AiSP NEWSLETTER
February 2024

NEWS & UPDATE

New Partners

AiSP would like to welcome Athena Dynamics, Magnet Forensics and M.Tech 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 Ensign Infosecurity, Nanyang Polytechnic, RSM, Singapore University of Social Sciences, Trend Micro and Votiro for their continued support in developing the cybersecurity landscape:

News & Updates

On 29 January, AiSP Secretary Ms Soffenny Yap visited the Google Office to brief Minister Josephine Teo about the 600 Google Scholarships available for AiSP PME members. These scholarships offer opportunities for PMEs to enhance their cybersecurity knowledge. Soffenny also discussed AiSP's SVRP program and the QiSA/QiSP certifications that PMEs can pursue following the completion of Google certification courses with Minister Teo.

Knowledge Series Events

Upcoming Knowledge Series

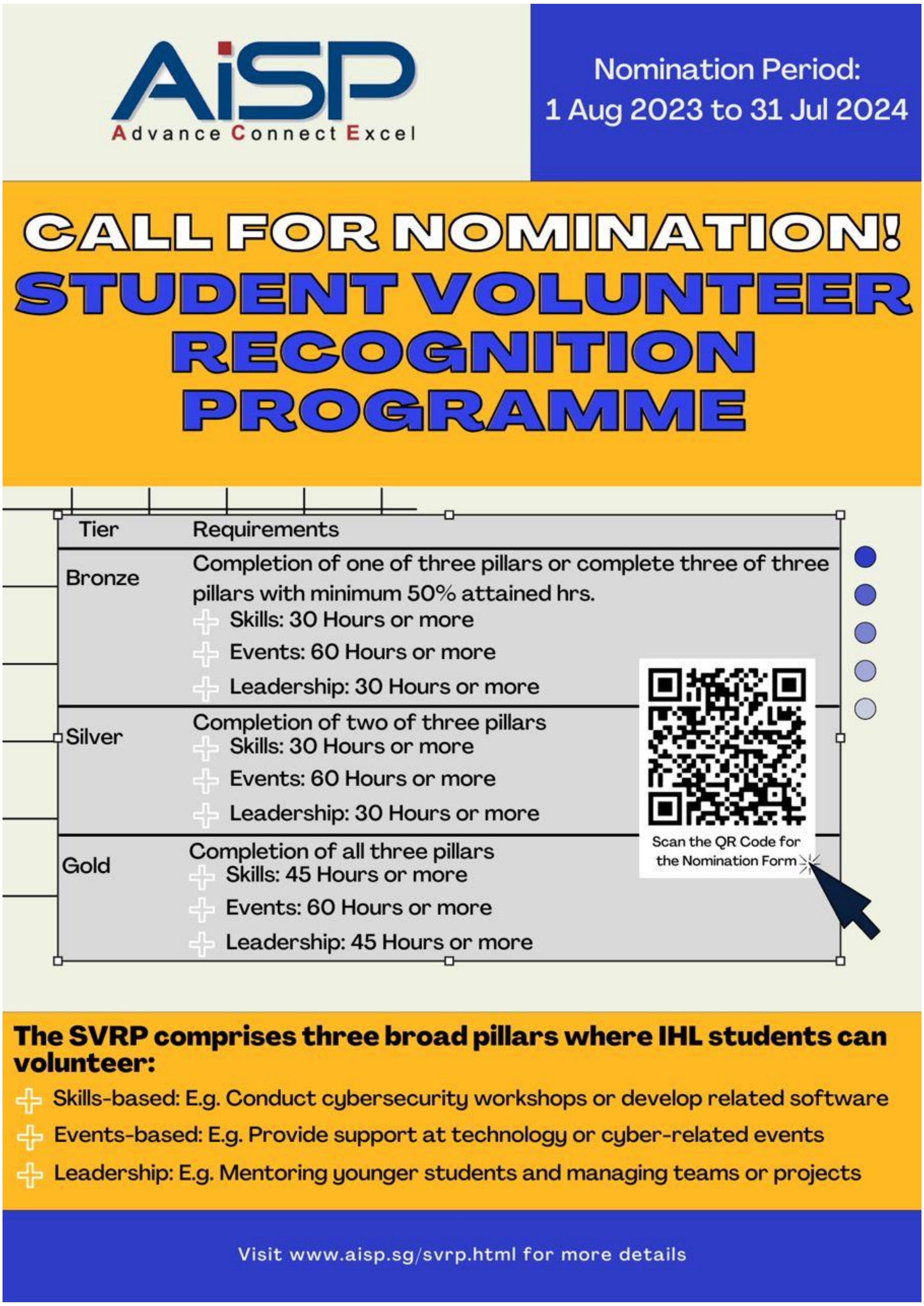
As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its **Information Security Body of Knowledge 2.0** topics. Our scheduled topics for webinars in 2024 are as follows (may be subjected to changes),

1. 25 Apr 2024, Red Team
2. 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)



AiSP
Advance Connect Excel

Nomination Period:
1 Aug 2023 to 31 Jul 2024

CALL FOR NOMINATION!

STUDENT VOLUNTEER RECOGNITION PROGRAMME

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

Scan the QR Code for the Nomination Form

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

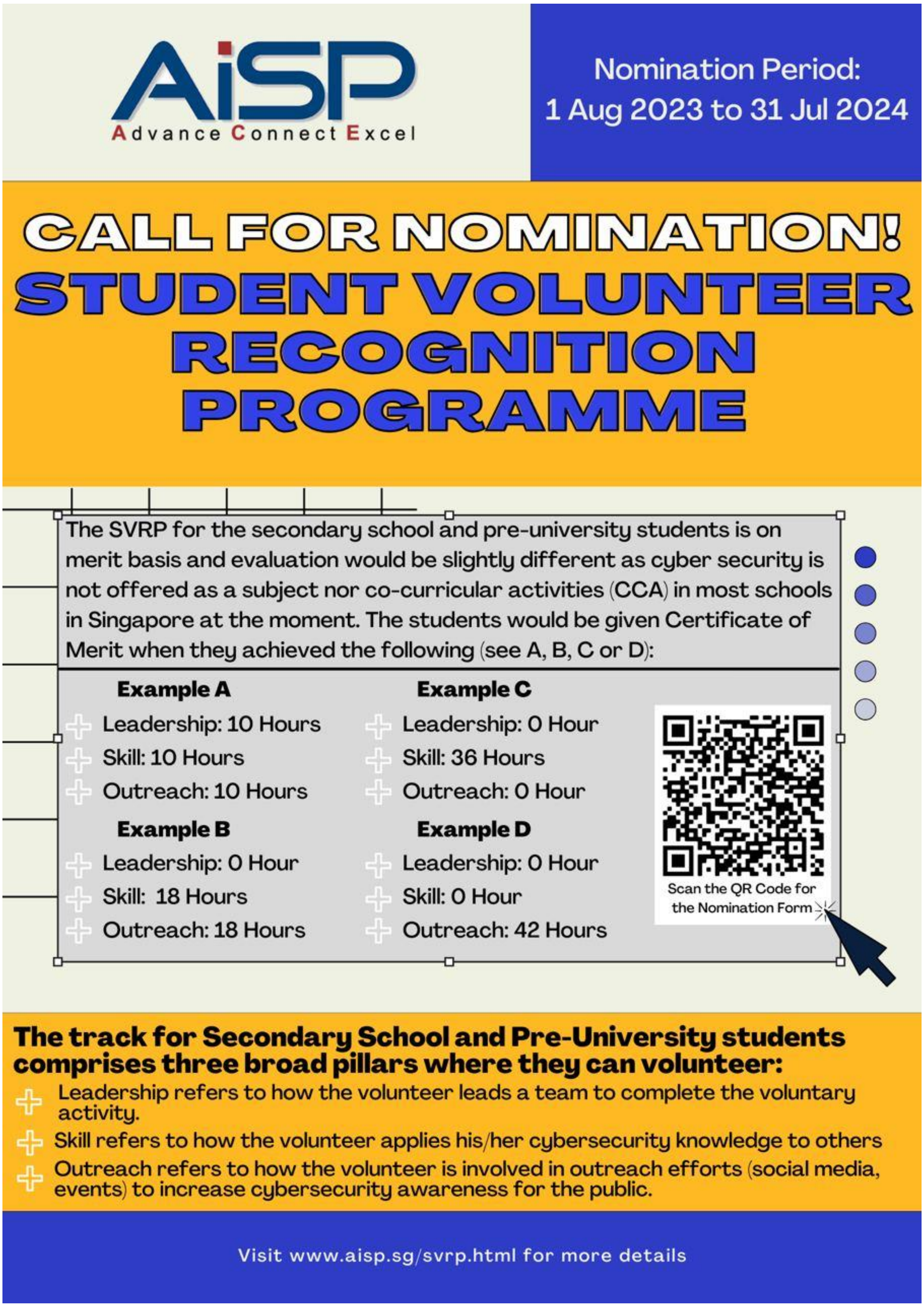
✚ Skills-based: E.g. Conduct cybersecurity workshops or develop related software

