NEWSLETTER

December 2022

NEWS & UPDATE

New Partners

AiSP would like to welcome Parasoft and Yeswehack as our new Corporate Partners and Nanyang Technological University (NTU) as our new Academic Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partners

New Academic Partner

Continued Collaboration

AiSP would like to thank Ensign InfoSecurity, Kaspersky and Trend Micro for their continued support in developing the cybersecurity landscape:

News and Updates

AiSP @ Singapore Fintech Festival from 2-4 November

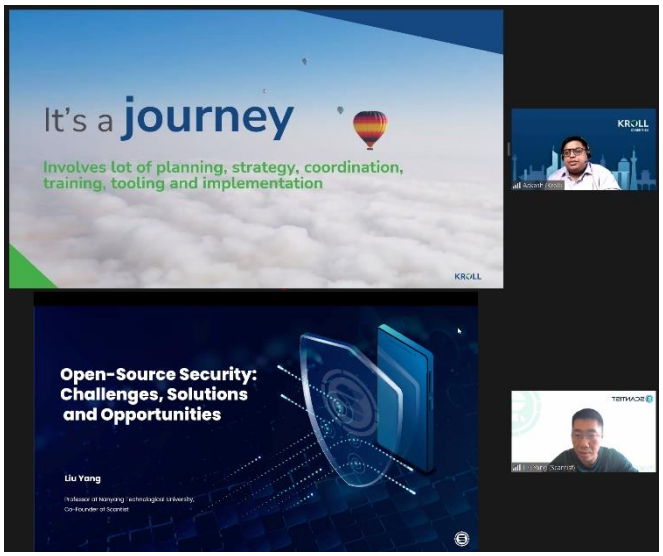
On 2-4 November, AiSP was down at Singapore Fintech Festival to set up a booth and share on what AiSP is about and encourage signups for membership. We also shared on the initiatives and events that AiSP provides for members and the community in general.

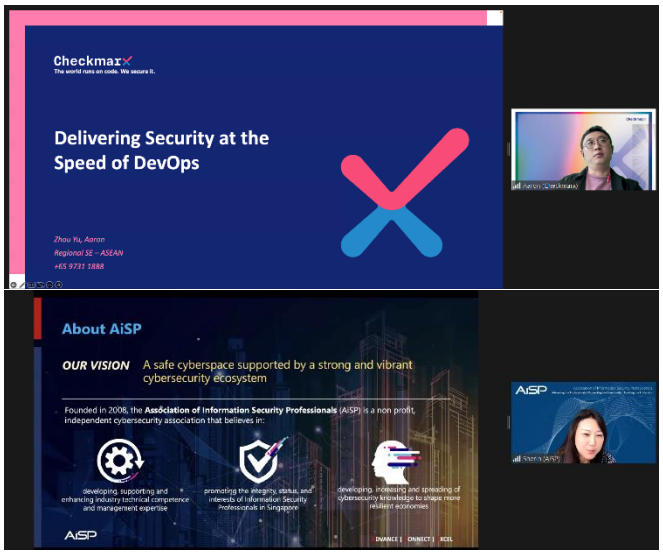
back to top

Knowledge Series Events

Dev Sec Ops on 17 November

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 17 November, we invited our Corporate Partners, Checkmarx, Kroll & Scantist to share insights on DevSecOps. We would like to thank AiSP Vice-President Sherin Y Lee for giving the opening address.





Upcoming Knowledge Series

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

1. Software Security, 18 Jan 23
2. Data & Privacy, 22 Feb 23
3. Business Continuity, Physical Security & Audit, 22 Mar 23

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

back to top

Cybersecurity Awareness & Advisory Programme (CAAP)

Malware Awareness Day on 6 January 2023

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

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

Click here to register.

back to top

Student Volunteer Recognition Programme (SVRP)

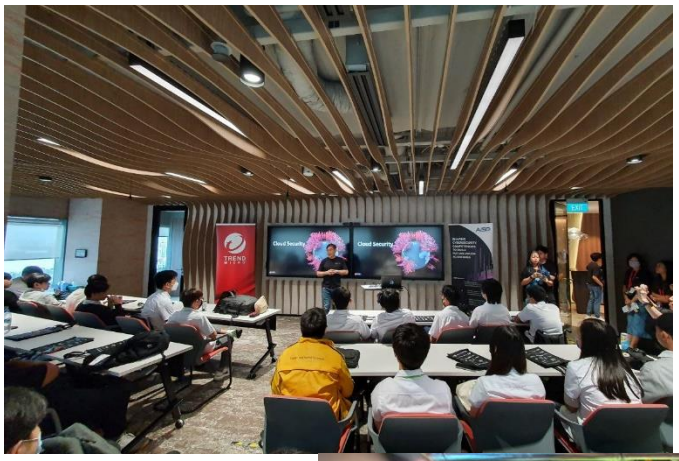
NTU – Scantist DevSecOps Networking Session on 2 November

