NEWSLETTER

December 2023

News & Update

- Knowledge Series
- SVRP
- AiSP Cyber Wellness
- Special Interest Groups
- CAAP
- The Cybersecurity Awards
- Digital for Life
- Regionalisation
- Annual General Meeting
- Corporate Partner Event
- Crest
- Upcoming Events

Contributed Contents

- IoT SIG: Internet of Things in Singapore: A Future Landscape
- 5 New Cybersecurity Challenges Chief Security Officers (CSOs) Should Be Aware of in 2023
- Career Progression through B.Tech in Computing, a Part-Time Work-Study Degree Programme at NTU
- GLOBAL ALLIANCE OF INDUSTRIES @ NTU (GAIN)

Professional Development

Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome DSTA, MySQL and Veracity Trust Network as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partners

Continued Collaboration

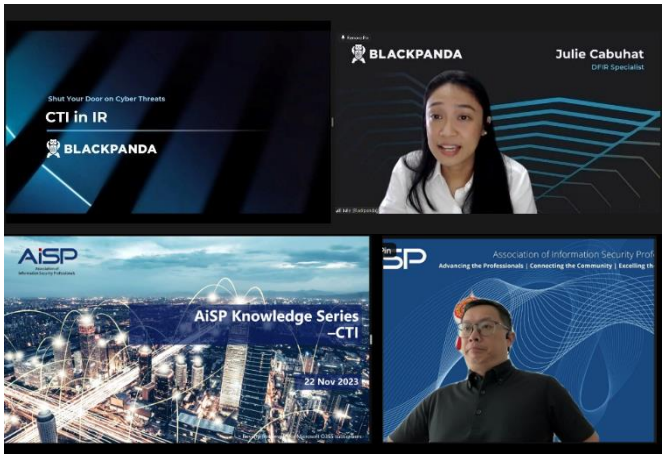
AiSP would like to thank CISCO, Detack, Grab, Responsible Cyber, softScheck, Wissen, YesWeHack, for their continued support in developing the cybersecurity landscape:

Knowledge Series Events

Cyber Threat Intelligence on 22 November

On 22 November, AiSP organised the Knowledge Series, focusing on Cyber Threat Intelligence where our Corporate Partners, Blackpanda and CrowdStrike shared insights with our attendees.

Thank you AiSP CTI SIG EXCO Lead, Mr Andrew Ong for giving the opening address. Shoutout to our Corporate Partner, Wissen International for sharing the cybersecurity courses during the webinar.



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 2024 are as follows (may be subjected to changes),

1. 14 Mar 2024, Cloud Security
2. 25 Apr 2024, Red Team
3. 9 May 2024, AI

Please email secretariat@aisp.sg for 2024 webinars if your organisation is keen to provide speakers!

back to top

Student Volunteer Recognition Programme (SVRP)

Student Volunteer Recognition Programme Awards Ceremony 2023

On 10 November, we held our fifth Student Volunteer Recognition Programme Awards Ceremony. Thank you AiSP Patron, Senior Minister of State for Ministry of Communications and Information, Mr Tan Kiat How for gracing the ceremony and presenting the Gold awards to the students.

Thank you Mr Wong Choon Bong for presenting the Silver awards to the students. Thank you SVRP Co-lead Mr Yu Pengfei for giving the welcome address and presenting the Bronze awards to the students.

Thank you Mr Breyvan Tan for presenting the Certificate of Merit to the students. We would like to thank our Academic Partner, Nanyang Polytechnic for hosting us at their beautiful premise.

We would also like to thank Cyber Security Agency of Singapore (CSA) and Wissen International for supporting the awards ceremony.

AiSP will be working with EC-Council to create information security training and certification programme. It represents a partnership aimed at fortifying the knowledge and skills of our cybersecurity professionals. With this collaboration, EC Council will be awarding 500 free exam vouchers across all polytechnics and Institute of Technical Education (ITE) students over the next two years.

Congratulations to all award winners.

back to top

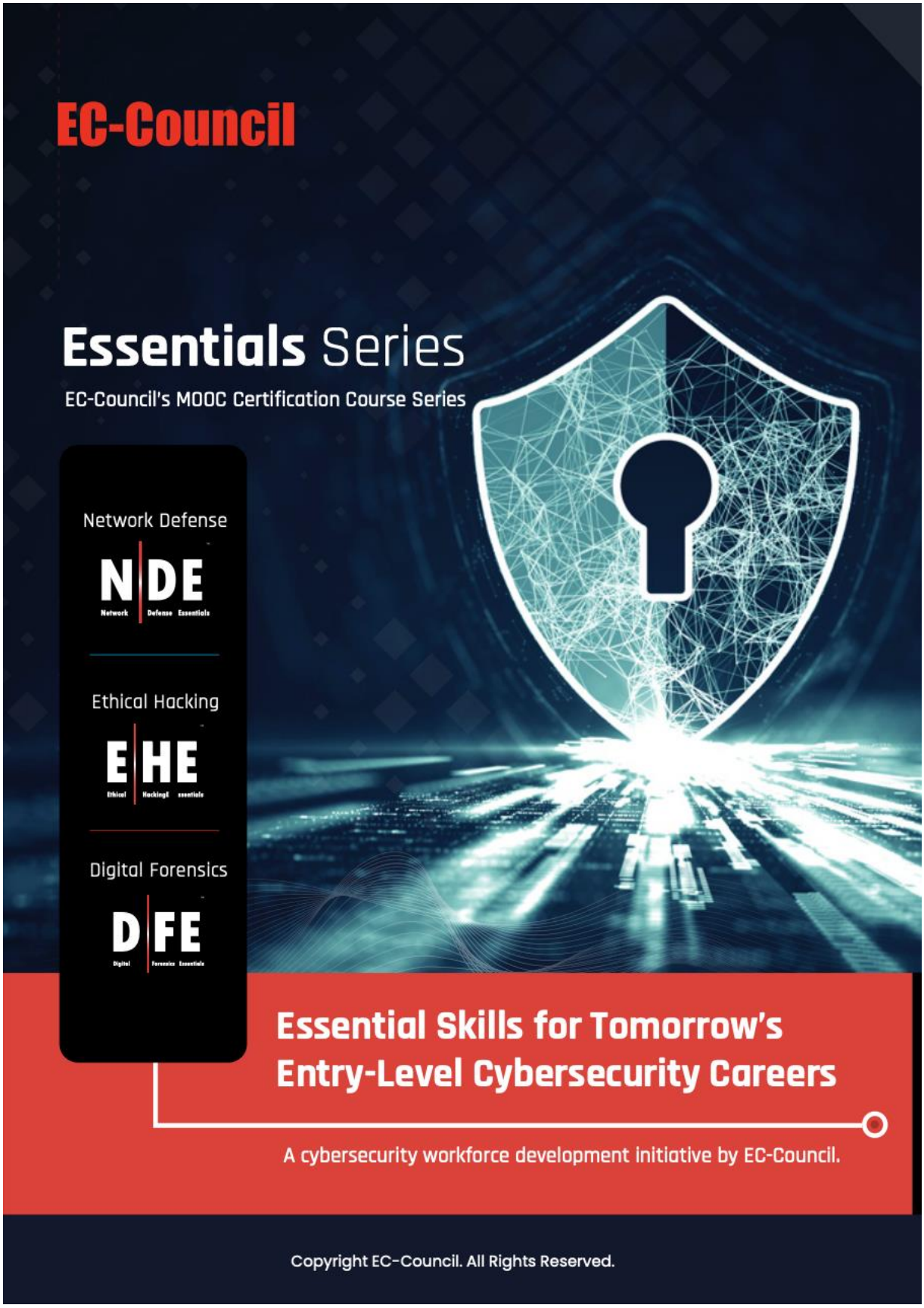

Elevating Cybersecurity Education Through Unprecedented Collaborations

In a pioneering initiative, EC-Council and Wissen have forged a collaboration with AiSP. This collaboration includes a sponsorship of 500 EC-Council Cyber Essentials certification vouchers. These vouchers aim to empower Polytechnic and Institute of Technical Education (ITE) students pursuing cybersecurity programs, enabling them to attain their inaugural industry certificate and commence their journey with EC-Council Essential certificates (NDE, EHE, DFE), thereby initiating their cybersecurity credentialing process.