✚ Events-based: E.g. Provide support at technology or cyber-related events

✚ Leadership: E.g. Mentoring younger students and managing teams or projects

Visit www.aisp.sg/svrp.html for more details

back to top



Advance Connect Excel

Nomination Period:
1 Aug 2023 to 31 Jul 2024

CALL FOR NOMINATION!

STUDENT VOLUNTEER RECOGNITION PROGRAMME

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

Example A

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

Example B

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

Example C

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

Example D

- Leadership: 0 Hour
- Skill: 0 Hour
- Outreach: 42 Hours

Scan the QR Code for the Nomination Form

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

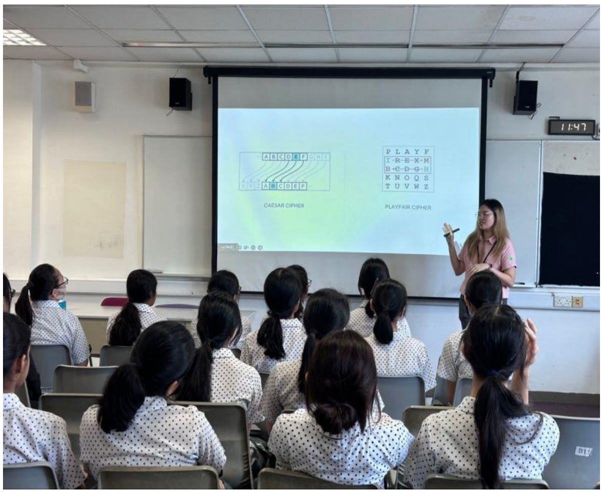
- Leadership refers to how the volunteer leads a team to complete the voluntary activity.
- Skill refers to how the volunteer applies his/her cybersecurity knowledge to others
- Outreach refers to how the volunteer is involved in outreach efforts (social media, events) to increase cybersecurity awareness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

Visit www.aisp.sg/svrp.html for more details

back to top

School talk at St Margaret's School (Secondary) on 2 January

AiSP started our new work year with school talk at St Margaret's School (Secondary) on 2 January. Our AiSP Member, Ms Thanh Van Christine Ngo from Grab shared her personal experience in Cyber with 40 Secondary 4 Female students on Personal Growth in The Cyber Security Field. Hope the students have gained insights from the sharing.



Learning Journey to Fortinet on 12 January

On 12 January, AiSP brought 18 students from the School of Science and Technology (SST) to attend an educational learning journey to our corporate partner, Fortinet's office. Mr Halley Shen, Ms Michelle Pareno and Mr Li Haoqi from Fortinet did an insightful sharing about their job scopes. Hope that students have gained new insights from the sharing.

back to top

School Talk at Bukit Panjang Government High School on 15 January

Our AiSP Member, Nicholas Chong from RSM - Singapore shared his personal experience in Cyber with 40 students in Bukit Panjang Government High School during the school career fair on 15 January. Hope that students have gained new insights from the sharing.

Learning Journey to RSM on 16 January and 18 January

AiSP brought a total of 51 students from Bukit Panjang Government High School (BPGHS) to attend an educational learning journey by our corporate partner, RSM – Singapore on 16 and 18 January. Hope the students gained new knowledge from the sharing.

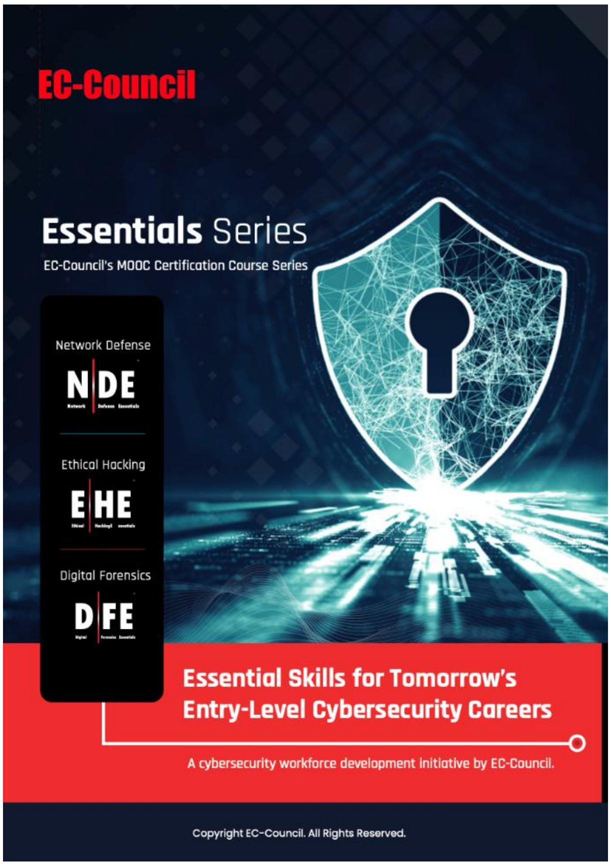
back to top

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.



EC-Council

Essentials Series

EC-Council's MOOC Certification Course Series

Network Defense
N|DE

Ethical Hacking
E|HE

Digital Forensics
D|FE

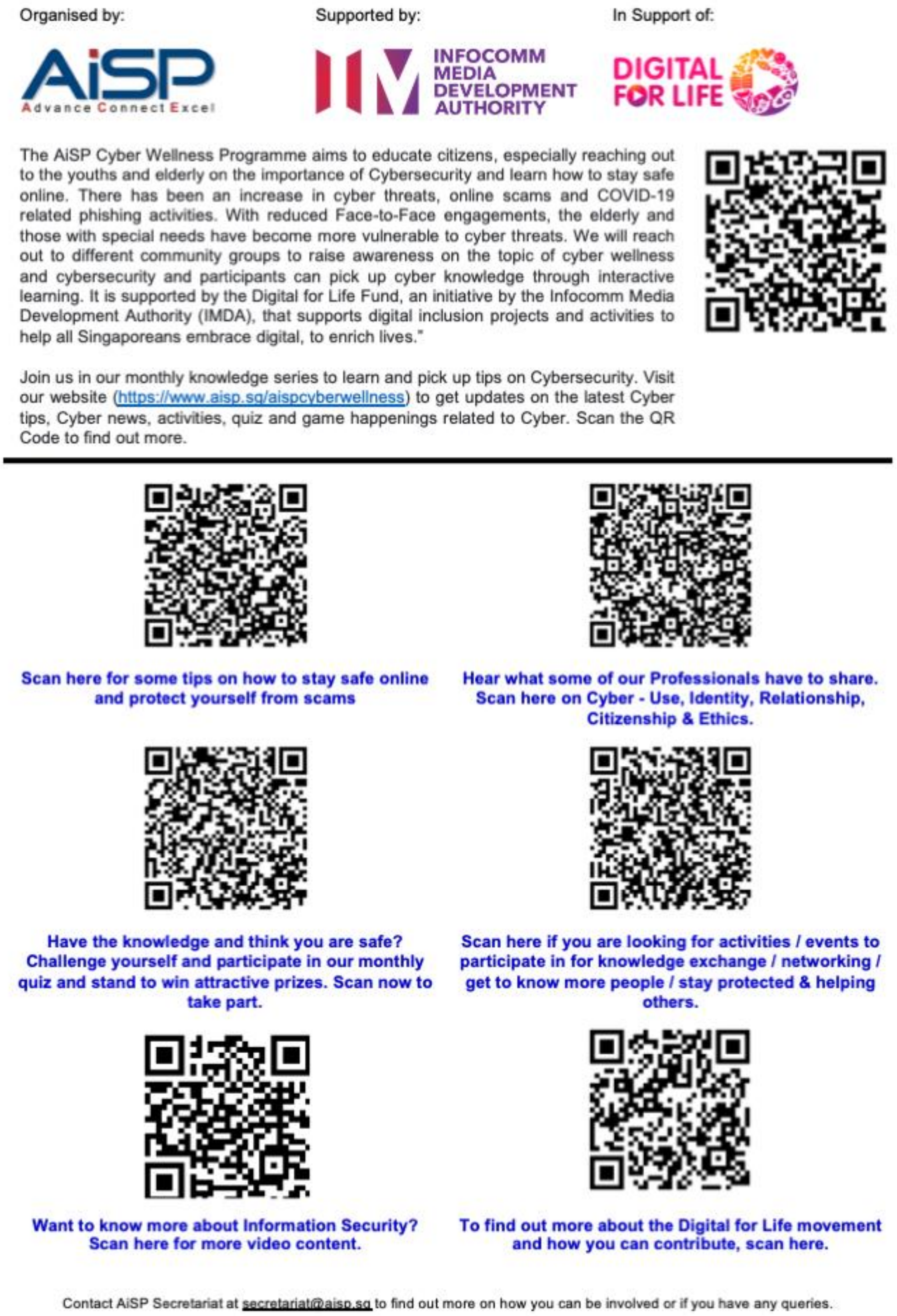
Essential Skills for Tomorrow's Entry-Level Cybersecurity Careers