On 2 November, Scantist invited AISP to set up a booth at NTU-Scantist DevSecOps Professional & Tools course launch in collaboration with Cyber Security Research Centre @ NTU (CYSREN). This course focus on addressing cybersecurity risks at the software development level. We would like to thank our Corporate Partner, Scantist for having us.

back to top

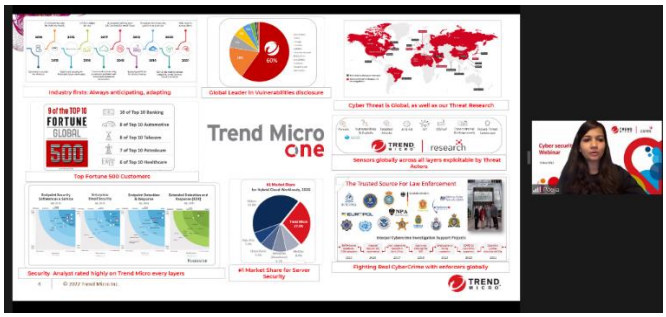
Learning Journey to Trend Micro for ITE West on 9 November

On 9 November, AiSP brought 40 ITE West Year 1 students on a learning journey to our Corporate Partner, Trend Micro's office. They played a game of hangman in groups and the winning group won exclusive merchandise from Trend Micro. We also hope that the students have gained insights from the sharing done by Winson Lau on Cloud Security.



AiSP x Trend Micro Stay Cyber-Aware on 9 November

Concurrently with the Learning Journey today, Trend Micro also conducted a webinar with IHL students on Introduction on Trend Micro and What is cybersecurity. The webinar ended with a short kahoot quiz and prizes are given out to the top 3 winners. We hoped that the students have enjoyed the virtual webinar.



back to top

Student Volunteer Recognition Programme Awards Ceremony on 16 November

AiSP Student Volunteer Recognition Programme Awards Ceremony has concluded on 16 November. Congratulations to our SVRP 2022 Award Winners!

We would like to thank Mr Tan Kiat How, Senior Minister of State, Ministry of Communications and Information & Ministry of National Development for gracing the event and presenting the awards to our Gold Winners. We would like to thank Singapore Institute of Technology for hosting us at their beautiful school and Huawei International and Cyber Security Agency of Singapore (CSA) for supporting the event.

Big thank you to Deputy President (Academic) & Provost of Singapore Institute of Technology, Prof. John Thong and AiSP EXCO & SVRP Lead, Ms Soffenny Yap for giving the opening speech at the ceremony.

back to top

AiSP Cyber Wellness Programme

Click here to find out more!

back to top

Ladies in Cybersecurity

Ladies Talk Cyber Series

For the Seventeeth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Jackie Low, who is currently working as Deputy Director in Infosecurity at Ensign InfoSecurity.

How to be successful in cybersecurity field

In celebration of SG Women year, AiSP's secretariat decided it was timely to launch a series of interviews of female leaders across industries who fulfil high impact roles, and learn about their journeys, experiences and insights. The initiative aims to shed some light on what it takes to make it in this field. The interviews can be source of invaluable career insights as well as opportunities for those in the field to get a deeper understanding of the industry, and how its leaders are innovating to disrupt the cyber landscape.

Introducing women with a deep interest in cybersecurity

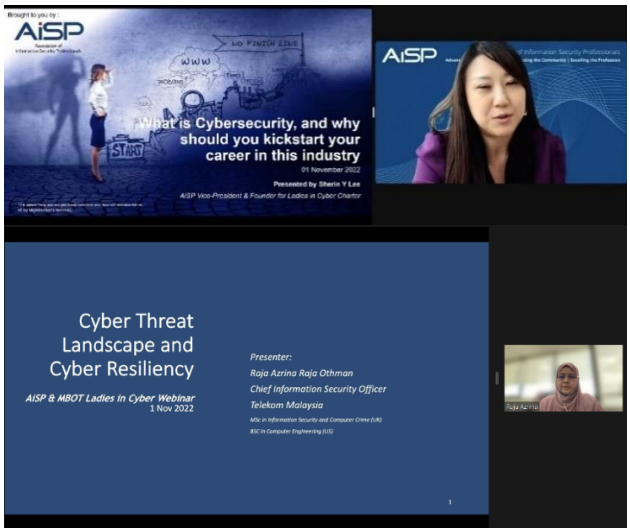
As a Deputy Director in Infosecurity at Ensign InfoSecurity, Jackie work closely with business leaders on a strategic and operational level, providing a consolidated and comprehensive view of the organisation's cybersecurity posture; ensuring that information security policies, procedures and control techniques support Ensign's business objectives and the industry's best practices. She is responsible for the cyber threat intelligence management in the organization and her role is to provide an oversight on the entire intelligence cycle to deliver actionable insights for informational advantages in the domains of cybersecurity, governance, risk, and compliance.

