy SIG: Singapore as a Trusted Data Hub
- Survey from NTUC U PME
- TCA 2022 Winner – Prof Lam Kwok Yan
- SVRP 2022 Winner – Johanan Chi

Professional Development

Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome Bugcrowd 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 Fortinet, Huawei and Mimecast for their continued support in developing the cybersecurity landscape:

News & Updates

Black Hat Asia on 11-12 May

AiSP was at Black Hat Asia 2023 on 11 May & 12 May at MBS Convention Centre to share about AiSP membership and QISP exam to interested individuals.

Visit to CSIT Openhouse on 15 May

AiSP visited our Corporate Partner, Centre for Strategic Infocomm Technologies (CSIT) open house on 15 May. Thank you CSIT for inviting us!

back to top

Fireside Chat with CISCO on 18 May

In collaboration with our Corporate Partner, Cisco, AiSP EXCO member, Dr. Vivek Balachandran, was at the fireside chat on 18 May where they shared about security and cyber resilience.

MOU Signing with SG Her Empowerment Limited on 30 May

On 30 May, during the Ladies in Cyber Learning Journey to Ensign Infosecurity event, AiSP has signed an MoU with SG Her Empowerment Limited (SHE) at the event. We look forward to future collaborations with SHE!


back to top

Knowledge Series Events

Upcoming Knowledge Series

Cyber Defence on 25 May

As part of the Digital for Life Movement, AiSP organised our monthly knowledge series on Cyber Defence where our Corporate Partners ExtraHop and Tenable, and Vectra AI shared insights to our attendees on 25 May. Thank you AiSP Vice-President, Sherin Lee for giving the opening address.
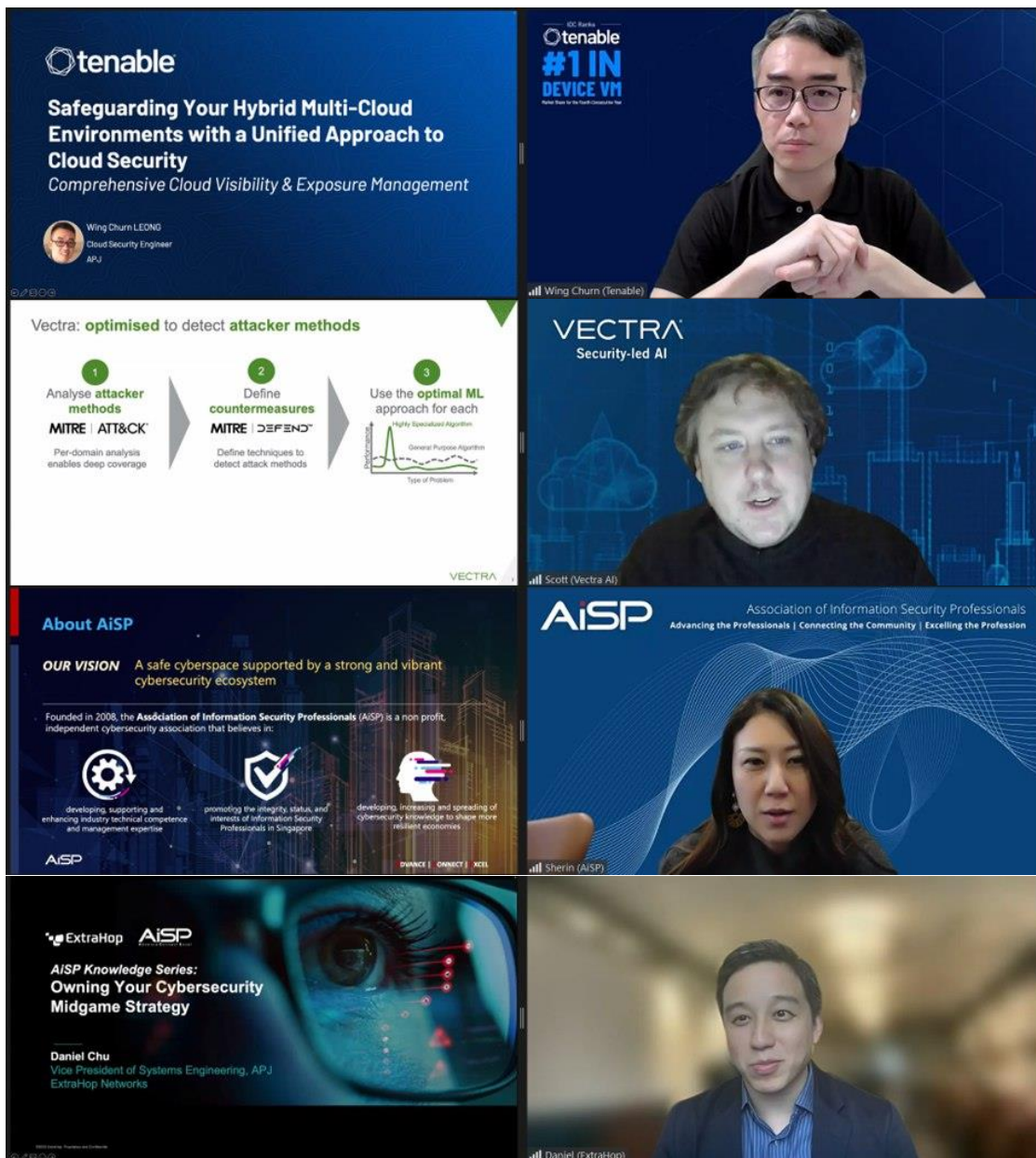
Operations & Infrastructure Security on 19 July

AiSP Knowledge Series – Operations & Infrastructure Security

In this Knowledge Series, we are excited to have Acronis, Eclypsium and Trend Micro to share with us insights on Operations & Infrastructure 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.

The importance of training up talent in Singapore for Operations & Infrastructure Security roles
Speaker: Gabriel Lim, Director, Government Relations & Partnerships, Acronis

Operations and Infrastructure Security is becoming an increasingly important area of focus for modern tech companies and service providers. With new tools and growing use of AI in such environments, engineers need to be equipped with the right skillsets in order to flourish in such roles. In this webinar, Acronis' Director of Government Relations, Gabriel Lim, will share more about the general growth in demand for such business and talent needs, and share some interesting plans that Acronis has in the next few months to address these needs.

Enhancing Operational and Infrastructure Security: Safeguarding Your Critical Systems
Speaker: Dr. Yuriy Bulygin, Chief Executive Officer and Co-Founder, Eclypsium

In today's evolving threat landscape, ensuring the integrity and resilience of your operational and infrastructure networks is paramount.

During this session, we will delve into the key aspects of Operational and Infrastructure Security, the different layers of an IT/OT network, and the role Supply Chain Security has as a critical element in maintaining the integrity of each layer of devices and systems.
We will discuss the different layers of an IT/OT network and highlight the role Supply Chain Security as a critical element in maintaining the integrity of devices and systems, and the importance of protecting against Cyberattacks in your devices and systems.