A cybersecurity workforce development initiative by EC-Council.

Copyright EC-Council. All Rights Reserved.

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

Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP Cybersec Conference 2024 on 15 May

AiSP CyberSec Conference 2024

Sustaining Growth and Innovation Securely In This Challenging Business Environment

15 May 2024 9.30AM - 3PM

Suntec Convention Centre, Summit 1

SAVE THE DATE!

AiSP Advance Connect Excel

ORGANISED BY

AiSP

SILVER SPONSORS

BeyondTrust | KnowBe4 Human error. Conquered. | MAGNET FORENSICS | Veracity Trust Network

BRONZE SPONSOR

CYBERSAFE | softScheck | xcellink.pte.ltd.

SUPPORTING PARTNERS

AmCham | ASPRI | ASME | AUTOMATIONSG

Cybersecurity Association | British High Commission Singapore | CREST | CSA cloud security alliance

CSCIS | CzechTrade Singapore | HFCAS | IASA

ISACA Singapore Chapter | SINGAPORE | OT-ISAC | associate

SCS Singapore Computer Society | SFA | SGTECH | AHK

back to top

Organised by the Association of Information Security Professionals (AiSP), the AiSP SME Conference is a unique event that brings together organisations to discuss the importance of being cyber aware and stay protected. The event will provide our speakers with the opportunity to share their experience, skills and knowledge to show how cybersecurity can help companies to stay protected. AiSP aims to elevate cybersecurity awareness among companies and establish a self-sustaining ecosystem with active participation from government agencies, business associations, cybersecurity communities, and solutions provider.

Our theme for this year conference is "Sustaining growth and innovation securely in this challenging business environment".

As part of AiSP Cybersecurity Awareness and Advisory Programme (CAAP), this event is for Singapore Enterprise and SMEs to know more about cybersecurity as a business requirement and how they can implement solutions and measures for cyber-resilience. CAAP hopes to elevate cybersecurity awareness as integral part of business owner's fundamentals and establish a self-sustainable support ecosystem programme with active participation from agencies, business associations, security communities and solutions provider.

Date : 15 May 2024
Time : 9AM – 3PM
Venue : Suntec Convention Centre
Guest of Honour:
Morning: AiSP Patron – Senior Minister of State, Ministry of Communications and Information & Ministry of National Development - Mr Tan Kiat How
Afternoon: Member of Parliament for Pasir Ris-Punggol GRC & NTUC U SME Director – Ms Yeo Wan Ling

Register here

back to top

Special Interest Groups

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

- Cloud Security
- Data and Privacy
- CISO
- 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

back to top

AiSP CISO SIG Networking & Louhei on 20 February 2024

AiSP CISO SIG Networking & Louhei

AiSP
Advance Connect Excel
EC-COUNCIL
WISSEN
CISO SIG
NETWORKING & LOUHEI
Event Details:
20 Feb 2024
6pm - 8.30pm
Justco @ Marina Square
REGISTER NOW!

AiSP will be launching our new Special Interest Group (SIG) - CISO SIG. Our Key Focus Areas are:

- Network of Trust to enable more effective and responsive cyber defence of our respective organisations
- Thought leadership and open exchange of ideas to help enhance universal cyber maturity
- Support organization for professional challenges and trials faced by senior cybersecurity leaders
- Socialising because not everything has to be a crisis

Our Vision is to enable CISO's to collaborate, network and exchange thought leadership in the pursuit of a mature cyber defence for their respective organizations and the community at large.

AiSP will be having our first SIG Activity focusing on the theme "CISOs of Tomorrow: Forging the Future Cybersecurity Leadership" and we would like to invite you to do join us for the networking and louhei

In the ever-expanding digital landscape, the role of Chief Information Security Officers (CISOs) has become pivotal in safeguarding organizations from cyber threats. As we stand at the intersection of technology and security, it is imperative to focus on nurturing the next generation of CISOs who will shape the future of cybersecurity.

back to top

Join us for an immersive journey into the evolving dynamics of the CISO talent pool at our event, "CISOs of Tomorrow: Forging the Future Cybersecurity Leadership." This gathering serves as a unique platform to explore the latest trends, challenges, and opportunities in the realm of cybersecurity leadership.
Event Date: 20 Feb 2024
Event Time: 6.30pm - 8.30pm (Registration Starts at 6pm)
Event Venue: Justco @ Marina Square

Registration Link: https://forms.office.com/r/at8xG3igH9

The Cybersecurity Awards

THE CYBERSECURITY Awards 2024

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)

back to top

THE CYBERSECURITY Awards 2024

Organised by

Supported by

Supporting Associations

Platinum Sponsors

Gold Sponsors

AiSP Advance Connect Excel
CSA SINGAPORE
CSA cloud security alliance SINGAPORE CHAPTER
CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES
HTCIA
ISACA Singapore Chapter
ISC2 CHAPTER SINGAPORE
OT-ISAC
SCS Singapore Computer Society
SGTECH WHERE TECH MEETS
THE LAW SOCIETY OF SINGAPORE
CISCO
HUAWEI
ST Engineering
BeyondTrust
DBS
ENSIGN INFOSECURITY
SANS
SIT SINGAPORE INSTITUTE OF TECHNOLOGY
TREND MICRO
wizlynx group

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

Regionalisation

Countering Emerging Technology's Potential for Malicious Abuse in the MFA-FOSS for Good (FFG) "Smart Nations: Strategies, Opportunities and Cybersecurity Management" on 19 January

Our AiSP EXCO Member & Fellow, Mr Freddy Tan addressed on the Countering Emerging Technology's Potential for Malicious Abuse in the MFA-FOSS for Good (FFG) "Smart Nations: Strategies, Opportunities and Cybersecurity Management" programme at Park Royal on Beach Road on 19 January. He shared insights on countering the potential misuse of emerging technologies with 25 government officials from various regions, representing over 25 countries including Bolivia, Bhutan, Dominican Republic, Fiji, Jordan, Seychelles, Tonga, Trinidad, Tobago & Zambia. During the session, Freddy also highlighted how AiSP's Cyber Security Awareness and Advisory Programme (CAAP) could be a valuable resource for enhancing awareness and address questions on AI verify tool and number of cyber incidents in Singapore. Thank you Civil Service College for inviting AiSP and Freddy for the sharing.