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

back to top

Association of Information Security Professionals (AiSP) and Malaysia Board of Technologists (MBOT) Ladies in Cyber Webinar on 1 November

In collaboration with Malaysia Board Of Technologists (MBOT), AiSP organised the Ladies in Cyber Webinar where AiSP Vice-President and Founder for AiSP Ladies in Cyber Charter Ms Sherin Y Lee & Chief Information Security Officer of Telekom Malaysia, Ms Raja Azrina Raja Othman did an afternoon sharing and discussion on the Importance of Cybersecurity and Career Options in the Industry on 1 November. Thank you Datuk Technologist Ingenieur Dr. Siti Hamisah Tapsir for giving a speech as well.



back to top

Learning Journey to Schneider Electric on 15 Nov

AiSP and Schneider Electric organised a learning journey to Schneider Electric on 15 Nov 22. This was followed by a Dialogue Session with Senior Parliamentary Secretary for Health & Law, Ms Rahayu Mahzam. More than 80 female students and PMETs attended the session where they get to tour Schneider Electric Innovation Centre and interacted with Schneider female staff to get to know more about a career in Cyber as well as the challenges that the industry face. We would like to thank our Panellist, Ms Ee Lin Lim (Senior Assistant Director at Cyber Security Agency of Singapore), SPS Rahayu Mahzam, Ms Cherry Ong and our Moderator, Ms. Sherin Y Lee, for sharing their personal experiences with the participants.

back to top

Special Interest Groups

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

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

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

Digital for Life

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

Together with People's Association & Trend Micro, AiSP organised a closed-door session with our Grassroots Leaders on Scam Awareness. With the theme of "elevating Cybercrime awareness", this session aims to enhance the capabilities of the Grassroots Leaders in identifying threats in the online space. Thank you David Ng from Trend Micro and Aileen Yap from Singapore Police Force for sharing insights. Thank you AiSP EXCO Member & Cyberwellness Co-Lead, Soffenny Yap for moderating the panel discussion with Minister of State Sun Xueling, Ryan Flores and Aileen.

back to top

Digital for Life - Singapore Appreciation Dinner on 4 November

AiSP would like to thank IMDA for inviting AiSP to the Digital for Life - Singapore Appreciation Dinner on 4 November! AiSP President, Mr Johnny Kho received the token of appreciation at the dinner.

back to top

Celebrate Digital @ Marsiling on 13 November

As part of the Digital for Life Movement, AiSP went to the northwest area to set up a booth at Celebrate Digital @ Marsiling. Thank you Senior Minister of State Zaqy Mohamad for visiting our booth.

back to top

AiSP Sharing at Tampines East on 13 November

AiSP went to Tampines East to share with the community on scam awareness. Participants who were mostly senior citizens benefitted from the sharing and also took the opportunity to clarify their doubts on the issue.

The Cybersecurity Awards

The Cybersecurity Awards (TCA) 2022 has officially concluded on 11 November 2022. Congratulations to all the TCA 2022 winners! AiSP would like to thank BeyondTrust, Cisco Systems, Ensign InfoSecurity, Huawei International & ST Engineering Cybersecurity & Trend Micro for their kind sponsorship as Platinum Sponsors for The Cybersecurity Awards 2022 (TCA22). CyberProof, CSIT, DBS Bank, Kaspersky, Singtel & Wizlynx for their kind sponsorship as Gold Sponsors for The Cybersecurity Awards 2022 (TCA22). And IronNet, PCS Security Pte Ltd, RSA, Singapore Institute of Technology (SIT), Thales Group & Workforce Singapore for their kind sponsorship as Silver Sponsors for The Cybersecurity Awards 2022 (TCA22). Thank you, all sponsors, for contributing to the Cybersecurity Ecosystem.

back to top

back to top

Regionalisation

South East Asia Cybersecurity Consortium (SEACC) Forum on 23 November

AiSP organized the inaugural South East Asia Cybersecurity Consortium (SEACC) Forum 2022 on 23 November at Lifelong Learning Institute where 7 cybersecurity associations from Brunei, Cambodia, Indonesia, Malaysia, Thailand, Myanmar and Vietnam signed a Memorandum of Understanding (MoU) together with AISP to foster regional collaboration for the South East Asia cybersecurity ecosystem. Theme for this forum is "Strengthening collaborations in Information Security across South East Asia".

Thank you Minister for Communications and Information & Minister In-Charge for Smart Nation & Cybersecurity, Mrs Josephine Teo for gracing the event.

back to top

South East Asia Cybersecurity Consortium (SEACC) Closed Door Discussion on 24 November

On the consecutive day after the forum, a closed-door discussion was held at Singapore Institute of Technology (SIT) where all the associations came together to share the issues faced in their community and brainstorm on the solutions. They also visited the living lab at SIT itself. Thank you SIT for hosting the discussion.

back to top




SME Cybersecurity Conference

SME Cybersecurity Conference was held successfully on 30 November with more than 300 participants attended the event. Member of Parliament for Pasir Ris Punggol GRC and NTUC U SME Director, Ms Yeo Wan Ling graced the event and had a panel discussion with the speakers facilitated by AiSP Vice President and CAAP Lead, Mr Tony Low. The theme for this year's conference is "Ready to build a secure digital business".