Visit (https://www.wissen-intl.com/Essential500.html) and register to start your cybersecurity credentialing journey! Terms & Conditions apply.

About the EC-Council Cyber Essentials Certification
EC-Council's Essentials Series is the first MOOC certification course series covering essential skills in network defense, ethical hacking, and digital forensics. The Network Defense Essentials (N|DE), Ethical Hacking Essentials (E|HE), and Digital Forensics Essentials (D|FE) are foundational programs that help students and early career professionals choose their area of competency or select a specific interest in cybersecurity. The Essentials Series was designed to give students the foundation on which to build and develop the essential skills for tomorrow's careers in cybersecurity. These programs educate learners in a range of techniques across industry verticals, such as securing networks, mitigating cyber risks, conducting forensic investigations, and more.

back to top



back to top

AiSP Cyber Wellness Programme

Organised by: AiSP Advance Connect Excel

Supported by: INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In Support of: DIGITAL FOR LIFE

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

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

AiSP IOT Security Sharing at NTU 2023 on 3 November

AiSP IoT Day was held in Nanyang Technological University Singapore on 3 November, focusing on "Empowering Tomorrow's IoT: Unveiling the Shield of Innovation and Igniting Lifelong Learning". Thank you Senior Minister of State, Ministry of Communications and Information & Ministry of Health, Dr Janil Puthucheary for gracing the event and AiSP Vice President Andre Shori for giving the welcome address.

Big thank you to our Corporate Partners, Armis, Cisco, Eclypsium, Fortinet, softScheck and Vectra AI for supporting the event. Thank you Nanyang Technological University for hosting us.

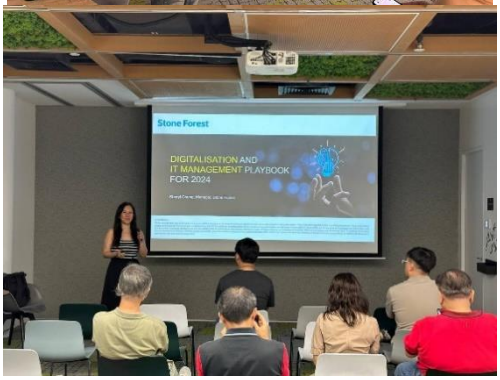
back to top

back to top

Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP Advisory Clinic on 17 November

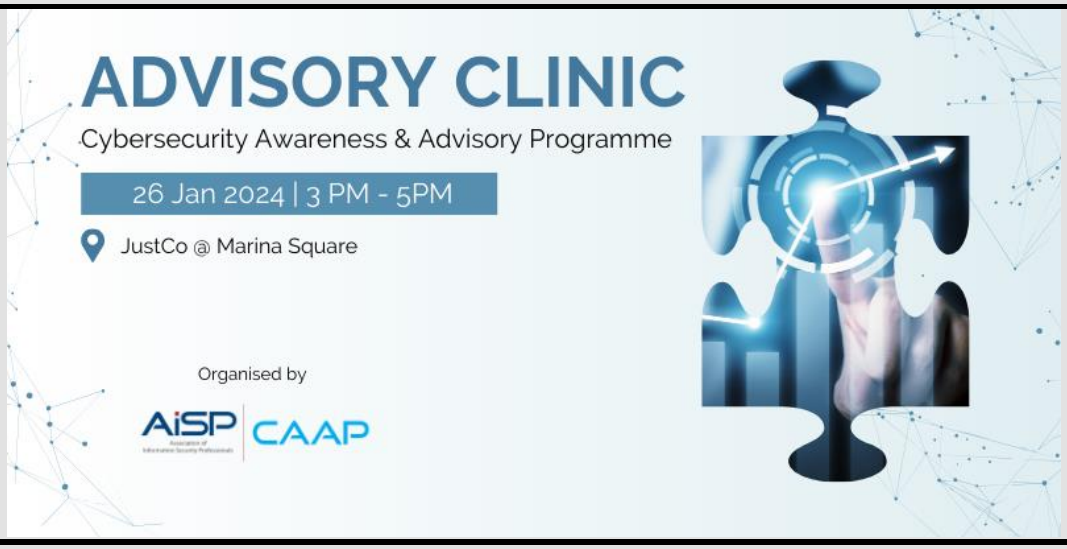
As part of AiSP Cybersecurity Awareness & Advisory Programme, we held our very first Advisory Clinic on 17 November. Thank you AiSP Vice-President, Tony Low, Workforce Singapore - WSG, SGTech & our Corporate Partner, RSM Singapore for sharing at the event. Thank you, our Advisors for providing the advisory knowledge to our attendees.



back to top

AiSP Advisory Clinic on 26 January 2024

AiSP Advisory Clinic



As part of AiSP Cybersecurity Awareness & Advisory Programme, AiSP hope to elevate CyberSecurity Awareness as integral part of SME Business Owner Fundamentals and Establish a Self-Sustainable Support Ecosystem programme with active participation from Agencies, Business Associations, Security Communities and Vendors.

Targeted for Singapore SMEs, the CAAP aims to drive digital security awareness and readiness. Supported by CSA, Our CAAP operating committee focuses on:

1. Enhance security awareness and training
2. Create cohesive security knowledge resources
3. Offer security solutions and service support

AiSP will be organising our advisory session and we would like to invite you to participate in our advisory clinic. Please see below for the details.

Date: 26 Jan 2024
Time: 3pm – 5pm
Venue: Justco @ Marina Square
Topic: Asset discovery, understand your current landscape
Objectives: this is the workshop clinic that will help to training SMEs and their staff to

- develop an initial inventory of their digital assets to better determine importance
- define priority of the asset
- determine how it should be protected at what price.

Our advisors will assist you to develop implementation plan for your own company and guide you along your implementation journey.
Registration: https://forms.office.com/r/PCZeVC7uJT

back to top

The Cybersecurity Awards

TCA 2023 has concluded on 13 October 2023. The Cybersecurity Awards 2024 nominations will start in February 2024.

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 2024! Limited sponsorship packages are available.

back to top

Digital for Life

Digital for Life Festival on 4-5 November

As part of Digital for Life movement, AiSP participated in the Digital for Life Festival from 28 Oct - 12 Nov. The second edition was held on 4-5 November with our corporate partner, Cisco at Heartbeat @Bedok. Thank you DFL Steering Committee and AiSP Patron, Senior Minister of State for Ministry of Communications and Information, Mr Tan Kiat How for visiting our booth.

Digital for Life Festival on 11-12 November

AiSP participated in the Digital for Life Festival from 28 Oct - 12 Nov. The third edition was held with our Corporate Partner, Wissen International at Toa Payoh Hub. Thank you Member of Parliament, Mr Saktiandi Supaat and Minister of State, Ministry of Education & Ministry of Manpower, Ms Gan Siow Huang for visiting our booth and interacting with our Nanyang Polytechnic students.