AiSP
Countering Emerging Technology's Potential for Malicious Abuse
About AiSP
OUR VISION

back to top

Cybersec Asia 2024 x Thailand International Cyber Week 2024 on 31 January

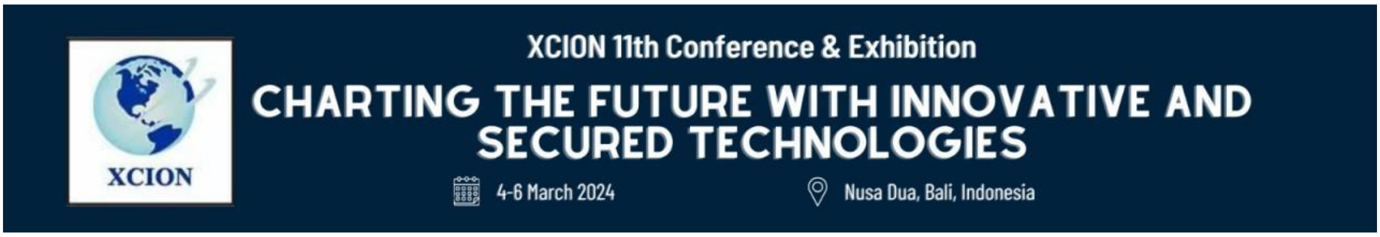
On 31 Jan 24, our AiSP EXCO Member & Fellow, Mr Freddy Tan represented AiSP to speak at the Cybersec Asia 2024 x Thailand International Cyber Week 2024, powered by NCSA in Thailand. During the session, Freddy highlighted how AiSP's Cyber Security Awareness and Advisory Programme (CAAP) could be a valuable resource for enhancing awareness and share about AiSP Body of Knowledge and AiSP QiSP Certification. Thank you Cybersec Asia for inviting AiSP to the event and thank you Freddy for flying the Singapore Flag high to share with our regional partners on the importance of Cybersecurity.

owledge (BOK)
CYBERSEC ASIA
X
THAILAND INTERNATIONAL CYBER WEEK 2024
Information Security Body of Knowledge (BOK)

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.
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.



XCION

XCION 11th Conference & Exhibition

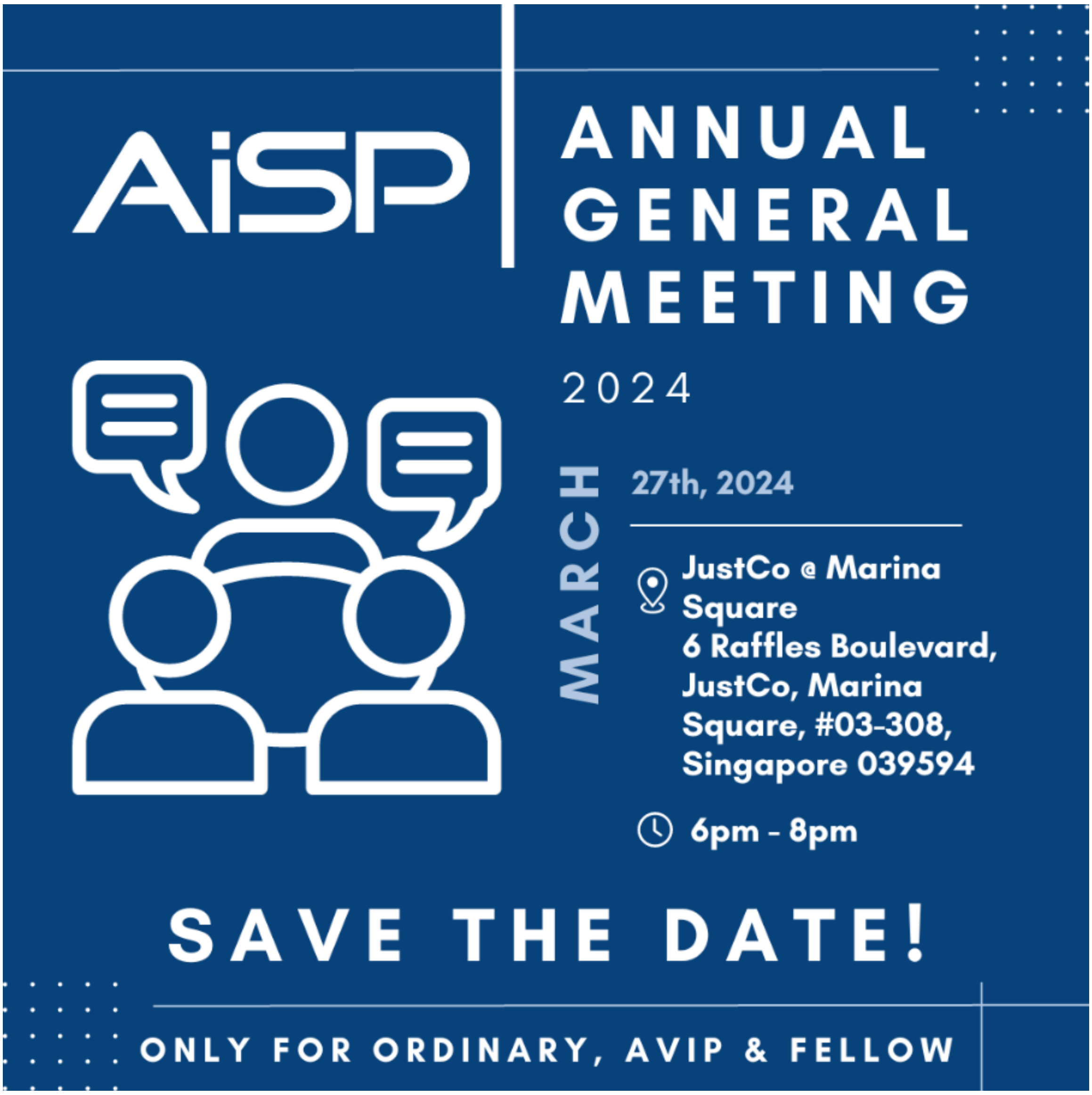
CHARTING THE FUTURE WITH INNOVATIVE AND SECURED TECHNOLOGIES

4-6 March 2024

Nusa Dua, Bali, Indonesia

back to top

Annual General Meeting



AiSP

ANNUAL GENERAL MEETING 2024

MARCH 27th, 2024

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

6pm - 8pm

SAVE THE DATE!

ONLY FOR ORDINARY, AVIP & FELLOW

back to top

Corporate Partner Event

A Proactive Approach to Protecting Public-facing Infrastructure on 18 January

AiSP collaborated with our Corporate Partner, OpenText to organise a coffee talk on A Proactive Approach to Protecting Public-Facing Infrastructure on 18 January. Thank you Niel Pandya, Jonathan Ho and Donald Ong for sharing insights with the attendees.

AiSP
opentext
GLOBAL ADVERSARY SIGNALS ANALYTICS FOR ADVANCED THREAT INTELLIGENCE
NIEL PANDYA
APJ BUSINESS DEVELOPMENT LEAD FOR CYBERSECURITY
OPENTEXT