The following topics were discussed during the conference

1. Securing Your SME's technology for the Threats of Today
2. Building a Competitive Edge for your Business with Cybersecurity
3. Threat Actor Strategies to breach SMEs in 2022
4. Handle with Care – Safeguarding Data through Visibility
5. Establish Digital Trust leading to Business Growth

A big thank you to all the speakers who shared insights with our attendees and Blackpanda, Fortinet, GlobalSign, Onesecure, Cybersecurity Agency of Singapore, Softscheck and Xcellink for sponsoring the conference.

back to top

back to top

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

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

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

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

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

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

back to top

CREST

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.

back to top

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
2 Dec	TCA2022 Judges Appreciation	AiSP
12 – 15 Dec	Learning Journey to KL	AiSP & Partner
17 Dec	DfL in the Community at Taman Jurong CC	AiSP & Partner
18 Dec	DfL in the Community at Whampoa CC	AiSP & Partner
6 Jan	Malware Awareness Day	AiSP & Partner
9 Jan	School talk at Bukit Panjang Government School	AiSP & Partner

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

back to top

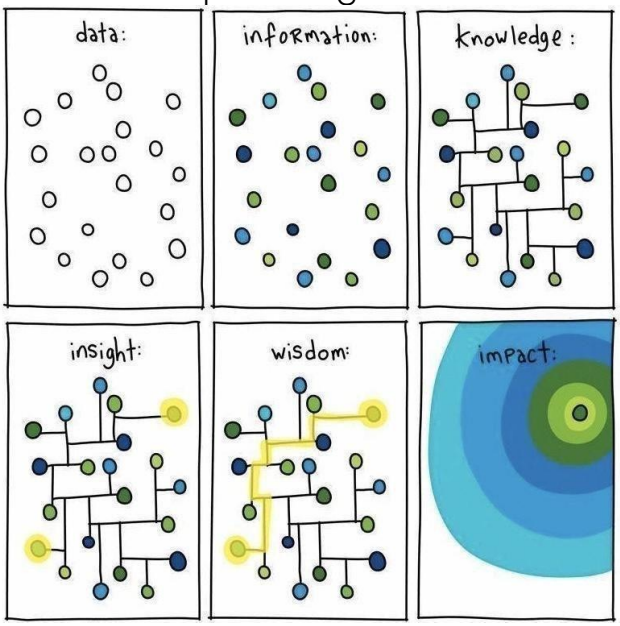
CONTRIBUTED CONTENTS

Article from Cyber Threat Intelligence SIG

Rantings of a Cyber Security Analyst

I recently attended an EC Council course for Cyber Threat Intelligence (CTIA) and through the course, I realized how large the gap is, especially for smaller businesses. In today's context, the threat landscape is ever changing. Cyber Threat Intelligence helps by equipping the security team with knowledge of what to look out for, what are the key infrastructure or service being attacked, or correlate with IOCs seen within the environment with external intelligence on what part of an IOA the IOC belongs to and hopefully identify the TTP of the attack which enables identification of the security gap within the environment.

This is no easy feat, and it is not as simple as buying a product. You can purchase CTI feeds, get a TIP or any other related CTI solution, but they are just helping with collection of the information, allow easy correlation and access to the collected data. This requires skilled analyst with expertise to know what they are looking for and how the data can be converted into intelligence which helps the organization.



I have always liked the above image, as I feel it accurately shows the complexity of providing the impact. Some organizations make the mistake of collecting threat feeds and assuming that provides an outcome of better security.

There is a need to generate strategic, operational, and tactical cyber threat intelligence for the organization. I will not go deep into this as it would be an extremely wrong write up, but on a high level:

back to top

- **Strategic Cyber Threat Intelligence** – Identifies the **Who** and **Why**, which provides organizations with crucial insights. This is often used by the C-Suite individuals, which allow them to understand threats the organization is facing and allows them to make risk-based decisions regarding staffing, technologies, cybersecurity requirements and budgets.

- **Operational Cyber Threat Intelligence** – Addresses the **How** and **Where**, which is used by the incident responders, network defenders, forensic analysts and so on. The CTI provides technical context, with a focus on the IOC, related links, and whether they might be found in the environments they are responsible for securing. Context is critical for operational users because every environment is unique in how they use various technology stacks.

- **Tactical Cyber Threat Intelligence** – Focuses on the **What** and is used by every organization. From the largest organizations with dedicated SOCs, to the smallest who only have a few cyber defenders or may have outsourced to a Managed Security Service Providers (MSSP). Users of tactical cyber threat intelligence are on the frontlines of an organization's cyber defenses. Tactical users leverage CTI provided IOCs, content, and context to directly prevent threat actors' attacks on their organizations.

Some of you may find the above too "advanced" and probably think your organization is too small and there is simply not enough resource to have such a team. The harsh reality is the adversaries do not care.
Be it a company with users count of 5 or even 1000, chances are, you have similar solutions in place. Do you have an Exchange server? MSSQL? Webservers? From large enterprises to a small supermarket, if you have an IT infrastructure, you will have similar weaknesses. Be it Windows or Linux servers, there is no difference based on the size of the company.