Additionally, we will touch upon the evolving threat landscape for Operational Technology (OT), including risks posed by insider threats, malware, and physical attacks.
Finally we will share best practices and mitigation strategies to safeguard your infrastructure and ensure the resilience of your critical operations.

Preventing Ransomware with Cybersecurity Monitoring
Speaker: Ransomware and other cyber attacks routinely take advantage of misconfigurations in cloud and IT systems and accounts. Gain insights on how cybersecurity monitoring tools can help strengthen overall attack surface risk management to improve your organization's cybersecurity posture.

Date: 19 Jul 2023, Thursday
Time: 3PM – 5PM
Venue: Zoom
Registration:
https://us06web.zoom.us/webinar/register/1016853407196/WN_QSNCXsTgT7O5Ekol1bC4-g

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 2023 are as follows (*may be subjected to changes*),

1. Operations & Infrastructure Security, 19 Jul
2. IoT, 30 Aug
3. Red Team, 20 Sep
4. DevSecOps, 18 Oct
5. CTI, 22 Nov

Please let us know if your organisation is keen to provide speakers! Please refer to our scheduled 2023 webinars in our event calendar.

back to top
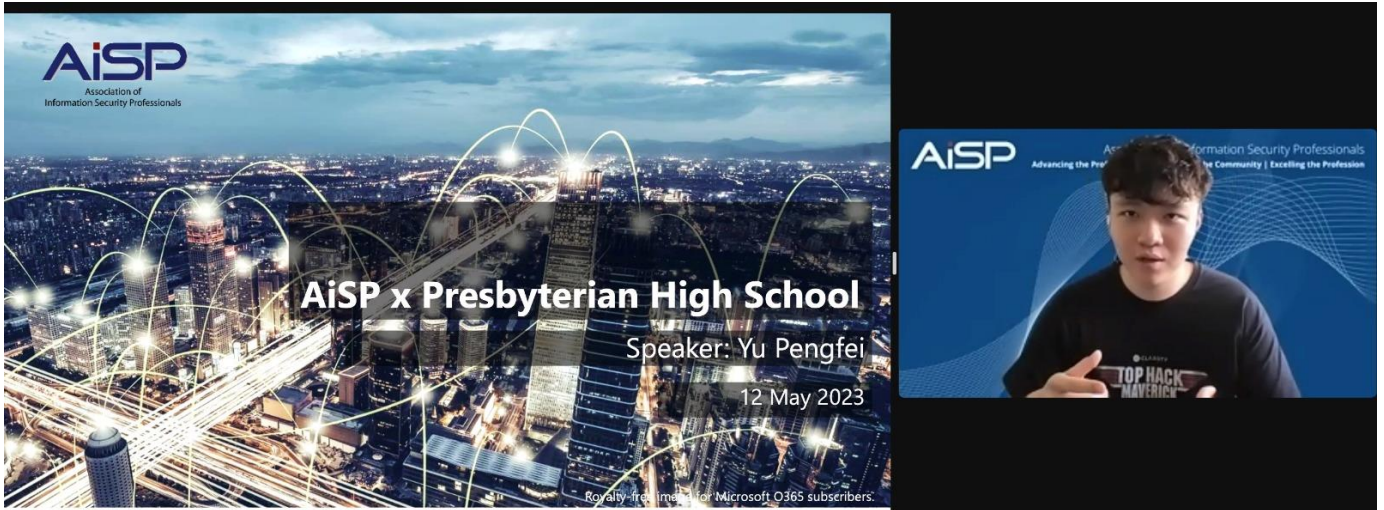
Student Volunteer Recognition Programme (SVRP)

Learning Journey to Grab on 11, 12 and 17 May

As part of Digital for Life Movement, AiSP brought a total of 79 ITE West Students on a learning journey to our Corporate Partner, Grab office on 11,12 and 17 May. Our Corporate Partner, Wissen International (EC-Council ASEAN) were present for all three days and shared insights with the students on the certification courses.

School talk for Presbyterian High School on 12 May

As part of Digital for Life Movement, AiSP conducted a school talk to over 800 Presbyterian High School students on 12 May. AiSP EXCO Member, Yu Pengfei shared insights on Cybersecurity awareness and Careers Opportunities in Cybersecurity to the students.

AiSP Youth Symposium 2023 on 2 July

SPONSOR

EC-COUNCIL

SUPPORTING PARTNERS

(ISC) SINGAPORE   ISACA Singapore Chapter   Yayasan MENDAKI   young ntuc U

U associate an NTUC initiative   NYC National Youth Council Singapore   SINDA Singapore Indian Development Association

ACADEMIC PARTNER PROGRAMME

ITE Institute of Technical Education   NYP NANYANG POLYTECHNIC   NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE   NUS National University of Singapore

NGEE ANN POLYTECHNIC   REPUBLIC POLYTECHNIC   SiT SINGAPORE INSTITUTE OF TECHNOLOGY   SINGAPORE POLYTECHNIC SP

SMU SINGAPORE MANAGEMENT UNIVERSITY   SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES   SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN Established in collaboration with MIT   Temasek POLYTECHNIC

As part of Singapore Youth Day 2023 on 2 July 2023 (Sun), AiSP will be organising the 2nd Youth Symposium to reach out to the Youths for a day of sharing, internship or career opportunities with our partners on 2 Jul 23 (Sun). We will also invite keynote speakers to share on the importance of Youths in Cyber and Tech.

We are expecting 100 Youths and professionals (Subject to COVID restrictions) for the Symposium in this Physical Event. We have invited our Patron, Senior Minister of State, Ministry of Communications and Information and Ministry of National Development, Mr Tan Kiat How as our Guest of Honour and to have a dialogue session with the attendees on how Youth play an important role in Cyber & Tech in the future. The event is open to all students in secondary and tertiary level.

The details for the event are as follow:

Date: 2 Jul 2023 (Sun)
Time: 11.30 am to 3.00 pm
Venue: JustCo @ Marina Square
Dress code: Smart Casual

Register here now

back to top

AiSP
Advance Connect Excel

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
- Leadership: 10 Hours
- Skill: 10 Hours
- Outreach: 10 Hours

Example B
- Leadership: 0 Hour
- Skill: 18 Hours
- Outreach: 18 Hours

Example C
- Leadership: 0 Hour
- Skill: 36 Hours
- Outreach: 0 Hour

Example D
- Leadership: 0 Hour
- Skill: 0 Hour
- 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

back to top

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!

back to top

Ladies in Cybersecurity

Ladies in Cyber Learning Journey to Ensign on 30 May

On 30 May, AiSP brought a group of students to our CPP Ensign InfoSecurity's office for a learning journey and a dialogue session with Ms Sim Ann, Senior Minister of State, Ministry of Foreign Affairs & Ministry of National Development, Dr Tan Mei Hui , Vice-President, SCS Cybersecurity Chapter, Ms Jackie Low, Deputy Director, Info Sec, Chief Information Office, Ensign InfoSecurity moderated by Ms Sherin Y Lee, Vice-President of AiSP & Founder for AiSP Ladies in Cyber Charter.