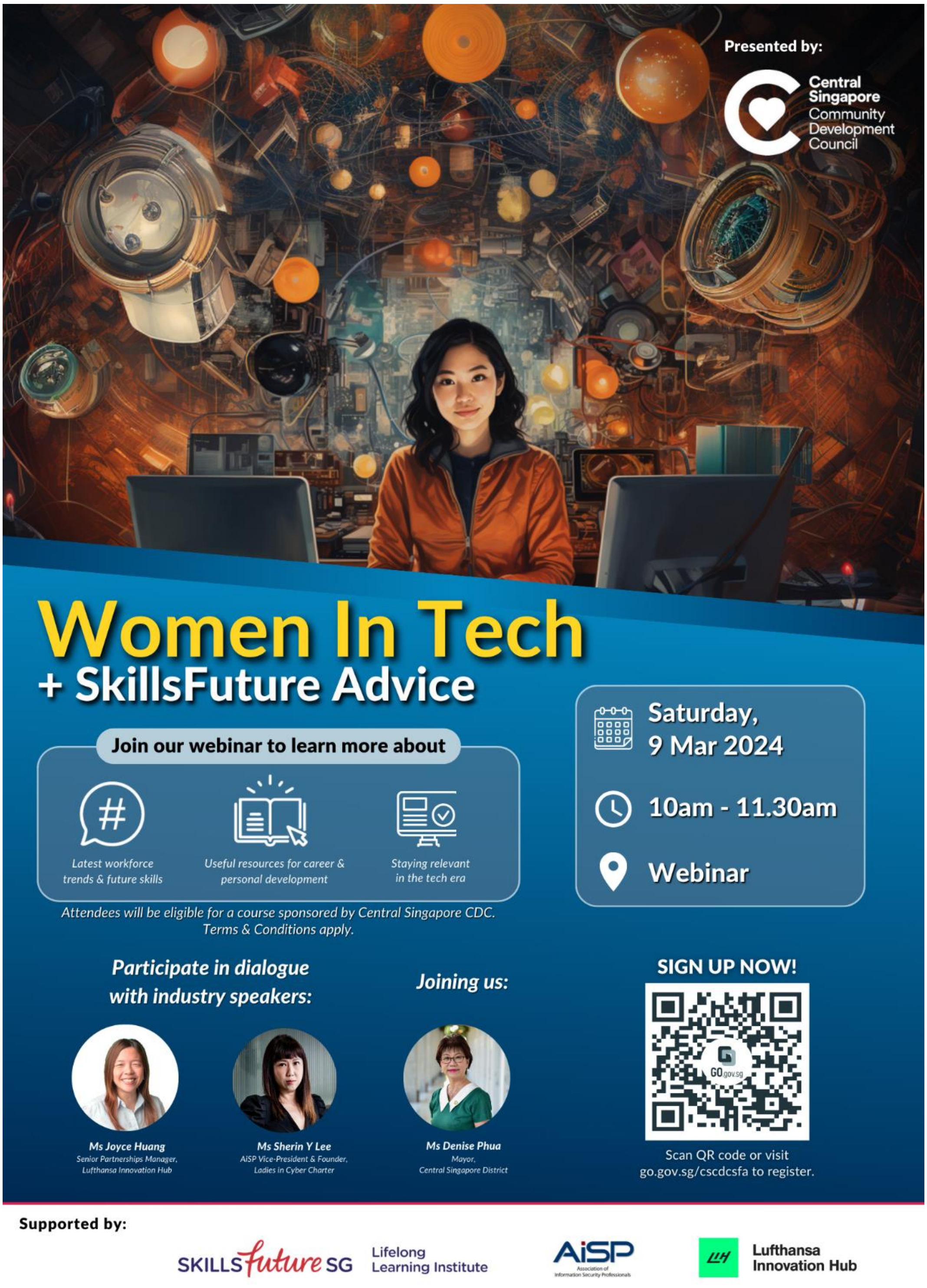
AiSP
opentext
GLOBAL ADVERSARY SIGNALS ANALYTICS FOR ADVANCED THREAT INTELLIGENCE
NIEL PANDYA
APJ BUSINESS DEVELOPMENT LEAD FOR CYBERSECURITY
OPENTEXT

Proliferation of clouds… and of cloud waste
State of cloud today: migrations to the cloud, increasing cloud consumption, and adoption of multiple providers
21.7
28%
15-25%
opentext

back to top

Ladies in Cyber

Women in Tech + SkillsFuture Advice on 9 March 2024



Presented by:

Central Singapore Community Development Council

Women In Tech
+ SkillsFuture Advice

Join our webinar to learn more about

- Latest workforce trends & future skills
- Useful resources for career & personal development
- Staying relevant in the tech era

Attendees will be eligible for a course sponsored by Central Singapore CDC. Terms & Conditions apply.

Saturday, 9 Mar 2024

10am - 11.30am

Webinar

Participate in dialogue with industry speakers:

Ms Joyce Huang
Senior Partnerships Manager, Lufthansa Innovation Hub

Ms Sherin Y Lee
AiSP Vice-President & Founder, Ladies in Cyber Charter

Joining us:

Ms Denise Phua
Mayor, Central Singapore District

SIGN UP NOW!

Scan QR code or visit go.gov.sg/cscdcsfa to register.

Supported by:

SKILLSfuture SG Lifelong Learning Institute

AiSP

Lufthansa Innovation Hub

Register here

back to top

Digital For Life

Nee Soon South Ang Pow Distribution on 21 January

Our student volunteers from our Academic Partner, Republic Polytechnic was at Nee Soon South Ang Pow Distribution Event on 21 January, where they shared about cyber hygiene awareness with over 800 seniors.

back to top

NTUC UPME x AiSP x TTAB Networking Event

On 31 January, participants had an enlightening and engaging event that delved into the realms of mentorship and relevant training programs organized by NTUC UPME and TTAB. Thank you Mr Bernard Menon, UPME Director sharing on the Mentorship Community initiative and AiSP EXCO Member and Managing Director of Wissen International, Mr Breyvan Tan for sharing on the relevant training programs to help equip tech professionals with the right skills. Big shoutout to Wissen International for supporting the event!

back to top

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
7 Feb	Safe App Standard	Partner
20-21 Feb	Seamless Asia 2024	Partner
20 Feb	CISO SIG Activity	AiSP
27 Feb – 6 Mar	Magnet Virtual Summit 2024	Partner
4 – 6 Mar	XCION	Partner
8 Mar	AiSP International Women Day Celebrations	AiSP
9 Mar	Women In Tech + Skillsfuture Advice	Partner
11-13 Mar	Lag and Crash	Partner
14 Mar	Agile Cyber Security BFSI Summit	Partner
17 Mar	DFL Event at Chong Pang	Partner
26 Mar	AiSP x Illumio CPP event	AiSP & Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

Cloud Security – Part 2 – Kubernetes and Container Security
With thanks to friends at docker.com, Kubernetes.io, Wikipedia, Check Point, Sysdig
Anthony Lim for AISP, May 2023

Let's start with the text book ☺

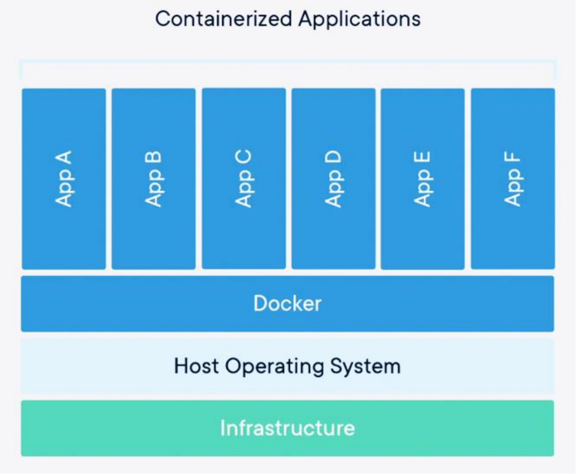
Container and Docker

A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.

A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.

A Docker is a software platform that allows you to build, test, and deploy applications quickly.

Docker packages software into standardized units called containers that have everything the software needs to run including libraries, system tools, code, and runtime.



Kubernetes

back to top

Kubernetes, also known as K8s, is an open-source system for automating deployment, scaling, and management of containerized applications.

It groups containers that make up an application into logical units for easy management and discovery.

- **Planet scale** - Designed on the same principles that allow Google to run billions of containers a week, Kubernetes can scale without increasing your operations team.

- **Never outgrow** - Whether testing locally or running a global enterprise, Kubernetes flexibility grows with you to deliver your applications consistently and easily no matter how complex your need is.

- **Run Anywhere** - Kubernetes is open source giving you the freedom to take advantage of on-premises, hybrid, or public cloud infrastructure, letting you effortlessly move workloads to where it matters to you.

Kubernetes has become the de facto operating system of the cloud. This rapid success is understandable, as Kubernetes makes it easy for developers to package their applications into
portable microservices.

However, Kubernetes can be challenging to operate. Teams often put
off addressing security processes until they are ready to deploy code into production. Kubernetes requires a new approach to security.

After all, legacy tools and processes fall short of meeting cloud-native requirements by failing to provide visibility into dynamic container environments. Fifty-four percent of containers live for five minutes or less, which makes investigating anomalous behavior and breaches extremely challenging.