back to top

Bukit Batok East AAC Wellness Day 2023 on 3 December

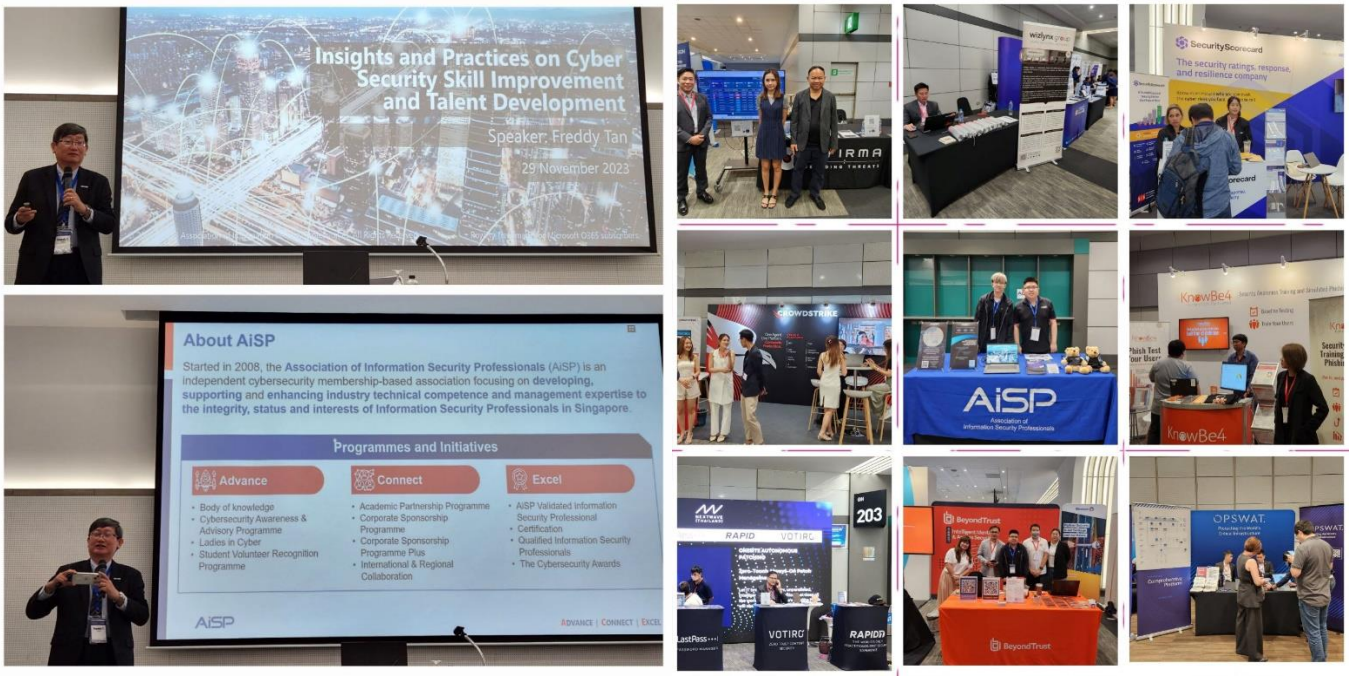
back to top

Regionalisation

CDIC Bangkok on 29 – 30 November

Together with our 8 other Corporate Members: BeyondTrust, CrowdStrike, CYFIRMA, KnowBe4, OPSWAT, SecurityScorecard, Votiro and wizlynx group, AiSP went to Bangkok for the Cyber Defense Initiative Conference (CDIC) 2023 from 29 – 30 November.

Our AiSP EXCO and Fellow Member Mr Freddy Tan was also in Bangkok CDIC Conference and shared with everyone at CDIC on the Insights and Practices on Cyber Security improvement and Talent Development. Thank you Freddy for taking time to travel to Thailand to share with everyone at CDIC 2023.



XCION 11th Conference 2024

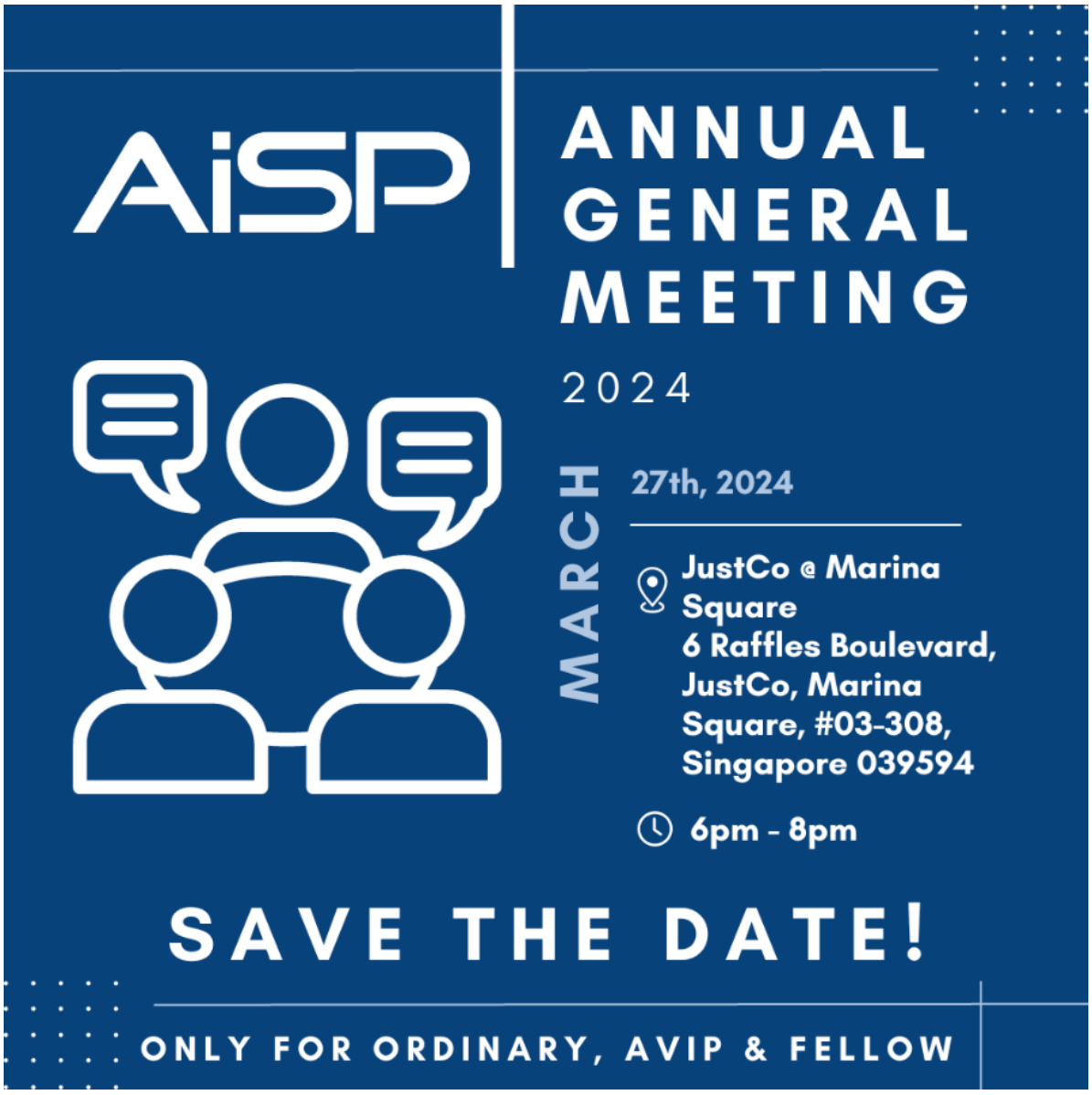
AiSP will be supporting the XCION 11th Conference at Bali happening from 4 March 2024 to 6 March 2024. The Theme for 2024 is Charting the Future with Innovative and Secured Technologies. It will be attended by the Indonesian CIO Network (https://www.linkedin.com/groups/3942786/). As our valuable AiSP Corporate Partners, we are pleased to offer you a 20% if you are interested to speak at the event by been a sponsor.

Do contact AiSP Secretariat at secretariat@aisp.sg for the sponsorship package. Please note that it is based on first come first served basis and the organisers have more than 10 sponsors enquiring on it already. There will be 20% discount for our Corporate partners. No discount if you to go direct to the organisers or sign up at the website.

back to top

Please see some of the highlights of the video (https://www.youtube.com/watch?v=-eM-hNtMFZ0) happening on the 10th XCION 2023 that took place earlier this year March 2023.

Annual General Meeting



back to top

Corporate Partner Event

A Proactive Approach to Protecting Public-facing Infrastructure

You would have heard in the news about DDoS attacks, websites being down due to attacks. With advanced adoption of generative AI, it is very challenging to keep up with targeted adversary campaigns.

Securing and managing infrastructure with actional insights is critical to our enterprise resiliency and spans beyond cyber resilience to include financial and operational resiliency. In addition to resiliency, driving efficiency into our infrastructure management is also a step towards your ESG program – ensuring our digital transformation limits impact to our environment.

Global Adversary Signals Analytics for Advanced Threat Intelligence
Speaker: Niel Pandya, APAC Business Development Lead, Cybersecurity , OpenText

In this session we will look at the underlying challenge and how modern-day signals intelligence can help close the gap on adversary activity, enabling us to be proactive when it comes to protecting public facing infrastructure. Signals feed into machine models to help us identify patterns in communication without compromising privacy. Observing signals flow helps us determine if the origin of these signals are from risky geographies or devices. It is like monitoring the internet and communications to your infrastructure.