Our AISP Ladies in Cyber Mascot, Thena was also present to welcome the panel and the students. The students benefitted from the sharing and learned about how women could contribute to strengthening cybersecurity ecosystem. AiSP would like to thank SG Her Empowerment Limited, an independent non-profit organisation, with Institution of Public Character ("IPC") status, that strives to empower girls and women through community engagements and partnerships for joining us today.

The students also get to tour the Executive Briefing Centre and get to speak to the staff of Ensign to get to know more on their day-to-day operations and the role that they are performing as a Cybersecurity professional.

AiSP also launched the Ladies in Cyber Mentor Reflection Book: An Inspiring Book of Women in Cybersecurity during the event by SMS Sim Ann.

Thank you, SMS Sim Ann for gracing the event and supporting AiSP Ladies in Cyber Programme!

Want to find out more on our AiSP Ladies in Cyber Programme such as mentoring or learning journey or engagement session? Contact the AiSP Secretariat at secretariat@aisp.sg.

back to top

Special Interest Groups

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

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

Thank you for all your nominations
TCA 2023 Call for Nominations has ended on 14 May.

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! Only Silver sponsorship packages are available.

back to top

TCA2023 Sponsors & Partners

Digital for Life

DFL E-Payment Learning Journey on 26 May

As part of Digital for Life Movement, AiSP was at Kampung Admiralty on 26 May for the E-payment Learning Journey where seniors learnt about cyber hygiene through our Cyber Watch game.

back to top

East Coast Digital Festival on 10 June

Regionalisation

SEA CC Webinar – Data & Privacy on 8 Jun

The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2023. The first webinar will be focusing on Data & Privacy where speakers will be sharing insights on the best practices for data protection.

Data Protection ABC
Speaker: Hoi Wai Khin, Partner, RSM [Association of Information Security Professionals]

The phrase "Not IF but WHEN" perfectly captures the reality of the current cyber threat landscape. Locally, security incidents, data breaches, and cases of non-compliance with the Personal Data Protection Act (PDPA) are becoming increasingly common. Your organization may have already been affected or will likely face these challenges in the future. With cyber attacks occurring daily and in multiple locations, it can be challenging to keep track of them all.

It is crucial for organizations of all sizes to stay Aware of the latest data breaches and threats, Be prepared for potential breaches or threats, and ensure Continuity of operations in the event of a breach. Using experiences gained on the ground, the session will be sharing the ABC of good internal controls that will help manage incidents, limit reputational damage, and reduce recovery time and costs.

Brunei Darussalam's Personal Data Protection Journey

back to top

Page 18 of 53

Speaker: Farah Zainal, Personal Data Protection Manager [AITI (Brunei)]

The webinar aims to provide the audience with a brief overview of the upcoming Personal Data Protection law in Brunei Darussalam.

Cambodia Data Protection Initiative
Speaker: Ou Phannarith, Founder of ISAC-Cambodia [Innovations for Social Accountability in Cambodia]

This presentation will discuss about the current landscape of data protection in Cambodia and the effort to establish the data protection regulations.

Data Protection and CyberSecurity
Speaker: Ts Alan Yau [Malaysia Board of Technologists]

Companies frequently create two discrete teams and purchase different tools to address cybersecurity and data protection separately. Two teams, two software sets, and considerable IT costs and administrative expenditures are required to maintain and manage them.
But is it the best course of action to separate data protection from cybersecurity? If you read the definitions of data protection and cybersecurity, it makes sense.
Data protection deals with a number of concerns connected to data storage, administration, and access, whereas cybersecurity deals with protection against cyberattacks. These two fields do differ from one another. To successfully handle data breaches, organisations should integrate cybersecurity and data protection into their routine operations.

Navigating Key Legal Issues on Data Privacy Compliance
Speaker: Maria Keala Mae M. Bleza, Data Privacy Lawyer [WiSAP (Women in Security Alliance Philippines)]

The presentation will delve on the discussion of the legal milieu of data privacy with focus on the following topics:
1. Key legal issues of data privacy concepts, compliance and implementation
2. Survey of data privacy cases in SEA

Date: 8 June 2023, Thursday
Time: 3PM – 5PM (SGT)
Venue: Zoom
Registration:
https://us06web.zoom.us/webinar/register/4216810994785/WN_llsql6lzSRy0VdqtSyKouQ

back to top

Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP x SBF Workshop on 31 May 2023

On 31 May, in collaboration with Singapore Business Federation, AiSP Vice-President & CAAP EXCO Lead Tony Low conducted CAAP Workshop where he shared insights on social engineering and data security.
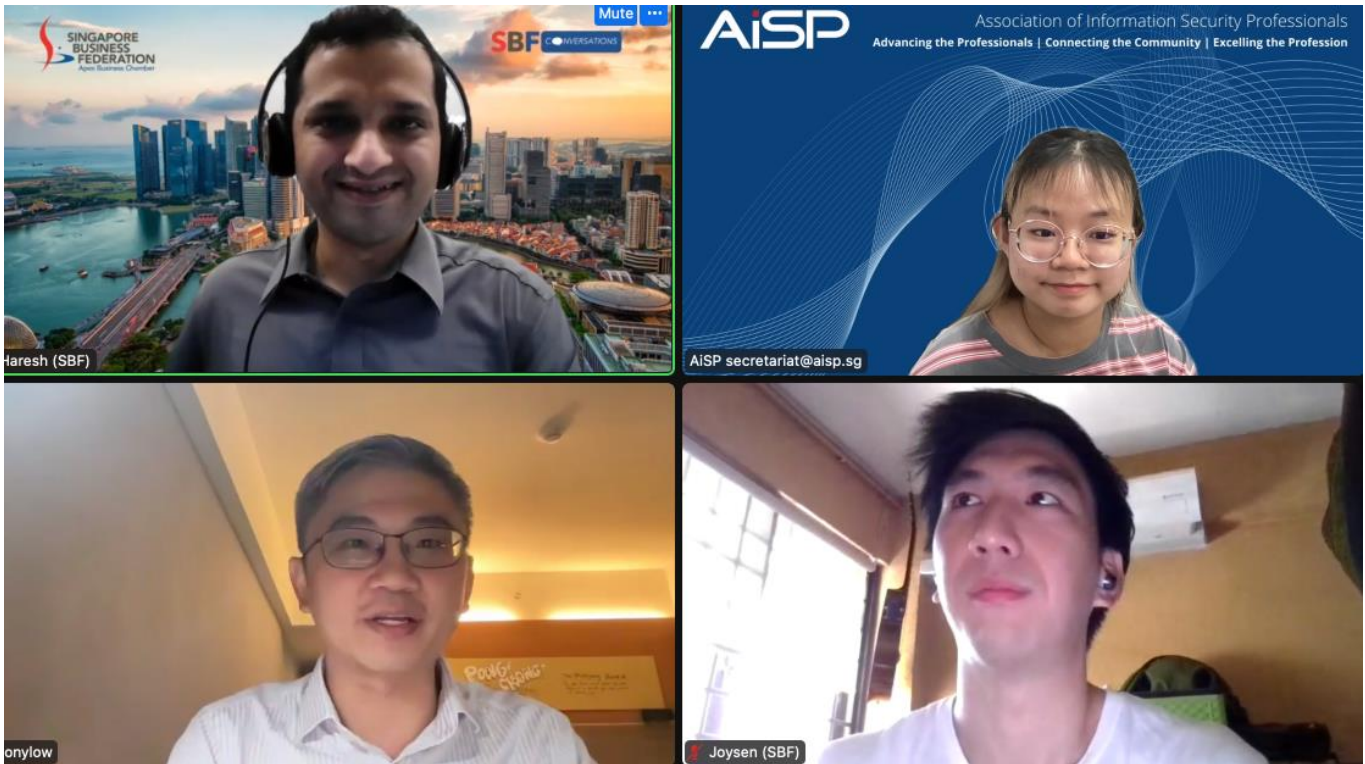
AiSP Validated Information Security Professionals (AVIP)