One of the key points of cloud-native security is addressing container security risks as soon as possible. Doing it later in the development life cycle slows down the pace of cloud
adoption, while raising security and compliance risks.

The Cloud/DevOps/DevSecOps teams are typically responsible for security and compliance
as critical cloud applications move to production. This adds to their already busy schedule to
keep the cloud infrastructure and application health in good shape.

Kubernetes Security Considerations

The first area to protect is your applications and libraries. Vulnerabilities in your base OS

back to top

images for your applications can be exploited to steal data, crash your servers or scale privileges. Another component you need to secure are third-party libraries. Often, attackers
won't bother to search for vulnerabilities in your code because it's easier to use known exploits in your applications libraries.

The next vector is the Kubernetes control plane - your cluster brain. Programs like the controller manager, etc or kubelet, can be accessed via the Kubernetes API. An attacker with access to the API could completely stop your server, deploy malicious containers or delete your entire cluster.

Additionally, your cluster runs on servers, so access to them needs to be protected. Undesired access to these servers, or the virtual machines where the nodes run, will enable
an attacker to have access to all of your resources and the ability to create serious security
exposures.

OWASP Top 10 Kubernetes Cybersecurity Issues (2022)

When adopting Kubernetes, we introduce new risks to our applications and infrastructure. The OWASP Kubernetes Top 10 is aimed at helping security practitioners, system administrators, and software developers prioritize risks around the Kubernetes ecosystem. The Top 10 is a prioritized list of these risks.

K01: Insecure Workload Configurations
K02: Supply Chain Vulnerabilities
K03: Overly Permissive RBAC Configurations
K04: Lack of Centralized Policy Enforcement
K05: Inadequate Logging and Monitoring
K06: Broken Authentication Mechanisms
K07: Missing Network Segmentation Controls
K08: Secrets Management Failures
K09: Misconfigured Cluster Components
K10: Outdated and Vulnerable Kubernetes Components

Prometheus

Prometheus is a free software application used for event monitoring and alerting. It records metrics in a time series database (allowing for high dimensionality) built using an HTTP pull model, with flexible queries and real-time alerting.

It is an open source project for monitoring cloud-native applications and Kubernetes. It is a graduated member of the Cloud Native Computing Foundation (CNCF) and has an active developer and user community.

back to top

A typical monitoring platform with Prometheus is composed of multiple tools:

- Multiple exporters typically run on the monitored host to export local metrics.
- Prometheus to centralize and store the metrics.
- Alertmanager to trigger alerts based on those metrics.
- Grafana to produce dashboards.
- PromQL is the query language used to create dashboards and alerts.

Prometheus is typically used to collect numeric metrics from services that run 24/7 and allow metric data to be accessed via HTTP endpoints. This can be done manually or with various client libraries. Prometheus exposes data using a simple format, with a new line for each metric, separated with line feed characters.

Non-secure deployments of Prometheus, JFrog warns, may pose an even larger security risk, via an optional management API that can be used to delete metrics and close the monitoring server.

One solution would be to secure the Prometheus server accesses using a reverse proxy, encrypting the communications between clients and a server. We can implement this security layer with an Apache or Nginx server configured as a reverse proxy that implements TLS encryption, authentication and other security features.

Security considerations of cloud containers

It's no secret that containerization has been one of the hottest tech trends of the last decade, and today containers are almost ubiquitous. In fact, Gartner projects that this year 75% of global enterprises will run containers in production.

With the rise in container popularity, there have been plenty of benefits. Containers are the cornerstone of microservices architectures that have enabled cloud native apps of all sizes. However, because of their popularity, containers are also a prime target for ransomware, hackers, and other threats.

As a result, enterprises that value a strong security posture must be able to address common container security issues. While there's no single silver bullet for addressing container security challenges, taking a holistic approach and leveraging the right tools can go a long way.

Cloud Container Security - Objectives:

- Leveraging the ShiftLeft tool to create automatically secure containers.
- Using agentless security tooling to protect all enterprise cloud assets.
- Gain posture management and deep visibility across all containers, even in multi-cloud environments.
- Enforce the principle of least privilege and help stay compliant.
- Detect configuration issues like exposed credentials.

back to top

- Scan container images for vulnerabilities, malware, and weak configurations.
- Automatically deploy granular security controls.
- Reduce risk with image scanning integrated into CI/CD pipelines and runtime.
- Secure runtime with out-of-the-box managed policies based on Falco and ML.
- Know what happened and why with an audit trail.

7 Cloud Container Security Issues and Challenges

To address container security challenges, enterprises need to understand the security risks impacting container workloads. The following 7 container security issues demonstrate the wide range of strategic and tactical challenges related to container-based infrastructure.

1. Effectively shifting left

DevSecOps and the concept of shift left security emphasize the importance of integrating security throughout the software development lifecycle (SDLC) and eliminating friction in the process of developing secure software.

While DevSecOps tools and automation garner a lot of the "shift left" headlines, a big part of effectively shifting left is cultural. Different organizational units within enterprises must move away from the idea of "security as the team of no" and embrace cooperation. The organizations that are able to truly adopt a DevSecOps mindset and make security "everyone's" responsibility are better positioned to improve security posture across an enterprise.

2. Managing ephemeral containers

Ephemeral containers are useful administrative and debugging tools in Kubernetes (K8s) clusters. For example, they can enable troubleshooting in environments that use distroless images. However, this also means ephemeral containers create an additional attack surface that wouldn't otherwise exist. As a result, managing ephemeral containers is an essential aspect of K8s security.

While ephemeral containers can be powerful tools for capturing debug information, enterprises should implement security policies restricting their use to only necessary workloads and environments.

3. Addressing misconfigurations

According to a leading cybersecurity vendor's recent cloud security survey, 27% of respondents reported a public cloud security incident. Of those incidents, 23% resulted from misconfigurations. That's just one of many examples of the security risk posed by misconfigurations.

back to top

To ensure robust container security and workload protection, enterprises must be able to continuously detect — and correct — misconfigurations in container cluster configurations. That means ensuring only secure configurations are used in production, and no sensitive information or secrets are exposed.

4: Countering known vulnerabilities

Zero-day threats are a real risk facing enterprises today, but many breaches exploit known vulnerabilities. By scanning container images, dependencies, and workloads, enterprises can detect and implement a plan to address known vulnerabilities before they're used in an exploit.

Integrating security tooling throughout the SDLC and CI\CD pipelines can go a long way in addressing this container security challenge. Enterprises that shift security left can often detect threats before they make it to production or mitigate them sooner than they otherwise could. For example, leveraging virtual patching to temporarily mitigate vulnerabilities until new containers are deployed.

5. Protecting against runtime threats

While signature-based detection works well to identify known exploits, many cloud workload security threats, such as zero-day exploits, require context to detect and mitigate. To provide enterprise-grade security for web applications and APIs, organizations need tooling that uses intelligence and context to detect new threats and limit false positives that hamstring productivity. Additionally, many cloud native applications can't accommodate traditional endpoint security agents and instead require an agentless approach to runtime security.

6. Addressing human error

Human error is a common factor in many security incidents today. Manual processes leave room for typos, misconfigurations, and oversight that can lead to a breach. While IPS, IDS, and firewalling can help reduce risk after these misconfigurations occur, they don't go far enough.

Enterprises should limit manual configuration and automate as much of their security configuration as practical. Additionally, they should implement scans that use policies to detect and help address misconfigurations before they're exploited.

7. Passing compliance audits

Compliance risk is one of the single biggest risks facing modern enterprises. Failing an audit related to standards like GDPR, HIPAA, or SOX can damage an enterprise's reputation and bottom line.

back to top

As a result, ensuring that container workloads and K8s clusters meet compliance requirements is a must. Cloud security posture management (CSPM) and Kubernetes security posture management (KSPM) tools can help automate compliance across cloud and container infrastructure.

Author Bio

Anthony Lim
MAISP
Fellow, Cybersecurity, Governance & Fintech, Singapore University of Social Sciences

Anthony is a pioneer of cyber-security and governance in Singapore and the Asia Pacific region, with over 25 years' professional experience, as a business leader, consultant, advocate, instructor and auditor.