Tame costs and Secure Cloud Infrastructure
Speakers:
Niel Pandya, APAC Business Development Lead, Cybersecurity , OpenText

back to top

Jonathan Ho, Technical Director, Southeast Asia , OpenText
Donald Ong, Senior Consultant, Cloud Cybersecurity Programme Office (CCPO)
Cyber Security Agency of Singapore

Whether you have a cloud-first , or hybrid infrastructure strategy, this session explores how you can gain better insights to optimise cloud spend with FinOps, and how we can protect both infrastructure and data better, at scale, to overcome cloud management roadblocks. We will look at the challenges in managing infrastructure efficiently – to help reduce operational cost through AI, machine learning and automation and reducing cost incurred through loss of service availability and quality.

Date: 18 January 2024, Thursday
Time: 3PM – 5PM, Registration starts at 2.30PM
Venue: Marina Square
Registration: https://events.opentext.com/en-sg-aisp-cybersecurity-workshop/register?ref=aisp

CREST

New CREST Registered Penetration Tester (CRT) exam offered globally for the first time with up to 75% off until 31 January 2024

New CRT exam now available for the first time in over 70 countries at over 1,000 Pearson VUE test centres, including Singapore and across Asia.

back to top

- To celebrate the launch of the new exam, CREST is offering 75% discount for anyone who works at a member company and 40% off for everyone else until 31 January 2024.
- Exams must be booked by 31 January 2024 in order to take advantage of the promotional period and taken by 30 April 2024.
- For more information and/or to book a CRT exam, please visit our dedicated webpage: https://www.crest-approved.org/skills-certifications-careers/crest-registered-penetration-tester/

CREST, an international not-for-profit, membership body representing the global cyber security industry, has launched its new Registered Penetration Tester (CRT) certification globally. It is now available in over 70 countries and in over 1,000 Pearson VUE test centres, offering greater availability to anyone looking to enhance and develop their cyber security skills to industry standards.

Reflecting the ever-changing needs of the cyber security sector, CREST has also updated the CRT exam. CRT is an intermediate level exam that tests a candidate's ability to carry out penetration testing tasks. It offers a greater depth of knowledge testing and introduces new content and sections that were not previously covered. Content now includes a wider range of topics – including Windows and Linux file permissions, processes and exploitations, mail and OS command injection and Web Application logic flaws, to name a few. CREST's expert assessors updated and added the new content to the exam, and it has all been rigorously tested by them.

Nick Benson, CREST CEO, said: "CREST's goal has always been to raise the quality and professionalism of cybersecurity practices, leading the way in penetration testing and vulnerability assessment as well as red teaming, incident response and threat intelligence. Our commitment to ensuring cybersecurity professionals adhere to rigorous ethical and technical standards is exemplified by the growing popularity and recognition of our CRT qualification internationally."

CRT is one of CREST's most popular exams, recognised by employers, buyers of cyber services and regulators alike across the world. It is mandated in many regions globally as the standard required and remains the technical exam aligned to NCSC's CHECK Team Member in the UK. The new CRT retains the high standards and security expected of CREST exams to ensure it will continue to be a badge of honour for the individual and a demonstration of competence for employers and regulators.

CREST is offering the new CRT exam with a 75% discount for anyone who works at a member company and 40% off for everyone else. The launch promotional period runs from now until 31 January 2024. Candidates who wish to take advantage of this promotional period must book their new CRT exam by 31 January 2024 and have taken their exam by 30 April 2024.

back to top

Candidates still need to hold a valid CREST Practitioner Security Analyst (CPSA) certification before sitting the CRT exam. CREST's CPSA exam is also available widely at Pearson VUE centres and is also discounted during the launch promotional period.

Andy Woolhead, CREST Head of Cyber Skills and Certifications, said: "We have fully refreshed the exam, retaining the high calibre that our member companies and exam candidates expect. We have gone to great lengths to ensure the quality of the new exam, with the support of our expert assessors and the broader CREST Community. The new CRT test is more evenly balanced across infrastructure and web and a larger skillset is tested. This is all part of our remit to fully support cyber security professionals everywhere in their ongoing professional development.

"CREST research has shown us that the quality of Pen Tests varies enormously and that the lack of defined standards complicates the landscape. The CRT exam has been designed to reflect current Pen Test practice and to accurately assess an individual's knowledge, skills and experience. Available to take in over 70 countries, we are seeing more of a logical progression to standardisation across the sector – which can only be a good thing."

CREST certifications ensure cyber professionals are qualified, ethical and capable. Offering CREST's updated globally recognised CRT qualification more widely is an important step towards creating greater standardisation in the largely unregulated cyber security industry.

Pearson VUE is a well-known global computer-based testing (CBT) and assessment services provider which importantly provides physical proctoring to ensure the integrity of the exam. The new exam now features a virtual machine (VM) of tools accessible during the exam that candidates can familiarise themselves with as part of their preparation, rather than candidates bringing their own laptop.

CREST provides a recognised career path from entry into the industry through to experienced senior tester level. CREST works with a large number of technical information security providers who support and guide the development of its examination and career paths.

For more information and/or to book a CRT exam, please visit our dedicated webpage: https://www.crest-approved.org/skills-certifications-careers/crest-registered-penetration-tester/

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
1 Dec	TCA 23 Judges Appreciation	AiSP
3 Dec	Bukit Batok East Active Ageing Committee Wellness Day	Partner
9 – 10 Dec	STANDCON 2023	Partner
2 Jan	School Talk at St Margaret Secondary School	AiSP & Partner
15 Jan	School talk at Bukit Panjang Government High School	AiSP & Partner
16 Jan	Learning Journey to RSM for Bukit Panjang Government High School	AiSP & Partner
18 Jan	Learning Journey to RSM for Bukit Panjang Government High School	AiSP & Partner
18 Jan	Event with Opentext	AiSP & Partner
23 Jan	TESA Programme with SMS Tan	AiSP & Partner
31 Jan	AiSP x NTUC x TTAB Networking event	AiSP & Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Internet of Things SIG

Internet of Things in Singapore: A Future Landscape

What is IoT?

The Internet of Things (IoT) is a system of connected objects or "things" that contain sensors, software, and other technologies capable of exchanging data with other objects. They are usually referred to as "smart" devices.

TechTarget also describes the Internet of Things as "a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."

While not all IoT devices require an internet connection to work, they do require a network connection to automate some operations, issue commands, or update their setup.

back to top

IoT in Singapore

In Singapore, both the private sector and the government are starting to outline their approach to IoT.

The Singapore government has already established an IoT technical committee to develop IoT foundational standards in the architecture, interoperability, security, and data protection industries.

In March 2017, the Open Connectivity Foundation (OCF), a leading IoT standards body, collaborated with the Singapore Semiconductor Industry Association (SSIA) to allow IoT devices to seamlessly communicate with one another regardless of manufacturer, operating system, and chipset of physical transport. The collaboration allowed SMEs and startups in the Singapore Smart Nation ecosystem to understand and adopt the specification in their design strategies.

As of today, five IoT standards have been published by Singapore's Infocomm Media Development Authority (IMDA) together with Information Technology Support Center (ITSC)'s Technical Committee. These IoT standards serve as a guide to create an ecosystem of interoperable sensor network devices and systems. They guide the application, development, and deployment of these devices for public areas, multiple industries, and homes in Singapore.
Of course, as security plays a big part in the IoT ecosystem, guidelines for IoT security for a smart nation have also been established.

How IoT Works

Now that we know what the "things" in the internet of things refer to and how they are interconnected, how do IoT devices work?

Essentially, the IoT ecosystem is made up of "smart" devices that gather, share, and analyze data using embedded systems such as sensors, chipsets, and communication hardware.

IoT devices send the data through an IoT gateway. These processes are often automated, requiring no human involvement. That said, people can still interact with the devices or access the data.

IoT can also leverage artificial intelligence (AI) and machine learning to collect data faster and make processes more dynamic.

back to top

What are the IoT Applications

There are various IoT applications across all industries including healthcare, manufacturing, transportation, and consumer retail. Most notably, the IoT gave rise to smart homes and buildings as well as industrial automation. Hospitals and healthcare facilities in Singapore are also starting to adopt IoT in their environment.