Take for example, a recent trend of attacks which focuses on vulnerable builds of MSSQL. Various threat actor groups started scanning the internet for exposed and vulnerable MSSQL servers. Depending on the threat actor, some will deliver cryptominers, while others perform ransomware attacks. All these done through exploitation of the MSSQL server. In my personal experience, I saw this firsthand affecting organizations of different sizes. Financial institutes, supermarkets, manufacturing companies. It was not an attack specific to an organization type. Do you think the adversary would check on what company is this before launching the attack? Being opportunistic, if there is a security gap, they would go for it.

With Cyber Threat Intelligence, these companies would have been able to see this trend and knowing this affects MSSQL. The operational users would check their environment for all their MSSQL servers and see if they are exposed to public and if they are running on a

back to top

vulnerable build. A more advanced team would begin a threat hunt to see if the server has already been compromised and investigate for any persistency or suspicious object on the server. If for some reason, patching is not possible, this would go towards the C-Suite for strategic planning. Maybe spending on a network IPS to mitigate the threat while putting down policies for patch management as the strategic plan to mitigate this risk.

A personal experience I had was when identifying signs of a breach through a vulnerable MSSQL server, the customer said this server is an application from a third-party application vendor. The vendor insisted not to patch for some odd reason, and it was left as-is. The server is part of the organization's network with access to other systems. It irks me, but there was no further action, nor was this intelligence and security risk being brought up to the management of the company. In this case, it is a ticking timebomb waiting to go off.

The sad truth is all organizations require cyber threat intelligence to truly be a step ahead and to reduce the risk of a breach. Realistically, it is hard to build a proper team. It would not be as simple as hiring a bunch of engineers.

Ideally, the team should also consist of host analysts, malware analysts, forensic analysts, and threat hunters. These are all very specific skillsets which even large enterprises do face issues hiring. This would be even worst for smaller companies which may have only a single general IT personnel.

There are MSSP and other vendors providing such services, which I highly recommend all organizations to consider this as an option versus building your own security team. Be it to compliment your existing SOC or simply to offload these monitoring and threat hunting responsibilities, should the organization be too small to justify building a SOC.

One thing I would caution is to find out how in-depth the service is. A vendor may charge cheap, but all they provide is log monitoring and flagging out alerts to you. Without a threat hunter in your organization, would this alert help or provide any improvements to your security?

Getting the right service to compliment your organizations current capabilities is key. If the service is simply selected based on a compliance of requiring monitoring and storage of data, you are setting up for failure and eventual breach.

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'

back to top

Managed Threat Response team. He is also a member of AiSP CTI SIG, EXCO and volunteer at CSCIS CTI SIG.

Views and opinions expressed in this article are my own and do not represent that of my places of work. While I make every effort to ensure that the information shared is accurate, I welcome any comments, suggestions, or correction of errors.

Article from SME Conference Sponsor, Cyber Security Agency of Singapore (CSA)

Cybersecurity as a Competitive Edge for your Business

Cybersecurity as an enabler in the changing digital landscape

The global pandemic has accelerated digital transformation in businesses by as much as 7 years[1]. As the extent of digitalisation increases, so too, does the attack surface, and cyber-attacks such as ransomware are evolving from sporadic and isolated incidents into massive and systemic attacks. Cybersecurity has now become a critical enabler for businesses to navigate the changing digital landscape.

Cybersecurity as a competitive edge for businesses

Threat actors have also turned to supply chain attacks instead of targeting organisations directly, and this exploitation of supply chain vulnerabilities undermines the trust-based relationships that organisations have with their third-party partners. Organisations that have invested in and taken steps to implement cybersecurity becomes a competitive edge, as it helps them to build and maintain trust with their customers.

Guided approach for businesses through SG Cyber Safe Programme

No business – large or small – is safe from cyber-attacks. Smaller organisations think that they will not be affected by cyber-attacks because they are small and less important. While they may not be the primary targets, smaller organisations can become collateral damage or be targeted because they are part of a large organisation's supply chain.
The Cyber Security Agency of Singapore (CSA) has launched the SG Cyber Safe Programme to help organisations to better protect themselves in the digital domain and strengthen their cybersecurity posture. The Programme provides organisations with a guided approach to implementing cybersecurity.

1. Free cybersecurity resources for small organisations

Smaller organisations tend to have fewer resources for cybersecurity, and so CSA has published free cybersecurity toolkits that help small organisations prioritise what they need to implement first. Organisations can also consider being certified for their cybersecurity practices through the Cyber Essentials mark, which is designed to be achievable for small

[1] "How COVID-19 has pushed companies over the technology tipping point – and transformed business forever", McKinsey, Oct 2020

back to top

organisations. This is a visible label for the organisation to demonstrate that it has implemented basic cyber hygiene, which helps them to build trust with their customers. CSA has also onboarded Cyber Essentials "as a service" providers that can support smaller organisations in their cybersecurity journey.