AVIP Meeting with CSA on 5 May

AiSP AVIP Members had an insightful discussion on 5 May on the current issues and topics for cybersecurity with Cyber Security Agency of Singapore (CSA).

Corporate Partner Events

Hybrid AD Cyber Resilience Life Cycle on 23 May

As part of Digital for Life movement, AiSP collaborated with our Corporate Partners, DT Asia Pte Ltd and RSM Singapore, for an event on Hybrid AD Cyber Resilience Life Cycle on 23 May. Thank you, Mike Tan, Ronino Tabanan and Hoi Wai Khin for sharing with our attendees.

Cyber Intelligence Briefings - The Threat Of ARES Leaks on 24 May
In collaboration with our Corporate Partner, Cyfirma, AiSP will be organising a series of webinars. On 24 May, Cyfirma shared about ARES: Unveiling a New Threat in the Cyber Landscape.
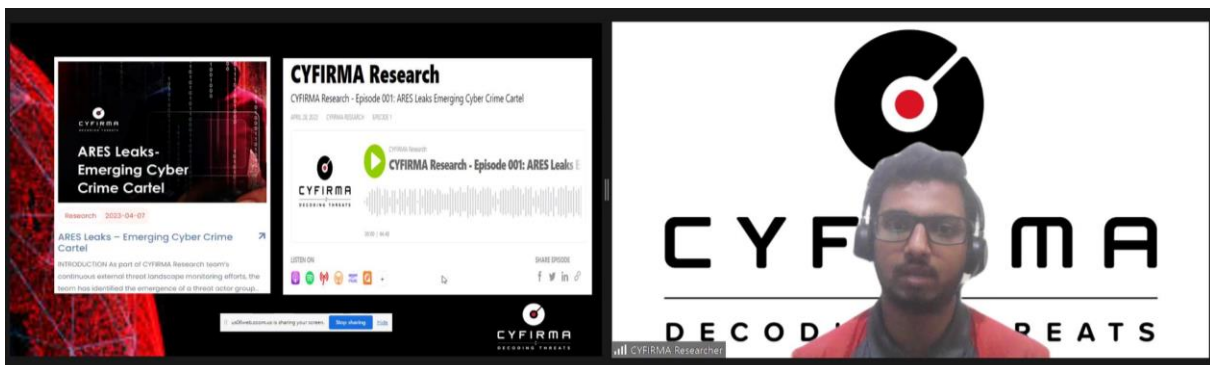
back to top

Upcoming Events

Cyber intelligence Briefings - The Rise of FusionCore An Emerging Cybercrime Group from Europe on 7 June

Cyber intelligence Briefings
The Rise of FusionCore - An Emerging Cybercrime Group from Europe

Dear Cybersecurity Professionals,

FusionCore is a European-based group that operates a malware-as-a-service and hacker-for-hire operation, offering a convenient platform for threat actors to purchase affordable and customizable malware. This development has led to an increase in the sophistication of cyber-attacks.

In this webinar, CYFIRMA Research team will share detailed insights into FusionCore, its evolution and modus operandi. This group offers comprehensive instructions to sellers of their services or products, allowing even individuals with minimal experience to carry out complex attacks.

The briefing will emphasize the importance of having complete visibility into the attack surface, as security teams cannot effectively protect against threats they cannot see.

Participate in the webinar to learn how to stay ahead in the battle against cybercrime.

Webinar Details:
Date: 7 June 2023
Time: 11:00AM Singapore Time (GMT +8)
Registration Link: https://us06web.zoom.us/webinar/register/8816838729432/WN_-_vvUyPLRYSj3M0HDWauow

back to top

Cyber intelligence Briefings: Tense China-Taiwan Relations - Engagement on the Cyber Battlefield on 21 June

**Cyber intelligence Briefings
Tense China-Taiwan Relations - Engagement on the Cyber Battlefield**

Dear Cybersecurity Professionals,

In our upcoming exclusive webinar, we will address the pressing issue of Chinese Advanced Persistent Threat (APT) groups and their escalating activities, particularly considering heightened tensions with Taiwan. Recent research conducted by CYFIRMA has revealed persistent cyberattacks from APT27, targeting at critical industries & organizations, and utilizing tactics and tools reminiscent of their counterpart, APT41.

During this engaging webinar, our Researcher Tomáš Meravý will delve into the following areas.

•   Rise of Chinese APT groups
•   Tactics & Connections
•   Risks & Impact
•   Recognizing signs of APT activities
•   Building resilience
•   Interactive Q&A Session

Feel free to share this invitation with your colleagues and industry peers who may benefit from the insights shared during this session.

Tense China-Taiwan Relations - Engagement on the Cyber Battlefield
Date: 21 June 2023, Wednesday
Time: 11:00AM SG Time (GMT +8:00)
Registration: https://us06web.zoom.us/webinar/register/WN_an-66JfFSK2sG9mCUEsMLA

AiSP x wizlynx group - Understanding Red teaming and Purple Teaming Exercise on 28 June

AiSP x wizlynx group - Understanding Red teaming and Purple Teaming Exercise

UNDERSTANDING RED TEAMING AND PURPLE TEAMING EXERCISE

AiSP X wizlynx group Event

28 JUN 23, WEDNESDAY | 3PM – 5PM
JUSTCO @ MARINA SQUARE

REGISTER NOW

As the prevalence and sophistication of cyber threats continue to grow, companies of all sizes are becoming increasingly aware of the risks posed by potential cyber-attacks. In response, organizations are implementing various defensive layers, mechanisms, and solutions to prevent such threats, including firewalls, IDS, IPS, and other systems that form the front line against malicious activities. Additionally, the human element – the so-called "Blue Team" – configures, maintains, and operates this infrastructure.

However, there is a notable challenge: these defenses involve numerous interactions and processes, some of which can be highly complex. In many cases, these defenses are only truly tested during stressful, harmful incidents. This raises questions about the effectiveness of these defenses and the preparedness of internal security teams and security operations centers (SOCs) to detect and respond to targeted attacks.