IoT applications in Singapore help industries simplify, automate, and control processes with speed and accuracy. Since IoT has many notable applications, new business models and revenue streams can be built as they allow businesses to create real-time data to develop new products and services.

For example, data collected by IoT devices helps businesses analyze big data with quick speed and accuracy. This quick analysis of data can help businesses improve services and products at a quick pace as compared to manually collecting and analyzing them, which could take years to accomplish.

Another example is how wearable health-tracking devices can keep track of patients' heart rates remotely and the data can be analyzed in real-time. This enables doctors to detect irregularities and monitor a patient so they can provide the patients with the needed care as soon as symptoms show up.

IoT Components

There are five distinct components in IoT:

- Devices or Sensors – The devices are fitted with sensors and actuators to collect data from the environment to give to the gateway. Meanwhile, actuators perform the action (as directed after processing of data).
- Gateway – The collected data from the devices and sensors are then sent to the gateway and some pre-processing of data is done. The gateway also acts as a level of security for the network and transmitted data.
- Cloud – The collected data are then uploaded to the cloud, which is a set of servers connected to the internet.
- Analytics – After being received by the cloud, various algorithms are applied to the data for proper analysis of data
- User Interface – User can monitor and control the data in this final component.

back to top

Major Components of IoT

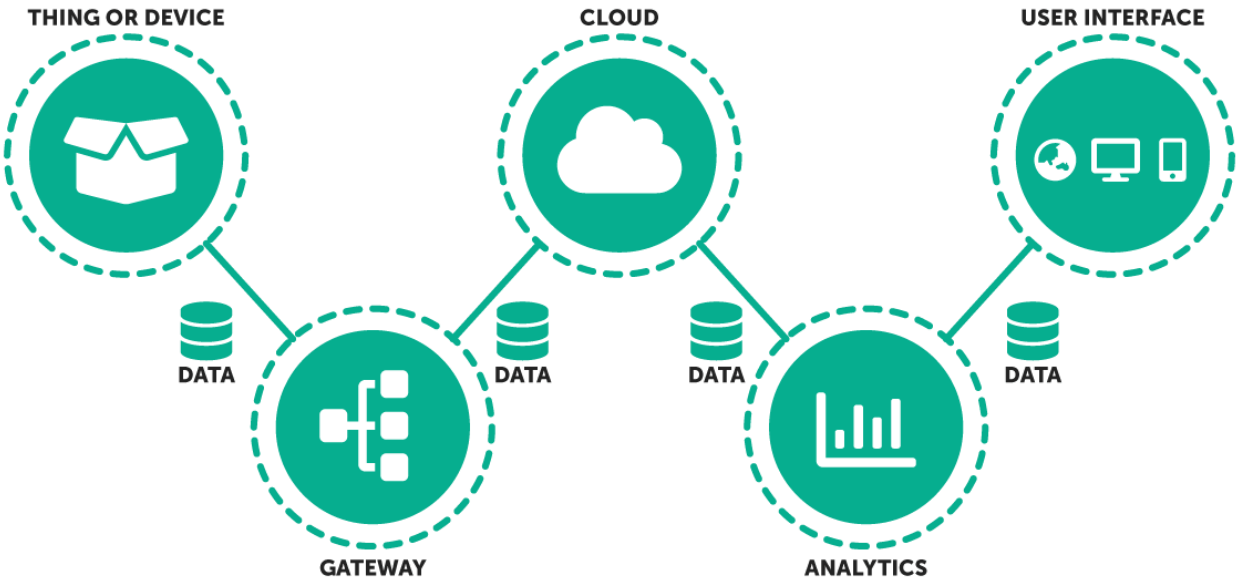


Image source: RF Page https://www.rfpage.com/what-are-the-major-components-of-internet-of-things/)

IoT Devices

IoT Devices Examples

There are several top IoT devices in the market, such as:

- Smart Mobiles
- Smart refrigerators
- Smartwatches
- Smart fire alarms
- Smart door locks
- Smart bicycles
- Medical sensors
- Fitness trackers
- Smart security systems and others

back to top

IoT for Security

Why Privacy and Security is Important in IoT

The number of linked IoT devices around the world has increased exponentially in recent years. By 2030, an estimated 50 billion IoT devices will be in use worldwide. As more device makers join the IoT ecosystem, it is important to note that security must not remain an afterthought. Without proper security put in place, hackers can easily gain access to personal data and seize the object's functionality.

What are the Biggest IoT Security Risks and Challenges?

- Poorly secured smart devices – They may compromise sensitive data. Moreover, attackers can target critical information structure.
- Lack of encryption and access controls – without encryption and access controls put in place, there is a big potential for a breach or compromised data.
- Lack of device management – unmonitored and improperly managed IoT devices can prevent organizations from detecting an immediate threat. When a device is compromised or tampered with, the effects are irreversible.
- Weak passwords – inconsistent management of passwords may give hackers the upper hand to compromise an entire business network. If one employee does not adhere to the security policy, password-oriented attacks increase. Since devices are interconnected, one compromised device may cause a domino effect.

How to Improve IoT Security

As part of its efforts to strengthen IoT security, boost overall cyber hygiene standards, and better safeguard Singapore's cyberspace, the Cyber Security Agency of Singapore (CSA), a national cybersecurity organization, has introduced the Cybersecurity Labelling Scheme (CLS) for consumer smart devices.

The CLS is the region's first of its sort in Asia-Pacific. Smart gadgets will be graded based on their cybersecurity provisions under the plan. This will allow consumers to discover items with stronger cybersecurity features and make more educated purchasing decisions.

Security for IoT Devices

Providing software protection is one of the main ways to secure IoT devices. Ensuring the security of device identity for connected devices through a strong IoT identity platform is a must.

back to top

To successfully manage IoT devices, organizations must develop unique strong device identities to account for all potential breaches.

Public Key Infrastructure (PKI)-enabled strong device identification can allow the principles of IoT security:

- Authentication
- Encryption
- Integrity

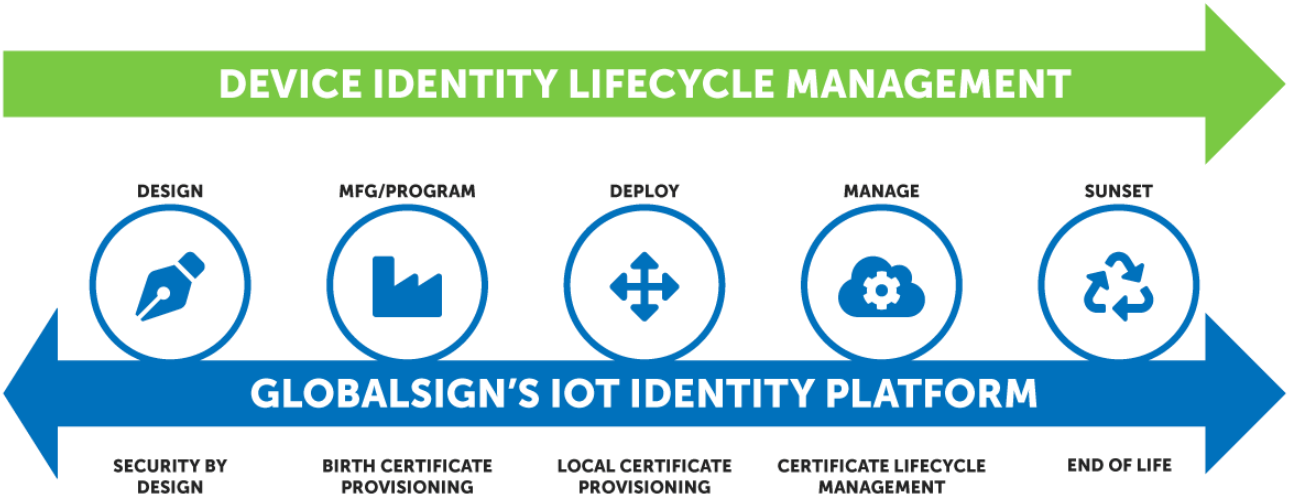
GlobalSign IoT Solutions

Here are some solutions that can be applied within the business landscape of all industries leveraging the benefits of IoT devices:

GlobalSign's IoT Identity Platform is the perfect solution for managing IoT device identity. It taps on the power of PKI backed by digital certificates with these innovative products:

- IoT CA Direct – helps operate and secure device identity lifecycle management program through a trusted, cloud-based commercial certificate authority (CA).
- IoT Edge Enroll – ensures secure device enrollment and provisions unique, strong, and secure device identities.