2. Guided risk assessment for larger organisations

For organisations that have gone beyond baseline cyber hygiene, it is important to perform a risk assessment to establish their risk profile and review if they have implemented the corresponding cybersecurity measures that commensurate with their risk profile and appetite. CSA's Cyber Trust mark provides a guided risk assessment for organisations to do this, and organisations can also be certified for the Cyber Trust mark to demonstrate they have implemented robust cybersecurity in the organisation.

Cybersecurity as a team effort

Everyone has a role to play in strengthening cyber resilience. End user organisations may refer to CSA's website at https://www.csa.gov.sg/sgcybersafe for free cybersecurity resources to help them in raising their own cyber resilience. Technology and learning providers may also apply to CSA to be onboarded as providers to help organisations in their cybersecurity journey.

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

Article from SME Cybersecurity Conference Sponsor, softScheck

Cyber Trust Mark Advisory

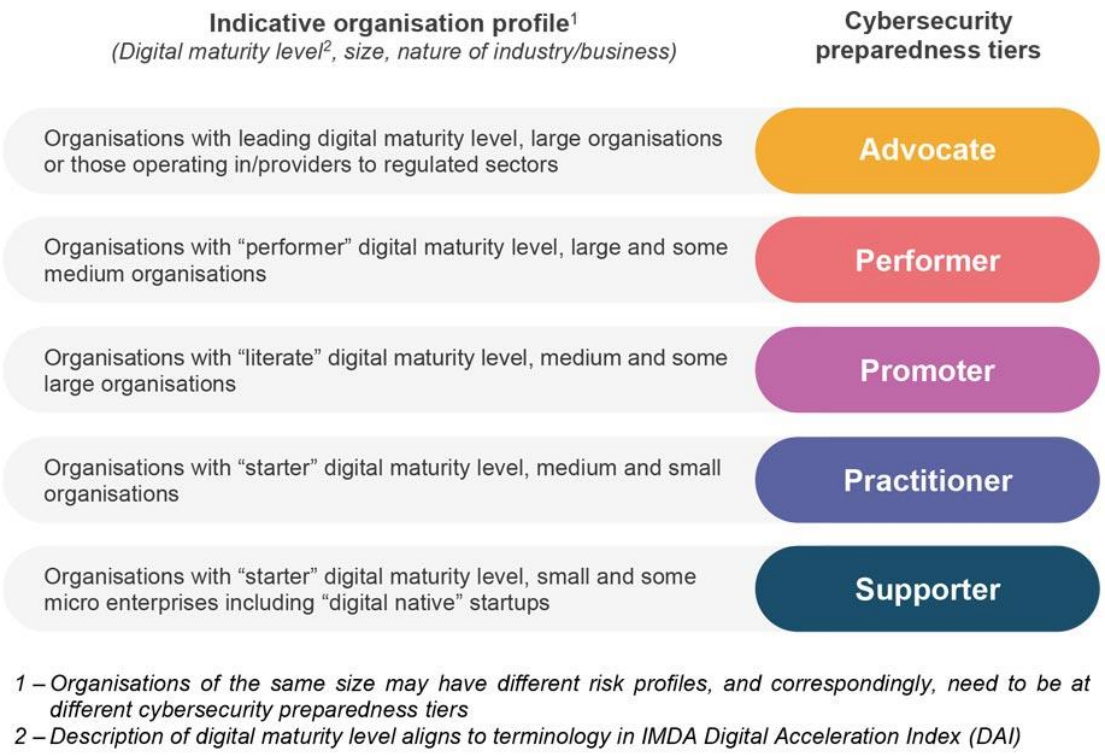
What is Cyber Trust Mark

Cyber Trust Mark is a cybersecurity certification issued by The Cyber Security Agency of Singapore (CSA). This serves as a mark of distinction for businesses who put in place good cybersecurity practices and measures that matches their risk profile.
(Note: Enterprise Development Grant (EDG) for CSA Cyber Trust Certifications is available!)

Indicative Organization Profiles and Cyber Security Preparedness Tiers

The five (5) different Cyber Security Preparedness tiers cater to the varying nature of organizations, sizes, and their digital maturity level. Depending on business needs, an organization may progressively improve their cybersecurity measures to reach the next tier.

back to top



*Source: Cybersecurity Certification for Enterprises – Cyber Trust mark (csa.gov.sg)

Who is Cyber Trust Mark Advisory for?

Do you find any of these statements true for your enterprise or business?

- Your business operations are robust and digitized
- You need to assess cybersecurity risks and preparedness
- You want to start implementing cybersecurity practices and international standards relating to IOT and cybersecurity such as ISO/IEC 27001 etc., but it seems daunting
- You are looking for a progressive pathway to adopt international information security standards (E.g., ISO/IEC 27001:2013)

If so, Cyber Trust Mark Advisory is suitable for you!