He has managed some national-level cybersecurity readiness assessment projects in Singapore and the region and was a co-author of an acclaimed international cloud security professional certification. He has held inaugural senior regional business executive appointments at Check Point, IBM and CA (now Broadcom), and was also client CISO at Fortinet and NCS. He has been active in industry association circles for nearly 2 decades, and is currently Advocate at (ISC)2 Singapore Chapter.

Anthony is an adjunct instructor and module developer for some tertiary academic & professional institutions. He has presented and provided content at many government, business, industry and academic seminars, committees, executive roundtables, workshops, trainings and media (print, broadcast, internet, including CNA, CNBC, Bloomberg, BBC) in Singapore, the region, and also for NATO, at Washington DC, Stanford University, ITU, Guangzhou Knowledge CIty and TsingHua University. He is a life alumni member of the University of Illinois, Urbana-Champaign.

back to top

Article from CISO SIG

“Some are born great, some achieve greatness, and some have greatness thrust upon them.”
- Act II Scene 5, Twelfth Night.
“It's lonely at the top, so you better know why you are there.”
- John C. Maxwell

I remember being simultaneously over the moon and a bundle of nerves when I received the offer for the role of APAC CISO at Schneider Electric. “Career is soon over!” teased a few industry colleagues. “This will test your mettle,” said others. But nothing, not even the best cyber education on the planet that I had just completed nor 30 years of pre-existing experience, could have prepared me for the absolutely most challenging and best role I’ve ever held. It’s a never-easy, generally thankless, demanding role that, in the end, will show you what you’re made of.

But the journey ought to be easier.

This CISO Special Interest Group (SIG) aims to create a network of peers to explore ways and means of supporting today’s CISOs as we lead our respective cybersecurity programs. The SIG will facilitate an environment of trust to enable knowledge exchange and more open discussions, create channels to communicate with one another (in peacetime or when we’re under attack), socialize with one another in good times and provide a shoulder to cry on when things go sideways.

There is true value in enabling a successful community comprised of all the CISOs in Singapore. Working together in pursuit of excellence enables economies of scale never seen before in this country. A thriving CISO community enables boundless opportunities to improve our jobs, careers, and lives.

But it's entirely up to us to make this work.

I call on you, the top level, primary decision makers or n-1’s of your organization's cybersecurity programs, to come together to support this initiative through a show of support at our first CISO SIG event on 20th February, 6PM – 8.30PM at JustCo@Marina Square. AiSP has generously opened the event to everyone to help socialize awareness of the formation of the CISO SIG. We’ll also be including a few interesting talks from our fellow CISOs and CISOs-to-be on succession planning.
To register for our event please click here to register.

back to top

Author Bio

Andre Shori
VP Outreach and Partnerships
AiSP

Andre Shori is the Regional CISO for Schneider Electric, covering both IT and OT Cybersecurity throughout the APAC region. Andre holds a Master of Science in Information Security Management from SANS and is the first person in Singapore and 19th globally to complete the program.

Andre hails from Canada and has over 20 year's international experience in Information Technology. He holds a variety of certifications in the Cyber Security arena and has been a full member of AiSP since 2009. He is also a current World Record holder in the Guinness Book of World Records.

back to top

Article from IMDA

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

THE (UPSIZED) BETTER DATA-DRIVEN BUSINESS PROGRAMME

Want to get started on data analytics, but do not know how to?

Transform raw data into actionable insights that drive greater results for your business with the free, user-friendly Business Intelligence (BI) tool!

4 NEW BUSINESS OBJECTIVES
specifically designed for Business-to-Business (B2B) SMEs

Download the BI tool to easily convert your business data into visual dashboards to help address common business objectives such as:

NEW! BOOST PRODUCT SALES & GROW DEMAND THROUGH DISTRIBUTORS

Identify and retain your high-value distributors to increase revenue

NEW! KNOW YOUR CLIENTS/DISTRIBUTORS

Identify your biggest client/distributor segments to improve sales performance

NEW! INNOVATE & DIVERSIFY PRODUCTS

Understand market trends and purchasing patterns to uncover business opportunities

NEW! MINIMISE COSTS & PRICE COMPETITIVELY

Monitor and analyse project and product costs to maximise profits

IMPROVE HR PLANNING

Analyse and strengthen your workforce to improve productivity

The BI tool is designed with built-in data protection components, and only collects necessary data that are generally pseudonymised.

DID YOU KNOW?

IMDA and Microsoft Singapore are offering free training to equip SMEs with foundational data use and protection skills.

Gain the skills needed to navigate the evolving data landscape and propel your business forward.

Register your interest at **go.gov.sg/smeworkshops** to stay updated on upcoming sessions!

Download the FREE BI tool for B2B SMEs at go.gov.sg/imdab2bbitool

FIND OUT MORE ABOUT THE BDDB PROGRAMME AT WWW.IMDA.GOV.SG/BDDB

IN SUPPORT OF
SG:DIGITAL

The BDDB is a free programme designed to help SMEs use data to gain valuable consumer insights and to grow their business through data analytics. Previously, our BDDB programme catered only to SMEs in the B2C arena, but we have taken in feedback from the ground and upgraded the BDDB programme to cater to B2B SMEs – any SMEs, regardless of their nature of business, can now take their first step in data analytics to enhance their business and gain that competitive advantage!

back to top

Article from SVRP 2023 Gold Winner, Ngui Jia Le Sherlena

SVRP 2023 Gold Winner – Ngui Jia Le Sherlena [NP]

How do you think SVRP has directly impacted your cybersecurity journey?
Participating in SVRP has impacted my cybersecurity journey as it has allowed me to gain exposure to various opportunities and, network with other like-minded individuals.

How has SVRP inspired you to contribute to the cybersecurity field?
SVRP has inspired others to contribute to the cybersecurity field as they feel motivated to have the opportunities offered to be able to network with security professionals and expand their knowledge within the field.

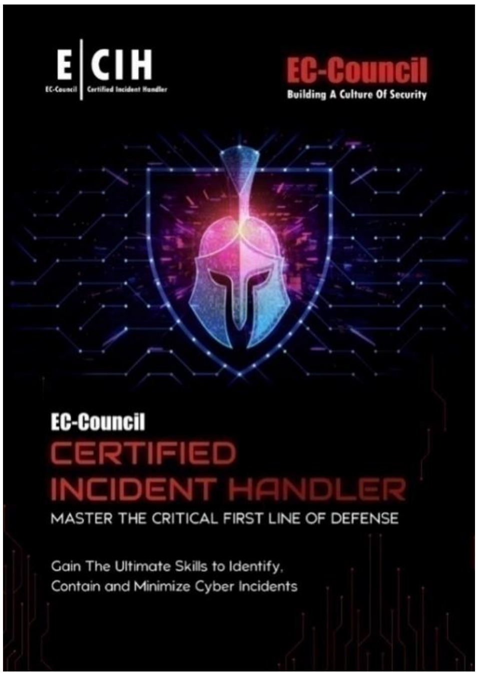
What motivates you to be a student volunteer?
What motivates me to be a student volunteer is to be able to meet like-minded individuals and to explore the field.

How would you want to encourage your peers to be interested in cybersecurity?
I would encourage my peers to be interested in cybersecurity by introducing them to various programs and CTFs that are beginner friendly. By introducing them to the programs and CTFs they can get an experience of the various portions of cybersecurity that may interest them.

back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International


E|CIH
EC-Council | Certified Incident Handler
EC-Council
Building A Culture Of Security
EC-Council
CERTIFIED
INCIDENT HANDLER
MASTER THE CRITICAL FIRST LINE OF DEFENSE
Gain The Ultimate Skills to Identify,
Contain and Minimize Cyber Incidents

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.