The IoT Identity Platform enables IoT Device Identity Lifecycle Management. Organizations can secure and manage their IoT device identities, from certificate issuance to renewals and revocations.



We also have our IoT Developer Program for IoT developers and organizations looking for top-level technology to streamline and secure device identities. The IoT Developer

back to top

Program and Portal provides a centralized platform where developers can access all the tools required to successfully integrate device identity provisioning. Organizations can also make devices stronger and more secure by collaborating and partnering with the GlobalSign IoT Solutions Group, a trusted IoT security partner for device identities, through the IoT Partner Program.
Here's all you need to know about our IoT security solutions and how they can meet the needs of businesses of all sizes.

Fighting and monitoring cybersecurity threats and IoT-related challenges to your company is essential for business continuity and security, but the process is incredibly difficult and time-consuming. A robust security solution is what most companies today need. A cybersecurity solution by GlobalSign is geared towards providing and securing device identities for IoT devices.

GlobalSign has a PKI-based cloud IoT Identity Platform designed for flexible, adaptable, and extensible IoT security. PKI provides a trustworthy IoT experience that is backed up by secure digital certificates issued by a reputable Certificate Authority (CA). You can request for a demo with us today to see how this solution can work for your business or you can speak with us to learn more about our IoT Device Security solution.

back to top

Article from IoT Partner, Nanyang Technological University

5 New Cybersecurity Challenges Chief Security Officers (CSOs) Should Be Aware of in 2023

November 2, 2023
| Executive Management

If you're a chief security officer (CSO), chief information security officer (CISO), or other cybersecurity leader, your job is never dull. Technology is constantly evolving, as are the threats to an organization's data and intellectual property. No chief security officer can rest on their laurels because each year brings new challenges. And 2023 is shaping up to be one of the most challenging years yet.

Here are five of the top new cybersecurity challenges for a chief security officer in 2023—and what you can do about them. If you're not a cybersecurity leader yet but hope to be one someday, you can still enjoy this look at 2023's top CISO challenges.

The 5 Most Recent Cybersecurity Threats That CSOs Need to Know About
From the cloud and AI (Artificial Intelligence) to data regulations, the top cybersecurity threats for a chief security officer in 2023 reflect current trends in technology and the world at large, including:

Security Control Gaps Due to AI and Cloud
2023 will likely go down as the year that AI went mainstream. The popularity of ChatGPT, Google Bard, and other interactive chatbots brought the power of AI, large language models, and machine learning to even non-technical users. While these developments have mostly been a net positive for the world, bad actors have also discovered the power of AI. With many cybersecurity tools and apps now using machine learning algorithms, it can be difficult to tell whether AI is good or bad for security professionals (Greer, 2023).

A chief security officer in 2023 can expect to see more realistic phishing emails and other social engineering attacks, thanks to machine learning's ability to mimic human speech. The speed at which AI operates has also led to an increase in automated exploits. Hackers can simply input a few parameters, watch AI perform automated vulnerability scanning, and then generate custom code to exploit those weaknesses.

At the same time, the enterprise shift to the cloud has been accelerated ever since the

back to top

start of the COVID-19 pandemic. The increased prevalence of remote work that started in 2020.

Is in full swing in 2023, creating another control gap for chief security officers. Cloud environments can be particularly vulnerable to data breaches if they are improperly secured. A cloud platform's identity and access management (IAM) can suffer from weak authentication methods and misconfiguration. A chief security officer in 2023 must adapt modern tools and solutions to close gaps between AI and the cloud.

Multicloud Adoption and Cloud Data Breaches

The shift to the cloud is so accelerated that many CSOs are now faced with securing a multicloud environment. However, each new cloud app or platform is also a potential new attack vector, making cloud data breaches one of the most pressing concerns in 2023.

One of the bigger hurdles for multicloud infrastructures is the difficulty of enforcing policy across different cloud apps or platforms. Security teams also may not get proper training on each new service, potentially leading to an increase in cloud data breaches. Even in the best cases, meeting compliance requirements across multiple clouds can be complex and requires careful planning.

A chief security officer should always be heavily involved in the process of evaluating new apps and platforms. That way, they can understand the security implications of bringing new systems online. The CSO should ensure that security considerations are a part of any new project's budget so that a multicloud adoption doesn't mean added data breaches.

Threat of Litigation with New Governing and Data Norms

While each new cloud service or platform brings new cybersecurity threats, that may be the tip of the iceberg. In the years since the European Union passed the General Data Protection Regulation (GDPR), other governments have passed several information privacy laws. Employee or customer data exposed in a data breach could violate these regulations, leading to the threat of litigation.

For example, in early 2022, the United Kingdom government announced plans to update its cybersecurity framework. The revised legislation is expected to expand the type of cyber incidents that must be reported to regulators (Ivory et al., 2023).

This is especially concerning when you consider that cyber attacks are getting more sophisticated with the use of AI and machine learning algorithms, deep fake

back to top

technology, and advanced phishing attacks. For companies with a presence in multiple jurisdictions, the chief security officer now has to become an expert in data security laws and evolving societal norms around data usage.

Catastrophic Weather Events Impacting the Business Continuity
Every year has its fair share of extreme weather events, but 2023 has had more than its fair share. From Cyclone Freddy in February to the unprecedented wildfires in Hawaii in August, not a month has passed without a catastrophic event (Rao, 2023). This shifts the chief security officer's concern from the virtual world to the physical one. Each extreme weather event disrupts power, cellular communications, and internet access, posing a grave threat to business continuity.

Beyond the disruptions lie other headaches for CSOs. Cybercriminals might even take advantage of the chaos around weather disasters and ramp up phishing and social engineering attacks. Data centers and off-site backup locations might become compromised, leading to serious concerns about data safety.

More than ever, CSOs must invest in disaster recovery, ensuring that cybersecurity and data availability plans are in place. Backup and redundancy for critical systems should be in place, with response plans tested. It also wouldn't hurt for cybersecurity teams to add weather monitoring to the alerts that their teams already receive. Extra preparation time can make all the difference in the case of catastrophic weather events.

IoT and 5G Security Gaps
The rollout of the 5G network represented one of the most significant upgrades ever to global internet connectivity. The increased speed, bandwidth, and capabilities of 5G are all positive developments. The technology has also led to an increase in the number of connected Internet of Things (IoT) devices. The number of 5G IoT connections is expected to increase from 17 million in 2023 to 116 million by 2026 (Juniper Research).

However, IoT devices have their own set of security concerns. Many use unprotected APIs for easy sharing of data, but this creates potential risks for enterprise data. Weak authentication methods are common among lower-cost IoT devices. Even worse, some IoT devices are set up outside the IT department and still use default passwords, leaving them wide open to attackers.

As IoT installations become larger with the advent of 5G, it's time for CSOs to start plugging the security gaps. Procedures should be implemented to keep firmware updated, and APIs should be protected with strong authentication. Security software vendors are also adding IoT-specific features to their packages, which security teams should investigate.

back to top

How Information Security Management Training Such as C | CISO is Useful

Finding new cybersecurity leaders is one of the top priorities for organizations worldwide. If you want to be considered for these roles, it's time to look at a certification program that has trained cybersecurity leaders worldwide, such as EC-Council's Chief Information Security Officer (C | CISO). The C | CISO certification offers world-class training in all of the issues facing cybersecurity leaders today, including governance, information security controls, strategic planning, and more.