Cyber Trust Mark Advisory Objectives

- Increase business resilience
- Lower cyber risk and legal threat exposure

back to top

- Minimize risk of monetary penalties
- Earn trust and confidence from clients and partners
- Ensure a match of your cybersecurity risk and needs without over-investment

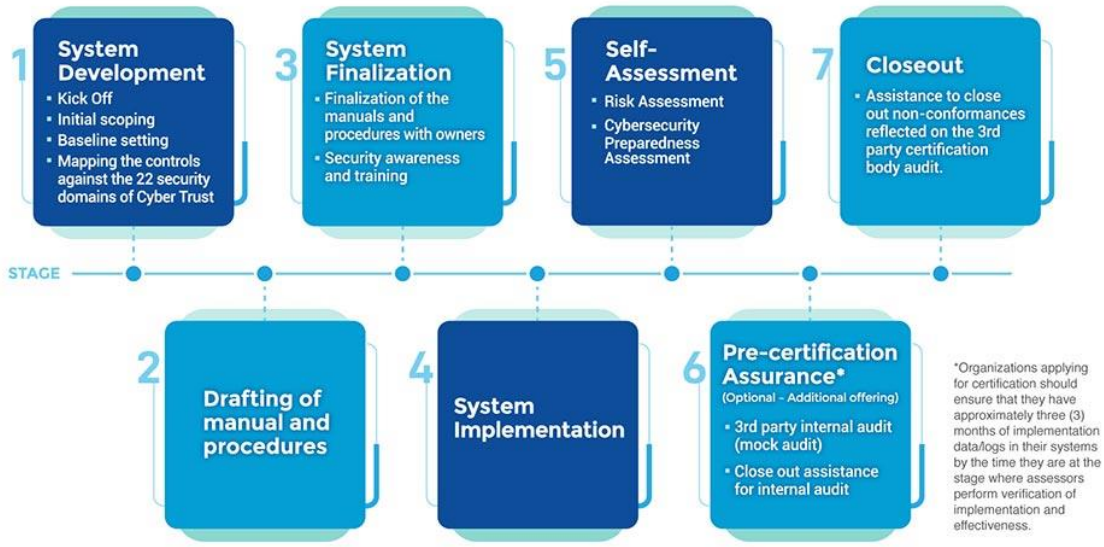
How can softScheck help me?

SoftScheck will help organizations achieve the Cyber Trust Mark in these ways:

- Provide expertise in areas of cybersecurity risk profile assessment
- Clear the path and provide a guided approach that saves time and hassle
- Support your organization through the arduous journey
- Substantially decrease the chances of failure

Approach and Methodology

Our goal is to handhold and walk with your organization throughout the various stages of your Cyber Trust Mark implementation and certification program. Our approach requires close engagement through the listed stages below:



Interested to know more? Contact Grace Fu, grace.fu@softscheck.sg today to find out more information!

back to top

Article from our Cloud Security Summit Sponsor, Armis

Identifying vulnerable critical assets that put you at risk

By Nadir Izrael, CTO and Co-Founder, Armis

Most organisations currently rely on vulnerability scanners to inform their day-to-day decisions. The problem with traditional scanners, however, is that they can only state which assets have what vulnerabilities. They cannot sort vulnerabilities based on their risk to the business or ongoing business operations.

Knowledge of a vulnerability itself is only the beginning of remediation efforts. Analysts must then gather whatever relevant asset attributes they can track down to make informed decisions. Yet pulling data from across endpoint management, EDR, VDI, cloud, and other organisational platforms is incredibly time-consuming. Moreover, varied data structures can lead to problematic correlations of asset information.

Overall, the cumbersome process often only leads to best guesses. It is all but impossible for security and IT operations teams to efficiently focus on the critical vulnerable assets that pose the highest risk to the business and gain control over the vulnerability management lifecycle.

When it comes to vulnerabilities, security and IT operations teams are facing a kind of "perfect storm". With every new asset deployed in support of growth, innovation, and efficiency efforts, the enterprise attack surface expands. The number of vulnerabilities is also rising rapidly year over year while the time it takes for attackers to exploit them is dropping. And with manual data-gathering approaches, the mean time to remediation (MTTR) has ballooned to 60 - 150 days.

One of the most effective ways to remediate risk is to access a real-time list of CVEs on connected assets. However, to prioritise efforts based on the organisational impact, there is a need to dig into the importance of every asset along with its relationships and dependencies within the environment. In other words, a clear understanding of the asset's business context is required.

Why context has become essential?
Did you know that most vulnerability scanners miss up to 40 percent of the assets in a typical scan of the organisation? This can be down to network restrictions, ephemeral type assets on Cloud, or missing or misconfigured vulnerability agents. Even for assets they can see, the sheer number of alerts combined with the lack of context makes it difficult to understand which of the critical vulnerabilities put critical assets at risk, and impossible to effectively prioritise them based on risk to the business.

back to top

Consider a bank with a list of thousands of CVEs, several hundred of which are deemed critical; not every critical vulnerability corresponds to a critical asset (based on function, location, and risk to the business). In fact, they are likely spread across assets with a low, medium, and critical impact on the business. But without context, all you can do is chase down every critical vulnerability as fast as possible. That may mean getting to an asset, such as a developer's laptop faster than a server running critical business banking applications. Delays and risks are only compounded as new vulnerabilities pop up. Moreover, despite avoiding incidents, it's a never-ending and very costly, cycle that is full of visibility gaps.