A Red Team assessment addresses this issue by approaching the problem from an adversarial perspective, utilizing tactics and methodologies distinct from traditional security assessments. By leveraging threat intelligence and well-defined tactics, techniques, and procedures (TTPs), the Red Team can effectively emulate realistic threats or adversaries, thereby providing valuable insights into an organization's security posture and preparedness.

back to top

Movement is Life: A Red Teaming Demonstration
Speaker: Gerard De Las Armas, Principal Cyber Security Consultant, wizlynx group &
Lei Yeh, Sr. Cybersecurity Consultant, wizlynx group

The presentation will commence with a warm-up session to introduce the audience to
Red Teaming concepts and terminology. Following this, our experts will analyse
Microsoft Active Directory data to identify potential attack avenues for lateral
movement. The audience will then be shown lateral movement techniques, along with
OPSEC safe and EDR bypass tips and tricks. Finally, we'll demonstrate the action-on-
objective phase of Red Teaming through a simulated ransomware attack.

**Why is it mandatory for CII sectors in Singapore to undergo comprehensive
Red Teaming and Purple Teaming assessments conducted by independent
parties?**
Moderator: Meng Chow Kang,Adjunct Associate Professor, Nanyang Technological
University Director & Principal Consultant, Averitus Pte Ltd

Panellists:
Sunny Neo, AiSP EXCO Member & Senior Red Team Consultant, Mandiant
Darrel Huang, Senior Cybersecurity Engineer, GovTech Cybersecurity Group
Leow Kim Hock, Asia CEO, wizlynx group

Red Teaming and Purple Teaming are security assessment exercises that test an
organization's security posture and readiness against cyber threats. In Singapore,
Critical Information Infrastructure (CII) sectors are required to undergo annual
Vulnerability and Penetration Testing (VAPT) by independent and licensed
Penetration Testing provider. At this moment, Red Teaming and Purple Teaming are
strongly recommended by Government of Singapore, but yet it is made mandatory.

By making Red Teaming and Purple Teaming exercises compulsory for CII sectors in
Singapore, the government can take proactive steps to protect critical national assets,
reduce the risk of cyberattacks, and ensure the continuity of essential services.

Date: 28 June 2023, Wednesday
Time: 3PM – 5PM
Venue: Justco @ Marina Square
Registration: https://forms.office.com/r/fT9wpirBFJ

back to top

SOC 101 TRUST NO FILES! I Votiro BFSI Workshop on 12 July

Financial institutions face an ever-growing threat from incoming files. Every loan application uploaded to a web portal emailed spreadsheet or signed PDF sent to an account manager can contain malicious code that threatens the organization. All files are suspect. Ransomware campaigns and other destructive malware are running rampant as malicious actors seek out high-value targets to coerce and compromise. And the need for strong security is more critical now as the risk of file-borne threats has never been greater.

 Join us in this evening workshop together with Votiro and Industry experts to further deep dive and discuss:

1. The challenges facing financial institutions in countering the risk of file-borne threats.
2. The threats and regulations, address why current security solutions offer inadequate protection to organizations.
3. Recommendations for how financial institutions can confidently mitigate the threat of file-borne malware, optimizing security in conjunction with business continuity and productivity.

back to top

Agenda:

Event Details

06:15 – 06.45pm	Registration & Refreshment
06:45 – 07.00pm	Welcome & Introduction
07:00 - 07.20pm	Zero Trust Framework
07:20 - 07.40pm	MAS TRM Best Practice & Compliance
07.40 - 07.55pm	Why Votiro and addressing to TRM
07.55 - 08.15pm	Panel Discussion
08.15 - 08.30pm	Demo Session
08.30 – 09.00pm	Q&A & Networking

Date: 12 July 2023 Wednesday

Time: 6pm SGT

Venue: JustCo @ Marina Square,
6 Raffles Boulevard, #03-308, S(039594)

Target Industry: Banking, Financial Services and Insurance (BFSI)

Register Your Seat Now

Who should attend:

Head of Security Operations Center, Chief Information Security Officer, Head of Cyber Security, Head of Cyber Defense, Head of Information Security (Infosec), Chief Security Officer, Head of Cybersecurity Policy/Compliance, Vice President of Security Assurance, Cyber Security Director/Lead, Threat Investigations Lead, IT Security Manager, Head of Digital Transformation Security, Cybersecurity Strategy, IT Risk & Data Compliance Team, Cyber Security Governance Officer, Cybersecurity Operations Officer, etc

Key Speakers

back to top

Johnny Kho

AISP, President

Johnny Kho has over 20 years of experience in Information Technology and Cyber Security with broad experience in Security Solutions, Operations, and Consulting in both technical and business roles. He is currently a Director leading the Managed Security Services Team under the Singtel Cyber Security Division. He has been active in contributing to the local IT Security area through various interest groups and now, volunteers in the President position in AISP as well as Committee Member in SCS IS Chapter. He takes a strong personal interest in SME Digital Initiatives and initiated the Cyber Awareness and Advisory Program (CAAP) in collaboration with Cyber Security Agency (CSA) to create a sustainable support ecosystem for business owners on their digital and cyber journey.

Paul Hadjy

CEO and Founder, Horangi Cyber Security & SFA Cybersecurity Committee

As the Chief Executive Officer and Founder of Horangi Cyber Security, Paul leads a team of cybersecurity specialists who create software that solves challenging cybersecurity problems. Horangi aims to bring world-class, cyber solutions to the Asian market. The company provides clients with the right, actionable data to make critical cyber decisions. Prior to Horangi, Paul worked at Palantir Technologies, where he was instrumental in expanding Palantir's footprint in Asia Pacific. He worked across Singapore, Korea and New Zealand to build Palantir's business in both the commercial and government space and grow its regional teams. He has over a decade of experience and expertise in Anti-Money Laundering, Insider Threat, Cyber Security, Government and Commercial Banking. In 2016, Grab selected Paul as their Head of IT to shape the company's internal technology, information security and business process architecture during their rapid scaling.

Grace Chong

Gibson Dunn, Of Counsel

Grace Chong is Of Counsel in Gibson Dunn's Singapore office and a member of the firm's Global Financial Regulatory Group. She heads the Financial Regulatory practice in Singapore which consists of three associates. Ms. Chong has extensive experience advising on cross-border and complex regulatory matters, including licensing and conduct of business requirements, regulatory investigations, and regulatory change. A former in-house counsel at the Monetary Authority of

back to top

Singapore (MAS), Ms. Chong regularly interacts with key regulators, is closely involved in regional regulatory reform initiatives, and has led discussions with regulators on behalf of the financial services industry.

Mark Chan

Votiro, Technical Director, APJ

Mark Chan is the Technical Director at Votiro, overseeing and supervising solutions in Asia Pacific and Japan. Mark Chan has over 20 years of diverse experience in all aspects of vendor and channel business with a successful track record as a Cybersecurity Solution Expert. He is highly skilled in system integration, consultancy, pre-sales support, partner enablement training, end-user training, and thought leadership. He is an expert in technology risk management and IS/Cybersecurity and holds leadership positions both locally and regionally.