References

Greer, R. (2023, September 12). Artificial intelligence in cybersecurity: Good or evil? CIO. https://www.cio.com/article/651967/artificial-intelligence-in-cybersecurity-good-or-evil.html

Juniper Research. 5G IOT CONNECTIONS TO SURPASS 100 MILLION FOR FIRST TIME GLOBALLY BY 2026; ACHIEVING 1,100% GROWTH OVER THREE YEARS. https://www.juniperresearch.com/pressreleases/5g-iot-connections-to-surpass-100-mn

Ivory, A. Pittman, F. P., Timmons, J., Caisley, L., Burke, A., Hahn, A. A., & Turgel, D. (2023, march 22). Cybersecurity Developments and Legal Issues. White & Case https://www.whitecase.com/insight-alert/cybersecurity-developments-and-legal-issues

Rao, D. (2023, September). The extreme weather events of 2023. The Week. https://theweek.com/in-depth/1021278/2023-extreme-weather

For more information on Certified CISO traning program please email enquiry@wissen-intl.com

back to top

Article from IoT Partner, Nanyang Technological University

Career Progression through B.Tech in Computing, a Part-Time Work-Study Degree Programme at NTU

It is Monday morning in the month of December, and Jack is with his favourite morning kopi-c kosong at his desk pondering over his year-end performance review meeting in two hours from now.

Jack, graduated from a polytechnic 5 years ago, has worked as a software developer in this company since he finished his National Services. He is happy with the work, the management and the work environment; and colleagues are kind and helpful; but Jack is not satisfied. Since graduation from Polytechnic, Jack has always aspired to grow professionally in his career into more exciting areas such as software engineering, artificial intelligence, and cybersecurity. However, due to family time commitment and other financial responsibilities etc, Jack is unable to pursue a formal degree training like many of his other peers in the Polytechnic. Jack therefore believes that an opportunity to pursue a formal degree in his areas of interest while enabling him to balance between his various commitments would help him in a tremendous way in his career development.

Very recently, NTU has launched a SkillsFuture Work-Study Degree Bachelor of Technology in Computing (BTech in Computing) to meet the aspirations of people like Jack. NTU's BTech in Computing is a 4-year part-time work-study degree programme that is developed for mid-career professionals who would like to pursue skills upgrade or conversion into the Information Digital Technology (IDT) sector. Unlike a traditional degree programme, BTech in Computing is a stackable degree programme where learners would be awarded professional recognition for skills acquired in the form of professional certificates, before a formal degree is awarded. The professional certificate is recognized in first two stacks, Full-Stack Developer Stack followed by a Specialization Stack, in either area of Artificial Intelligence Engineering, Cybersecurity, or Software Engineering.

back to top

NTU also knows of Jack's dilemma in balancing between study, work, and family time; hence the BTech in Computing programme has built-in flexibility to provide online learning blended with tutorial, discussion workshops and other laboratory training. In order to help Jack apply all his learning into practical use, there are capstone projects designed as a part of the programme.

By the time Jack has acquired his first two professional certificates, the final year is an On-the-Job (OJT) year where Jack will be placed into an OJT job role according to his programme specialization where he will put all his knowledge and training into a work environment. This OJT practice period together with an industry-sponsored capstone project would help to cement Jack's professional competencies in his area of expertise. You may find NTU's BTech in Computing programme structure as shown in Figure 1.

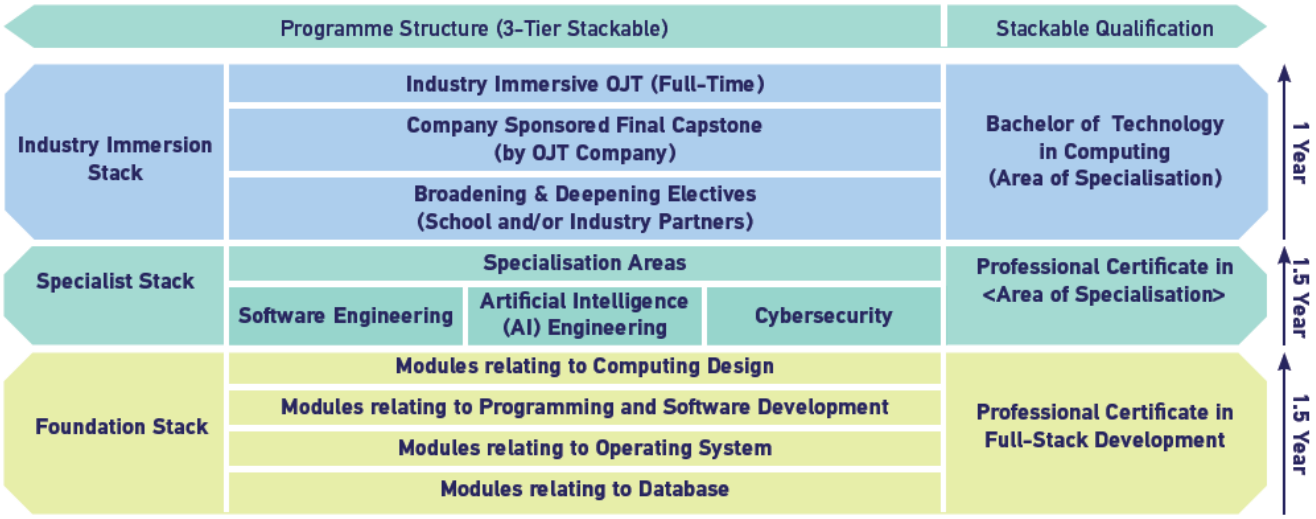


Figure 1 – NTU's Part-Time Work-study Degree Programme, Bachelor of Technology in Computing

For interest and further information about the programme, please visit our website at: https://www.ntu.edu.sg/scse/admissions/programmes/undergraduate-programmes/detail/bachelor-of-technology-in-computing-skillsfuture-work-study-degree

back to top

Article from IoT Partner, Nanyang Technological University

GLOBAL ALLIANCE OF INDUSTRIES @ NTU (GAIN)

Nanyang Technological University, Singapore (NTU Singapore)

About Us

The Global Alliance of Industries @ NTU (GAIN) catalyses industry-university partnerships for strategic collaborations and knowledge sharing. Serving as a gateway for industries, GAIN fosters cross-collaboration and co-creates innovative solutions with NTU Singapore's robust network of research advances, world-renowned talents, and state-of-the-art facilities.

One-Stop Solution for Industry: Driving Innovation through Partnership

GAIN acts as a matchmaker for industry partners who are seeking research partnerships with the relevant NTU entities to expedite the information-sharing process and provide guidance on all research aspects. NTU has a robust industrial collaboration ecosystem, collaborating with industry partners across various partnership models, including:

- Corporate Laboratories
- Joint Centres
- Research Institutes
- Consortia
- Technology Demonstrators & Living Labs
- Research Projects

back to top

Interdisciplinary & Translational Research

NTU is dedicated to advancing translational research that closely aligns with industry needs and demonstrates a strong commitment to driving research initiatives with an industry focus. To support its research and innovation initiatives, NTU has established an extensive network. The NTU Network encompasses 20 corporate/joint labs in collaboration with industry partners and 36 university-level research institutes. This network serves as a vital bridge, connecting over 250 industry partners with about 7,900 world-class faculty, researchers, and staff from 76 countries, all at the forefront of pioneering research and innovation.

The unwavering commitment to research has earned NTU international recognition across a wide range of fields. According to the *2022-2023 Best Global Universities Rankings by U.S. News & World Report*, NTU has achieved the *top position worldwide* in five subjects: *Condensed Matter Physics*, *Energy and Fuels*, *Materials Science*, *Nanoscience and Nanotechnology*, and *Physical Chemistry*. Additionally, it holds the *second global position* in *Artificial Intelligence*, *Electrical and Electronic Engineering*, and *Engineering*.

This remarkable recognition is a testament to NTU's dedication to pushing the boundaries of knowledge and innovation. NTU's Intellectual Properties are managed by NTUitive, NTU's Innovation and Enterprise (I&E) Company, which also plays a pivotal role in

back to top

facilitating the commercialisation of research. Over the past 3 years, NTUitive has reviewed over 1,500 new technology disclosures, secured 300 licenses, and created over 180 new startups & spinoffs. These impressive achievements underscore NTU's commitment to translating cutting-edge research into real-world impacts and fostering economic growth.

Vibrant NTU-Industry Ecosystem
As a leading university, NTU's vibrant research culture has resulted in global recognition across various fields. With extensive research capabilities, NTU attracts international industry partners, catalysing innovation through collaborative efforts and establishing itself as a pioneer in the university-industry ecosystem.