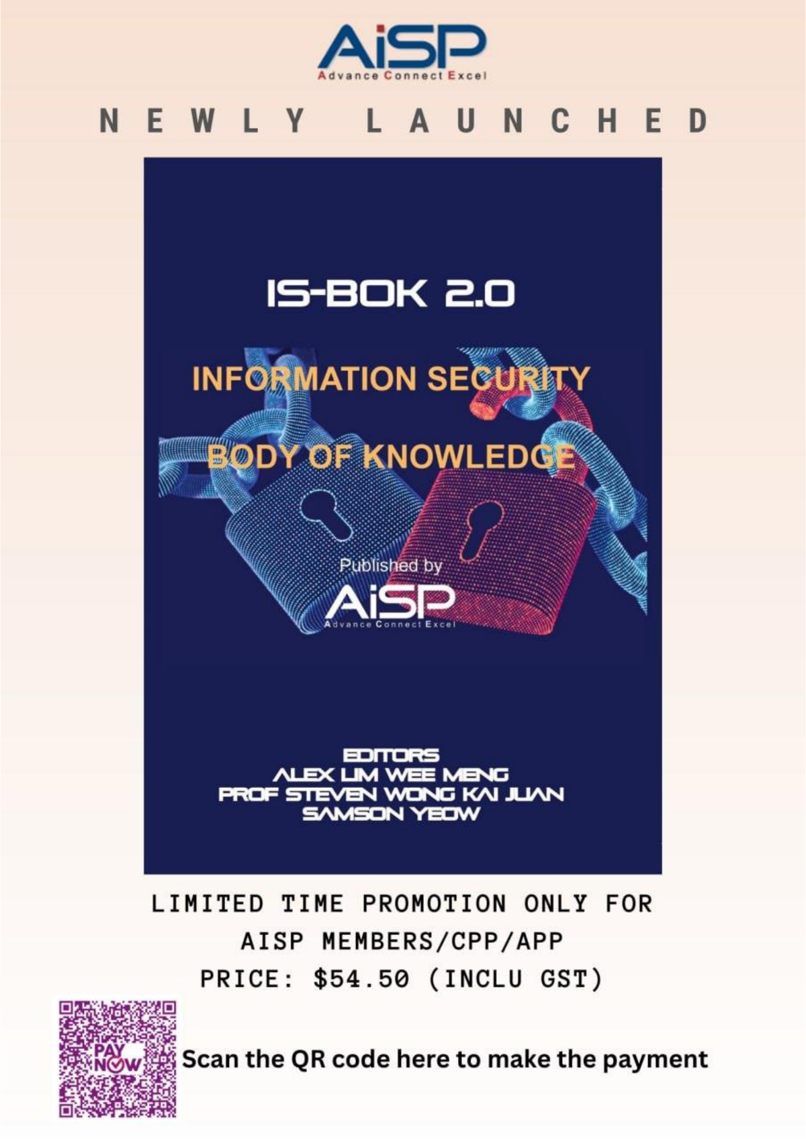
Special discount available for AiSP members, email aisp@wissen-intl.com for details!

back to top

Qualified Information Security Professional (QISP®)

Body of Knowledge Book Promotion!

For a limited time, get our newly launched Information Security Body of Knowledge (BOK) Physical Book (U.P $80 before GST) at the limited promotional price of **$54.50 (inclusive of GST). While stocks last!**



AiSP Advance Connect Excel

NEWLY LAUNCHED

IS-BOK 2.0

INFORMATION SECURITY BODY OF KNOWLEDGE

Published by AiSP Advance Connect Excel

EDITORS
ALEX LIM WEE MENG
PROF STEVEN WONG KAI JUAN
SAMSON YEOW

LIMITED TIME PROMOTION ONLY FOR AISP MEMBERS/CPP/APP
PRICE: $54.50 (INCLU GST)

Scan the QR code here to make the payment

Please scan the QR Code in the poster to make the payment of **$54.50 (inclusive of GST)** and email secretariat@aisp.sg with your screenshot payment and we will follow up with the collection details for the BOK book. Limited stocks available.

back to top

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

Online

QISP Exam Preparatory E-Learning Course

Governance and Management

Physical Security and Business Continuity

Security Architecture and Engineering

Operation and Infrastructure Security Software Security

Software Security

Cyber Defense

Prepare for QISP Exam via E-Learning Anytime, Anywhere!

Our e-learning program is perfect for those who want to prepare for the QISP Exam based on AiSP IS-BOK domains. With access for 12 months, you can study at your own pace on our beautifully designed and responsive e-learning platform.

Grab the exclusive launch offer at SGD 499 nett!

Special price of SGD 429 nett for AiSP members!

WISSEN Cyber Security Competency Development

enquiry@wissen-intl.com | www.wissen-intl.com

The QISP examination enables the professionals in Singapore to attest their knowledge in AiSP's Information Security Body of Knowledge domains. Candidates must achieve a minimum of 50-64% passing rate to attain the Qualified Information Security Associate (QISA) credential and 65% and above to achieve the Qualified Information Security Professional (QISP) credential.

Our highly responsive e-learning platform will allow you to learn anytime, anywhere with modular courses, interactive learning and quizzes. Complete the course in a month or up to 12 months! Enjoy lean-forward learning moments with our QISP/QISA preparatory e-learning course. Receive a certificate of completion upon completion of the e-learning course. Fees do not include QISP examination voucher. Register your interest here!

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 2024 to 31 Dec 2024. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. This does not include Plus! card holder (black-coloured card), please clarify with NTUC on your eligibility.

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

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

CPP Membership

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

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

For any enquiries, please contact secretariat@aisp.sg

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 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

WORK, LIVE, PLAY

LIKE NEVER BEFORE WITH THE NTUC-U ASSOCIATE MEMBERSHIP COLLABORATION!

READY TO ADD SPARK TO YOUR MEMBERS' LIVES AND LIVELIHOODS?

The NTUC-U Associate Membership Collaboration is an exclusive add-on membership for professional associations in the U Associate network. It will give your members access to exciting career, lifestyle and leisure benefits!

What are the benefits for your association?

- Additional privileges for your association members.
- Opportunities to engage your members at NTUC Club venues or participate in interest-based activities.
- Leverage U Associate's resources to reach out to a database of close to **300,000** professionals.

What are the benefits for your members?

- Career advancement and professional development through U PME Centre's suite of career advisory services.
- Enhanced lifestyle through interest-based leisure activities.
- Savings on lifestyle products and services through the Link Rewards Programme.

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

AiSP Corporate Partners

Acronis	athena dynamics	ASIA-PACIFIC
BD	BeyondTrust	BLACKPANDA
bugcrowd	cisco	CLIXER
C8N+FINITY	CROWDSTRIKE	CSA SINGAPORE
CSIT Centre for Strategic Infocomm Technologies	CYBERSAFE YOUR SECURITY, OUR PRIORITY	CYBER SECURITY HUB
CYFIRMA DECODING THREATS	CzechTrade SINGAPORE	DBS
DETACK	DSTA Defence Science & Technology Agency	DTASIA Security with Confidence
eclypsium	ENSIGN INFOSECURITY	Fidelis Services Redefined
FORTINET	GETVISIBILITY own your data	GOVTECH SINGAPORE
Grab	HORANGI CYBER SECURITY	HUAWEI

back to top

image engine

INTfinity

IT SEC ASIA

kaspersky

KnowBe4
Human error. Conquered.

MAGNET FORENSICS

mimecast

MySQL

M.TECH
Your Preferred i-Security Partner

ncs

NETWITNESS
An RSA Business

ONESECURE

opentext

OPSWAT.

PARASOFT

RAJAH & TANN
CYBERSECURITY

Responsible Cyber

Right-Hand
CYBERSECURITY

RSM

SailPoint

SCANTIST

Schneider Electric

Security Scorecard

SGS

Singtel

softScheck
We Build Trust

ST Engineering

TEMASEK

tenable

TREND MICRO

VECTRA

Veracity
Trust Network

VOTIRO

back to top

WISSEN
Cyber Security Competency Development

wizlynx group

xcellink.pte.ltd.
completing your technology chain

YesWeHack

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

ITE Institute of Technical Education

NYP NANYANG THE INNOVATIVE POLYTECHNIC

NGEE ANN POLYTECHNIC

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

NUS National University of Singapore

REPUBLIC POLYTECHNIC DISCOVER. TRANSFORM. ACHIEVE

SiT SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SMU SINGAPORE MANAGEMENT UNIVERSITY

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek POLYTECHNIC

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

AiSP Advance Connect Excel

🌐 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