George Seah

Votiro, Technical Consultant, APAC

George Seah is the Technical Consultant at Votiro and implements strategic and operational intelligence to customers across the Asia Pacific region. He is a technical expert in Network Security, Infrastructure Integration, Saas, Application Security, Pre-sales, Solution Design, Cloud Transformation, and Cloud Security.

Secure Your Seat Today

Jointly brought to you by:

![AiSP logo - Association of Information Security Professionals](#)

back to top

Undergraduate and Internship Opportunities at CSIT

Passionate about cutting-edge technologies? Join us as our scholar or intern to kickstart an exciting ICT career that focuses on digital technologies to meet Singapore's national security needs!

Apply here

Career opportunities at CSIT

Passionate about cutting-edge technologies? Join us in our work to conduct applied research and build products to meet Singapore's national security needs!

Apply here

back to top

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
7 Jun	Cyfirma Webinar	AiSP & Partner
8 Jun	SEA CC Webinar – Data & Privacy	AiSP
9 Jun	AVIP Event with SMS Tan Kiat How	AiSP
10 Jun	Celebrate Digital @ East Coast	Partner
10 Jun	Zheng Hua Community Day	Partner
20 Jun	N0H4TS Cyber Week	Partner
21 Jun	Cyfirma Webinar	AiSP & Partner
22 – 24 Jun	CYSummit	Partner
25 Jun	DFL @ Bukit Panjang	Partner
27 – 28 Jun	Seamless Asia	Partner
28 Jun	Event with wizlynx	AiSP & Partner
2 Jul	**Youth Symposium**	AiSP
5 Jul	Learning Journey to Singtel for RP	AiSP & Partner
5 Jul	Cyfirma Webinar	AiSP & Partner
11 Jul	Learning Journey to ASUS for Pri Sch	AiSP & Partner
12 Jul	Learning Journey to RSM for Pri Sch	AiSP & Partner
12 Jul	Event with Votiro	AiSP & Partner
17 – 19 Jul	CISO Melbourne	Partner
18 Jul	Learning Journey to Grab	AiSP & Partner
19 Jul	Cyfirma Webinar	AiSP & Partner
19 Jul	Knowledge Series – Operations & Infrastructure Security	AiSP & Partner
26 Jul	Learning Journey to DBS for Pri Sch	AiSP & Partner
26 Jul	Cyfirma webinar	AiSP & Partner
28 – 29 Jul	Skills for Good Festival	Partner
28 Jul	ITE West Security Summit	Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Data & Privacy SIG

Singapore as a Trusted Data Hub

As the world becomes increasingly digitised, personal data has become an essential part of business operations. With the increase in cyber threats, it is essential for businesses to ensure that they protect the personal data of their customers and employees. In 2021, the Cyber Security Agency of Singapore (CSA) reported a 54% increase in Singapore firms hit by ransomware attack[1], and in a separate 2021 Cisco Cybersecurity for SMBs report, as many as two in five Singapore Small-Medium Enterprises (SMEs) suffered a cyber incident in the past 12 months, with 75% of these incidents involving loss or breach of customer data[2]. With affected companies expecting to lose an average of USD$2.87mil from a data breach[3], suffering a data breach could mean the end of business for a SME.

To ensure that Singapore remains competitive with a strong reputation as a trusted data hub in the digital economy, and to help organisations, especially SMEs level up their data protection standards, the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) developed a series of data protection initiatives to help organisations strengthen their data protection standards and gain the competitive advantage in the digital economy.

Data Protection Essentials – helping SMEs acquire the essentials

The Data Protection Essentials (DPE) is a programme designed to support SMEs in acquiring a basic level of data protection and security practices to protect customers' personal data and recover quickly from a data breach. Under this programme, SMEs can tap on a one-stop professional service for a holistic implementation of basic data protection and security practices through a one-time setup and retainer service.

DPE One-Stop Professional Service

The DPE one-stop professional service provides SMEs with a suite of professional service offered by service providers appointed by IMDA. This includes a one-time set up service that would cover 5 keys areas:

---

[1] Singapore Cyber Landscape 2021 Report
[2] Cisco Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense 2021
[3] IBM Cost of a Data Breach Report 2022

back to top

1)   Accountability – establish data protection and cyber security practices to provide confidence and foster trust with customers and business partners.

2)   Basic Data Security Practices – put in place basic data security practices to better protect your business and customers' personal data, and to recover quickly should a data breach occurs.

3)   Incident Management – develop an incident management plan to manage any data breach in a systematic manner.

4)   Training and communications – facilitate/ conduct data protection and cyber awareness training to help employees understand their data protection obligations and foster a culture of personal data protection.

5)   Review – conduct desktop and phishing exercises to review the robustness of the practices after six months of implementation.

SMEs can also subscribe to a retainer service provided by the service providers to ensure that their policies and practices are up-to-date. Under this retainer service, SMEs can expect bi-annual reviews and refreshers of their data protection and security practices implemented through desktop and phishing exercises.

Why should SMEs go for the DPE?

Besides acquiring basic data protection and security practices to mitigate risks of data breaches, SMEs that implemented the one-time setup and signed a minimum 1-year retainer service under the DPE one-stop professional service would enjoy:

1)   Recognition for their efforts in being accountable by being listed on IMDA's website and awarded the DPE logo; and
2)   In the event of a data breach, the PDPC may consider a SME's implementation of the DPE as a mitigating factor.
Data Protection Trustmark

Launched in 2019, the DPTM is a voluntary enterprise-wide certification and will be a visible indicator that an organisation adopts accountable and responsible data protection practices. Assessed by independent third parties, DPTM-certified organisations not only have to demonstrate good practices but also an effective system to monitor and detect incidents, along with ready plans to manage and recover from incidents.

The DPTM certification framework and controls were developed based on Singapore's Personal Data Protection Act (PDPA), coupled with elements of international benchmarks and best practices[4]. Certification is valid for 3 years.

Why should organisations go for the DPTM?

DPTM-certified organisations agree on the following benefits:

1)   Demonstrate PDPA Compliance

DPTM-certified organisations would be able to demonstrate that, at the point of their certification, they have in place robust policies and practices that are in compliance with the PDPA, providing assurance to customers, business partners and regulators in their commitment to protecting personal data.

In the unfortunate event of a data breach, DPTM-certified organisations may request from the PDPC a voluntary undertaking in lieu of an investigation to allow them the opportunity to implement their remediation plans. PDPC may also consider DPTM as a mitigating factor.

2)   Establish Good Data Governance

The DPTM involves a robust third party assessment that would validate your data protection regime. During the assessment, the assessor would highlight gaps or areas that can be improved and provide recommendations to allow the applicant organisations to remediate and strengthen their overall data governance standards. Most importantly, it would give you peace of mind knowing that your organisation is in good shape.