Establishing a single source of truth for assets, risks, and vulnerabilities

Armis Asset Vulnerability Management (AVM) eliminates cumbersome manual tasks, visibility gaps, and guesswork so organisations can focus on what matters most to vulnerability management. Our context and risk-based approach enable organisations to quickly identify and remediate the vulnerabilities that attackers are most likely to exploit in order of importance to the business.

Most importantly, AVM performs this multidimensional analysis on all of your assets continuously, providing up-to-date views of the attack surface and evolving vulnerabilities. Given how fast cyber threats are moving, real-time awareness of vulnerabilities, threats, and exploit attempts is now a necessity–not a nice-to-have.

AVM also provides full end-to-end vulnerability lifecycle management to assist and track remediation efforts. Moreover, leadership can use AVM to track the organisational effectiveness of the vulnerability strategy and make data-driven decisions on the state of the attack surface, ultimately helping establish a more strategic and streamlined approach to vulnerability management.

For any enquiries, please contact Ms Gwen Lee at gwen.lee@armis.com

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

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

back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

Hi, did you know ...

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

"The 20 Most Valuable Online Colleges in America,"

Graduate and Undergraduate Programs in Cyber Security

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

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

Hi, did you know ...

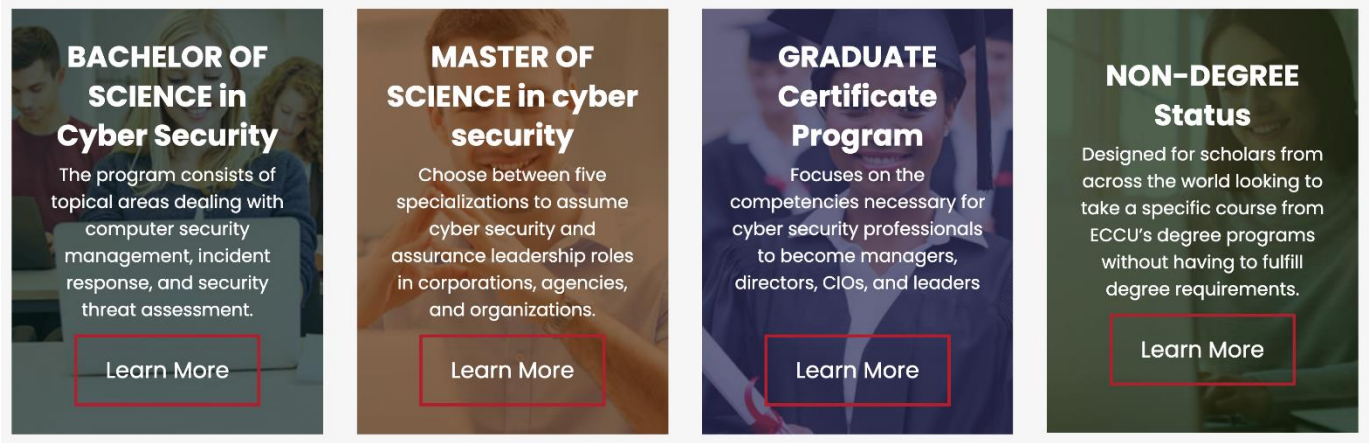
back to top

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

And...

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

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



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

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

back to top

Listing of Courses by ALC Council

Stand out from the crowd

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

We offer the most in-demand cyber certifications including:

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

The right training makes all the difference

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

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

back to top

AiSP Member Pricing – 15% discount

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

Upcoming Training Dates

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

Special Offers.

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

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

Thank you.

The ALC team

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

back to top

Qualified Information Security Professional (QISP®) Course

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

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

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

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

back to top

COURSE DETAILS

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

TARGET AUDIENCE

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

COURSE CRITERIA

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

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

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

Program Partner

Transformists NETWORK

Delivery Partners

Ai Network 360

OPUS ACADEMY

NETASSIST

back to top

Cybersecurity Essentials Course

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

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

Course Objectives

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

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

back to top

- Cloud Computing
- Cybersecurity Operations

COURSE DETAILS

Training dates for year 2022 and 2023 can be found on
https://www.aisp.sg/cyberessentials_training.html
Time: 9am-6pm
Fees: $ $1,600 (before GST)*
**10% off for AiSP Members @ $1,440 (before GST)*
***Utap funding is available for NTUC Member**
*** SSG Funding is available!**

TARGET AUDIENCE

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

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

back to top

MEMBERSHIP

AiSP Membership

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

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

On **membership application**, please do not email your personal data to us via email if your information or attachment is not password-protected. Please send us your password via **Telegram** (@AiSP_SG).

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

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

back to top

Sign up for AVIP MEMBERSHIP

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

BENEFITS

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

PRICE

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

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

back to top

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

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

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

Please check out our website on Job Advertisements by our partners.
For more updates or details about the memberships, please visit
www.aisp.sg/membership.html

AiSP Corporate Partners

back to top


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

back to top

Our Story…

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

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

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

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

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

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

back to top