Furthermore, in line with Singapore's mission to become a global research and innovation hub for Digital Trust and Cybersecurity, NTU is at the forefront of this transformation. The University offers selected industry-leading initiatives that enable the exploration of cutting-edge developments in digital security and governance:

- CyberSG R&D Programme Office (click here for Media Release)
- Digital Trust Centre (DTC)
- National Integrated Centre for Evaluation (NiCE)
- Strategic Centre for Research in Privacy-Preserving Technologies & Systems (SCRiPTS)
- Centre for Smart Platform Infrastructure Research on Integrative Technology (SPIRIT)
- Mastercard-NTU Joint Lab (click here for Media Release)

If you're interested in exploring various opportunities for partnering with NTU, please reach out to us at GAIN-Events@ntu.edu.sg for further discussions.

Connect with Global Alliance of Industries @ NTU (GAIN)
- For more information, please visit our website at https://www.ntu.edu.sg/gain.
- Follow us on LinkedIn and stay tuned to the latest events and happenings.

Latest Publications of NTU
NTU Annual Report 2023 | NTU AT A GLANCE 2023 | Pushing Frontiers 2023

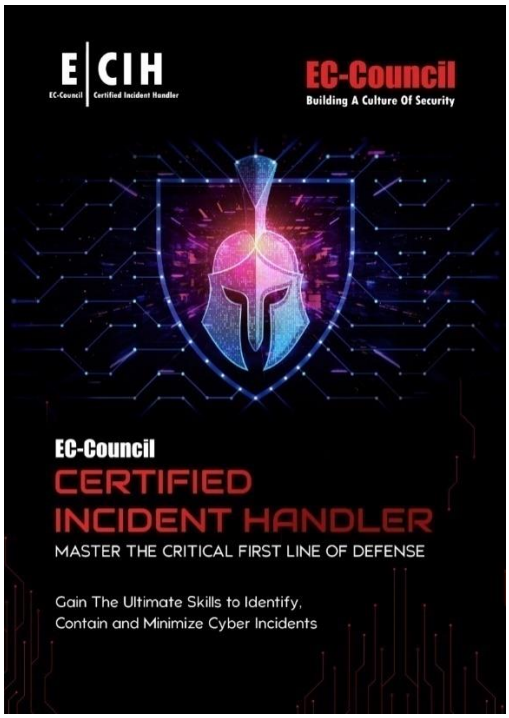
Visit https://www.aisp.sg/publications for more contributed contents by our partners.

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



The question is not if, but when a cyber incident will occur?

EC-Council's Certified Incident Handler (ECIH) program equips students with the knowledge, skills, and abilities to effectively prepare for, deal with, and eradicate threats and threat actors in an incident.

The newly launched Version 3 of this program provides the entire **process of Incident Handling and Response** and hands-on labs that teach the **tactical procedures and techniques** required to effectively **Plan**, **Record**, **Triage**, **Notify** and **Contain**.

ECIH also covers **post incident activities** such as **Containment, Eradication, Evidence Gathering** and **Forensic Analysis**, leading to prosecution or countermeasures to ensure the incident is not repeated.

With over **95 labs**, **800 tools** covered, and exposure to Incident Handling activities on four different operating systems, ECIH provides a well-rounded, but tactical approach to planning for and dealing with cyber incidents.

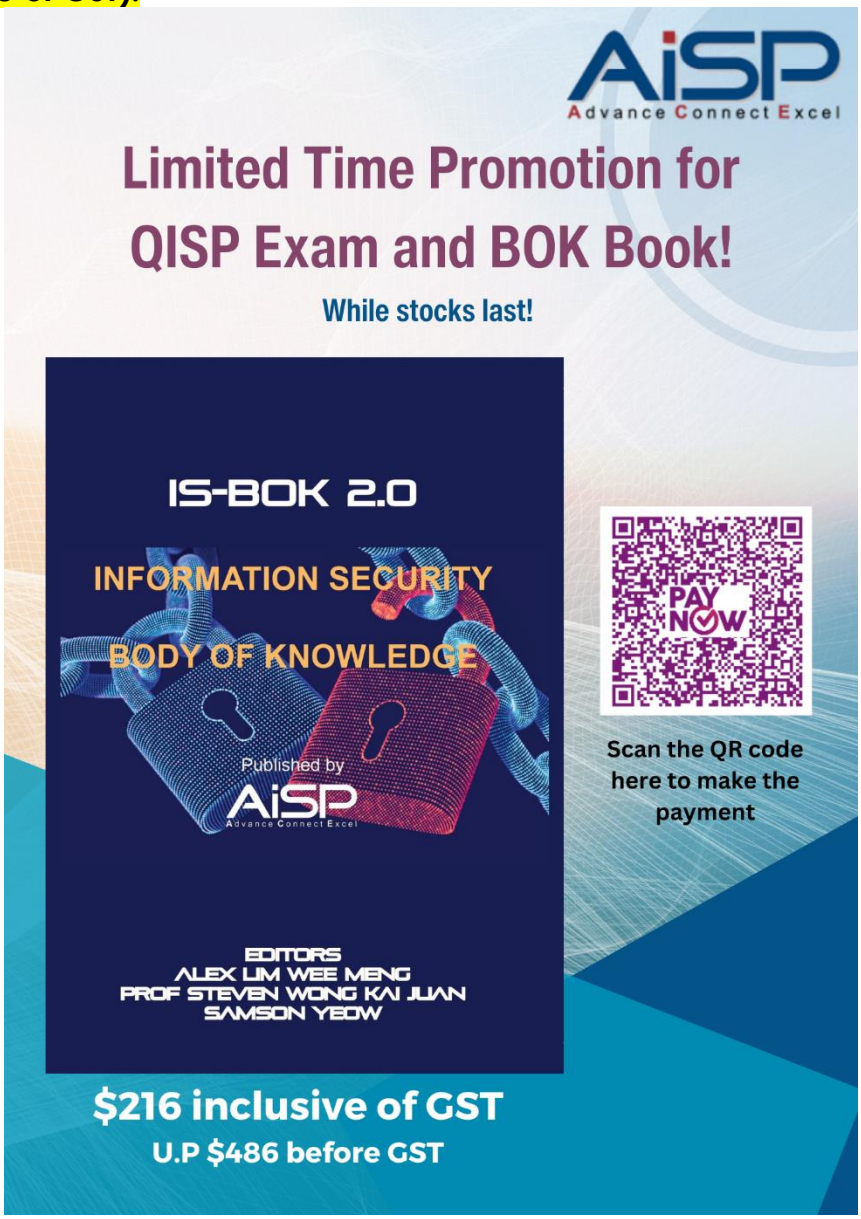
Special discount available for AiSP members, email aisp@wissen-intl.com for details!

back to top

Qualified Information Security Professional (QISP®)

BUNDLE PROMOTION VALID TILL 16 December 2023

For a limited time, get our Qualified Information Security Professional (QISP) Exam Voucher (U.P $370 before GST) along with the newly launched Information Security Body of Knowledge (BOK) Physical Book (U.P $80 before GST) at the limited promotional price of **$216 (inclusive of GST).**



back to top

Why This Bundle?

- QISP Exam Voucher: Propel your career with the QISP certification. Prove your skills and stand out in the competitive cybersecurity landscape.
- BOK Book: The Body of Knowledge (BOK) is your comprehensive guide to mastering the key concepts, principles, and practices in cybersecurity.

Please scan the QR Code in the poster to make the payment of **$216 (inclusive of GST)** and email secretariat@aisp.sg with your screenshot receipt and we will follow up with the collection details for the BOK book. Limited stocks available.

Promotion is valid until **16 December 2023.**
Please note that the QISP Exam must be taken by 16 December 2023.

Terms and conditions apply.

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

Online

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: 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

For any enquiries, please contact secretariat@aisp.sg

back to top

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 from now till 31 December to avoid the 9% GST increase 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!

NTUC U Associate Membership

Some benefits include

Career Advisory services - https://upme.ntuc.org.sg/upme/Pages/CareerCoaching.aspx

Benefits and privileges from RX Community

Member Programme

https://www.readyforexperience.sg/

Please fill in the form below and make payment if you would like to sign up for the membership.

https://forms.office.com/r/qtjMCK376N

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

back to top

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.

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.

back to top