3)   Increase Competitive Advantage

Based on a recent PDPC Survey[5], 4 in 5 companies preferred to do business with DPTM-certified companies. The DPTM is also increasingly recognised and incorporated by public agencies in their procurement as a way to identify trusted vendors and suppliers, as the DPTM is aligned to the government's IM8 Personal Data Protection Policies and Standards[6].

Conclusion

As consumers become increasingly aware of their personal data protection rights, and with the increase in data breaches, there would be a demand for businesses to be

---

[4] These include data protection laws of Australia, Hong Kong, the European Union, as well as the Organisation for Economic Cooperation and Development (OECD) Privacy Guidelines, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems.

[5] PDPC Industry Survey on the Personal Data Protection Act 2021

[6] Smart Nation Singapore – Government's Personal Data Protection Laws and Policies

back to top

accountable and to show that they have robust data protection standards in place when managing personal data. Thus, it is imperative that organisations recognise that being accountable in managing personal data is not simply a matter of compliance, but a worthwhile investment that would strengthen their organisation's reputation, build consumer trust, and help them stand out from their competitors.

To find out about the Data Protection Essentials and the Data Protection Trustmark and the available grants, please visit:
DPE – www.imda.gov.sg/dpe
DPTM – www.imda.gov.sg/dptm

About the Author
The Infocomm Media Development Authority
The Infocomm Media Development Authority (IMDA) leads Singapore's digital transformation by developing a vibrant digital economy and an inclusive digital society. As Architects of Singapore's Digital Future, we foster growth in Infocomm Technology and Media sectors in concert with progressive regulations, harnessing frontier technologies, and developing local talent and digital infrastructure ecosystems to establish Singapore as a digital metropolis.
For more news and information, visit www.imda.gov.sg or follow IMDA on Facebook (IMDAsg) and Twitter (@IMDAsg).

Survey from NTUC U PME
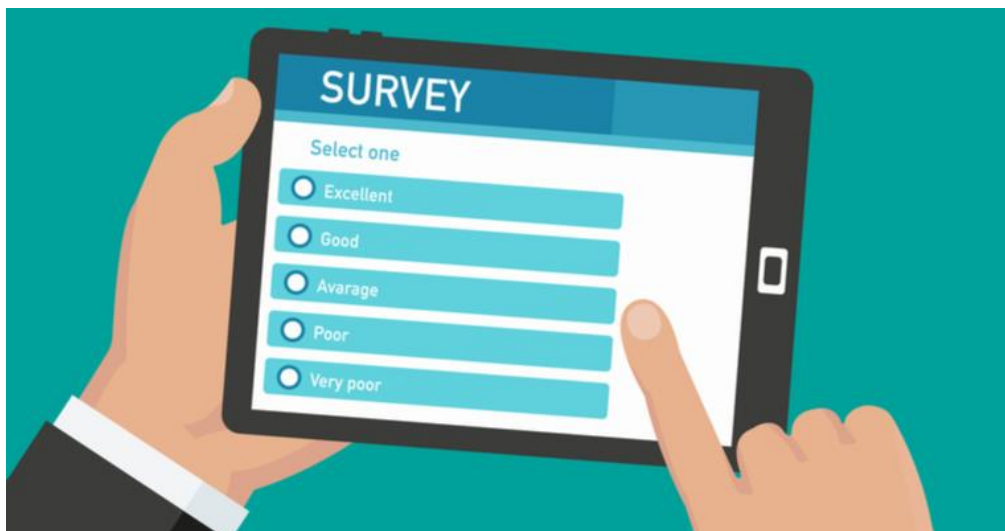
In partnership with AISP, NTUC U PME is planning to curate an exclusive bundle deal comprising of discounted events and promotional product offerings. Through this short survey, we aim to gather more insights about your profile and interests so that we can understand you better.

Please take the survey here

back to top

Article from our TCA 2022 Winner, Prof Lam Kwok Yan

It is my great honour to be the recipient of the Cybersecurity Awards 2022 in the Hall of Fame Category. I feel incredibly overjoyed to be recognized for my contributions to the Cybersecurity development in Singapore.

As a cybersecurity researcher, practitioner, and enthusiast, I have always been passionate about ensuring the safety and security of digital assets. In 1997, I founded PrivyLink Pte Ltd, a spin-off from NUS, to develop a secure file encryption software for enabling secure document exchange in e-Commerce and e-Government environments. I also designed and developed cryptographic toolkits for secure Internet application development. Now, 25 years on, these products have been widely adopted, and remain as relevant today in the face of the ever-increasing threat of cyberattacks.

In 2012, realising the numerous challenges with data mobility and consumerization of IT, I founded SODA Pte Ltd. At the time, cloud and consumer mobile applications were rapidly proliferating throughout the workplace; I saw a need for organizations to enable professionals to efficiently collaborate using their own devices, while ensuring the safety and privacy of the organisation's network and data. This motivated me to develop a suite of applications suitable for mobile and desktop environments, designed to work seamlessly with existing corporate networks and storage infrastructures.

Throughout my career, I had the opportunity to serve as a security consultant and advisor to various agencies, including government and commercial organisations. I observed that processing and analysing insights and alerts inferred from clusters of observations in cybersecurity was an extremely time-consuming and laborious task, which required a high level of expertise and attention to detail. Recognizing the inefficiencies in processing and

back to top

analysing cybersecurity data, it spurred me to consider the use of AI and machine learning to improve productivity in this area.

This led me to start another company in 2018, Tau Express Pte Ltd, a spin-off from NTU, to adopt a Platform approach in using AI to automate many of the routine tasks. The company has had success in leveraging the power of AI to improve the productivity of cyber analysts, allowing them to focus on more complex and high-value tasks. It has been my goal for many years to tap on the potential of AI to revolutionize the way insights and alerts are processed and analysed in cybersecurity.

My academic duties aside, I will remain committed to advancing capability development in cybersecurity through research and education. As the cybersecurity landscape continues to evolve in the years to come, the road ahead will be fraught with new, unseen challenges. Investing in research and education to develop new technologies will thus remain critical to help build a strong cybersecurity ecosystem and a trusted digital economy. I strongly believe that industry leaders and fellow like-minded peers in this community will continue to drive innovation and development to ensure that individuals and organisations of all sizes can protect themselves and stay ahead of the curve.

In addition to advancing capability development, I am also passionate about promoting international collaboration in cybersecurity. Cyber threats do not respect borders and will continue to pose global challenges. This will require strong international collaboration and information sharing to address such challenges to promote a trusted digital economy. In this regard, the work that AiSP has done, and continues to do, is most commendable. The Association has built a strong network of individuals and organisations that share a common interest to encourage partnerships, innovation, and creativity.

> "*If you want to go fast, go alone, if you want to go far, go together*"
> – Martha Goedert

As Martha Goedert once said, "If you want to go fast, go alone, if you want to go far, go together." By working together, we can create a culture of trust and transparency, to build a prosperous and secure future for individuals, organisations, and societies around the world.

I want to take this opportunity to express my heartfelt thanks to AiSP for recognizing my contributions to the cybersecurity ecosystem. I am deeply honoured to receive this award and look forward to continuing to work together to build a better, safer world.

back to top

Reflection from our SVRP 2022 Winner, Johanan Chi

I am thrilled to announce that I have been awarded the Gold Award for AISP's SVRP, or Student Volunteer Recognition Programme. This recognition means a lot to me, as it acknowledges the hard work and dedication, that my team and I have put into giving back to the cybersecurity community.

Throughout 2022, I was given the opportunity to organize and lead on various events like Youth Cyber Exploration Programme (YCEP), and it was truly an enriching experience. Seeing the students ranging from various schools and background learning about cybersecurity was fruitful to me as I knew that I'm able to make a positive impact by educating the youth on cybersecurity.

I had hosted and organized various cybersecurity workshops for Republic Polytechnic students ranging from concepts such as Open-Source Intelligence to Penetration Testing and its tools. Personally, the practical element of learning is very important to me, and I was joyed to see the positive feedback from students when I included my own set of hands-on elements to these workshops. It was a great experience to plan and organize practical elements to allow for critical thinking and growth for the students.

It was truly an honour to organize and work with various exceptional talents across Singapore for Lag and Crash 3.0 as seeing how committed fellow students were in hosting a CTF for students just like us truly inspired me to thrive in my growth.

Of course, not forgetting my various lecturers and peers which supported me throughout the process, I would like to give my bottomless gratitude to them as I would not have been able to do it without them. I hope that my peers and juniors would continue to make a positive impact to the industry in any way that they can, it truly is an amazing feeling to know that I could make a change and inspire others.

back to top

In conclusion, receiving the Gold Award for SVRP has reminded me of the importance of service and the power of volunteerism. My time as a student volunteer has impressed upon me the crucial nature of promoting cybersecurity awareness and education. Furthermore, it has allowed me to learn, develop, and contribute to the cybersecurity ecosystem positively.

Thank you to AISP for this recognition, and again to all those who have supported and encouraged me along the way. Let's continue to work together to create a brighter future for all.

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
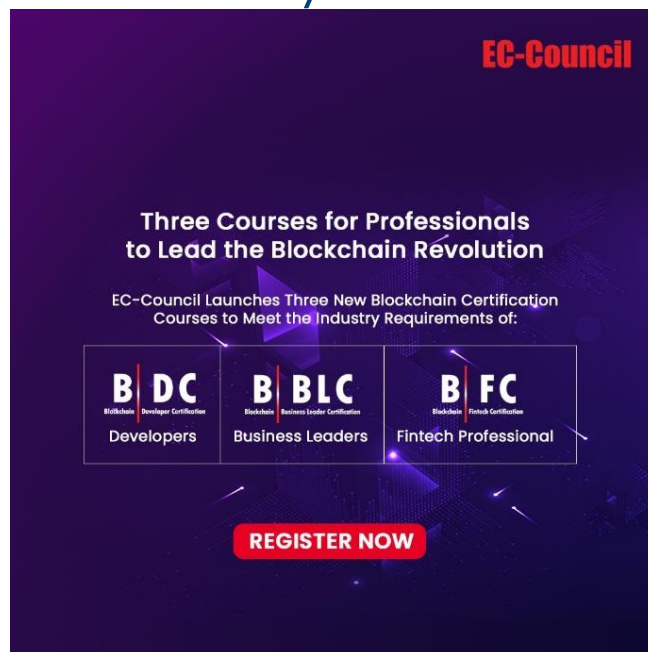
EC-Council's Blockchain Certifications Overview

EC-Council's blockchain certification courses are curated by experts to support the growing demand for skilled blockchain professionals.

back to top

These programs have been designed to meet the industry requirements of developers, business leaders, and fintech professionals in this rapidly growing area.

Our blockchain certification courses consist of three knowledge and competency areas: development, implementation, and strategy.

During the course, students get exposure to multiple blockchain implementation concepts and a unique guideline for sustainable and scalable blockchain development using quantum-resistant ledgers.

Considering the market opportunity and skills required for different target groups, EC-Council has launched three new blockchain programs:

1. **Blockchain Business Leader Certification (BBLC)**
2. **Blockchain Fintech Certification (BFC)**
3. **Blockchain Developer Certification (BDC)**

Blockchain technology is becoming more prominent in today's digital world, and getting certified is a great way to showcase your knowledge and lend credibility to your resume.

EC-Council's expert-designed courses will provide you with hands-on experience and help you gain valuable insights that are mapped to real job roles.

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®

back to top

- CIPM, CIPT, CIPP/E

The right training makes all the difference

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

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

AiSP Member Pricing – 15% discount

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

Upcoming Training Dates

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

Special Offers.

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

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

Thank you.

The ALC team

ALC Training Pte Ltd
3 Phillip Street, #16-02 Royal Group Building, Singapore 048693
T: (+65) 6227 2883 | E: learn@alctraining.com.sg | www.alctraining.com.sg

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.

back to top

Qualified Information Security Professional (QISP®)

Promotion for Qualified Information Security Professional (QISP) Exam until 30 June!

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

Online

Qualified Information Security Professional (QISP)

NEW

Prepare for QISP Certification with QISP e-Learning Programme!

- For professionals with at least 1 year of experience in IT and cybersecurity awareness and those who will be taking on a senior technical or management role in IT enterprise governance
- Deep-dive into security principles and concepts and gain understanding for cyber defence strategies and different levels of security implementation
- Earn an internationally-recognised certification and become a security expert on Singapore and across ASEAN

Objectives

Understand and attain knowledge in enterprise governance, risk analysis and management, security controls, security principles and lifecycle, business continuity planning, develop and implement security goals, objectives, strategies and programmes and maintain and review security operations.

Modules

1. Governance and Management
2. Physical Security, Business Continuity and Audit
3. Security Architecture and Engineering
4. Operation and Infrastructure Security
5. Software Security
6. Cyber Defence

AiSP Certification Road Map

Qualified Information Security Professional (QISP) E-Learning Programme → Specialisation Courses in Threat Intelligence, Forensics, Network Defense, Ethical Hacking

Transformists NETWORK

WISSEN Cyber Security Competency Development

Scan the QR Code
to register your interest!
Email aisp@wissen-intl.com
for more information.

back to top

Physical

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**

back to top

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.

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

DT ASIA
Security with Confidence

eclypsium

ENSIGN INFOSECURITY

ExtraHop

FERGUS CONSULTANCY GROUP

FORESCOUT
Automated cybersecurity across your digital terrain

FORTINET

GOVTECH SINGAPORE

Grab

HUAWEI

image engine

INTfinity

ITSEC ASIA

kaspersky

KnowBe4
Human error. Conquered.

KROLL

LEARNCOLLAB

Lookout

MANDIANT

METASECURITY

MICRO FOCUS

mimecast

NCS

NETWITNESS
An RSA Business

NOZOMI NETWORKS

ONESECURE

PARASOFT

psb ACADEMY

RAJAH & TANN CYBERSECURITY

Responsible Cyber

Right-Hand CYBERSECURITY

RSM

SCANTIST

back to top

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

🌐 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 us for any enquiries.