AiSP NEWSLETTER

November 2023

NEWS & UPDATE

Continued Collaboration

AiSP would like to thank Image Engine, Tenable and Xcellink for their continued support in developing the cybersecurity landscape:

News & Updates

SICW GovWare 2023 on 17-19 October

AiSP had a booth together with the SEACC partners, Aptiknas, Brunei Cybersecurity Association (BCSA) and Women in Security Alliance Philippines (WISAP) at the SEACC pavilion from 17-19 October.

ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS (AISP)
AiSP
GovWare 2023
Conference and Exhibition
SEACC PAVILION

back to top

17 October

AiSP EXCO Member, Mr Freddy Tan moderated the roundtable session on Securing Critical Information Infrastructure in a Borderless World organised by our Corporate Member Beyond Trust at Day 1 of GovWare 2023. Freddy shared on the critical infrastructure in a borderless world, where information, goods, services, and people flow seamlessly across traditional perimeters. The session also brought together leaders from the critical infrastructure industries to exchange ideas, share best practices, and explore strategies for preventing and mitigating cyber-attacks on vital systems. The participants had a good time in discussions focused on fortifying the cyber posture of critical infrastructure operators and explore strategies in stopping attackers at the point of infiltration, preventing unauthorized access to critical systems, and mitigating the risk of lateral movement within the environment.

Thank you BeyondTrust for inviting AiSP for the session.

back to top

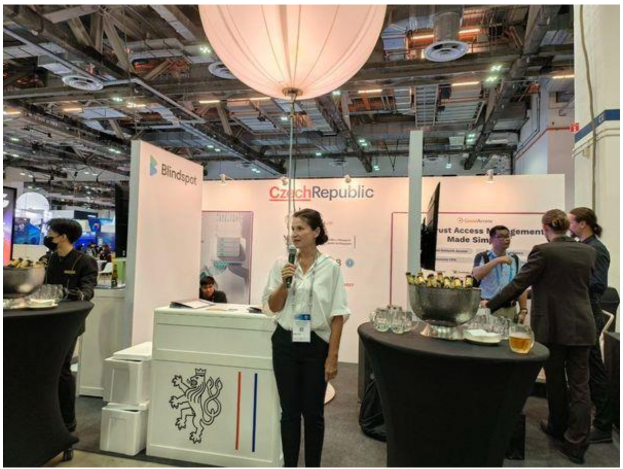
AiSP EXCO Member, Mr Freddy Tan participated in a dialogue session on cyber talent development organised by Huawei International on Day 1 afternoon at GovWare 2023. Freddy shared on what are the core challenges in terms of cyber security skills and talent development in our domain and in Singapore and the skill framework standards for cyber security talent cultivation in the Asia-Pacific. He also shared on some policies and industry best practices mitigate the above challenges and how vendors, industry associations, universities, academic institutions, and regulatory bodies strengthen collaboration and make greater contributions to cyber security talent cultivation and skill development.

Thank you Huawei International for inviting AiSP for the session.

back to top

On the first night, AiSP President, Mr Johnny Kho joined Deputy Minister of Foreign Affairs of the Czech Republic Mr. Jiří Kozák in the GovWare Czech Beer & Cyber at Czech Pavilion (B02) at GovWare 2023. Johnny delivered an opening speech and toasted along with Deputy Minister of Foreign Affairs of the Czech Republic Mr. Jiří Kozák, Ambassador of the Czech Republic to Singapore Mdm. Michaela Froňková and organizer of GovWare/ SICW to kick-off the networking session.

Thank you Czech Republic for having us at the networking session.



back to top

18 October

AiSP EXCO Member, Mr Freddy Tan moderated the session on Securing Healthcare Now and in the Future: Navigating the Shifting Threat Landscape at the GovWare Healthcare Forum at Day 2 of GovWare 2023. Healthcare is a leading target for cyberattacks and they are constantly rising. Amongst the bread-and-butter issues CISOs face from DDoS, data breaches, ransomware, phishing etc., vulnerabilities continue to be exploited through existing systems but are made more challenging as digitisation increases which clouds the attack surface landscape. Thank you GovWare for inviting AiSP for the session.

AiSP President, Mr Johnny Kho moderated the session on Cybersecurity as an Essential Enabler: Who, What, Where, When and How at Day 2 of GovWare 2023. Thank you GovWare for inviting AiSP for the session.

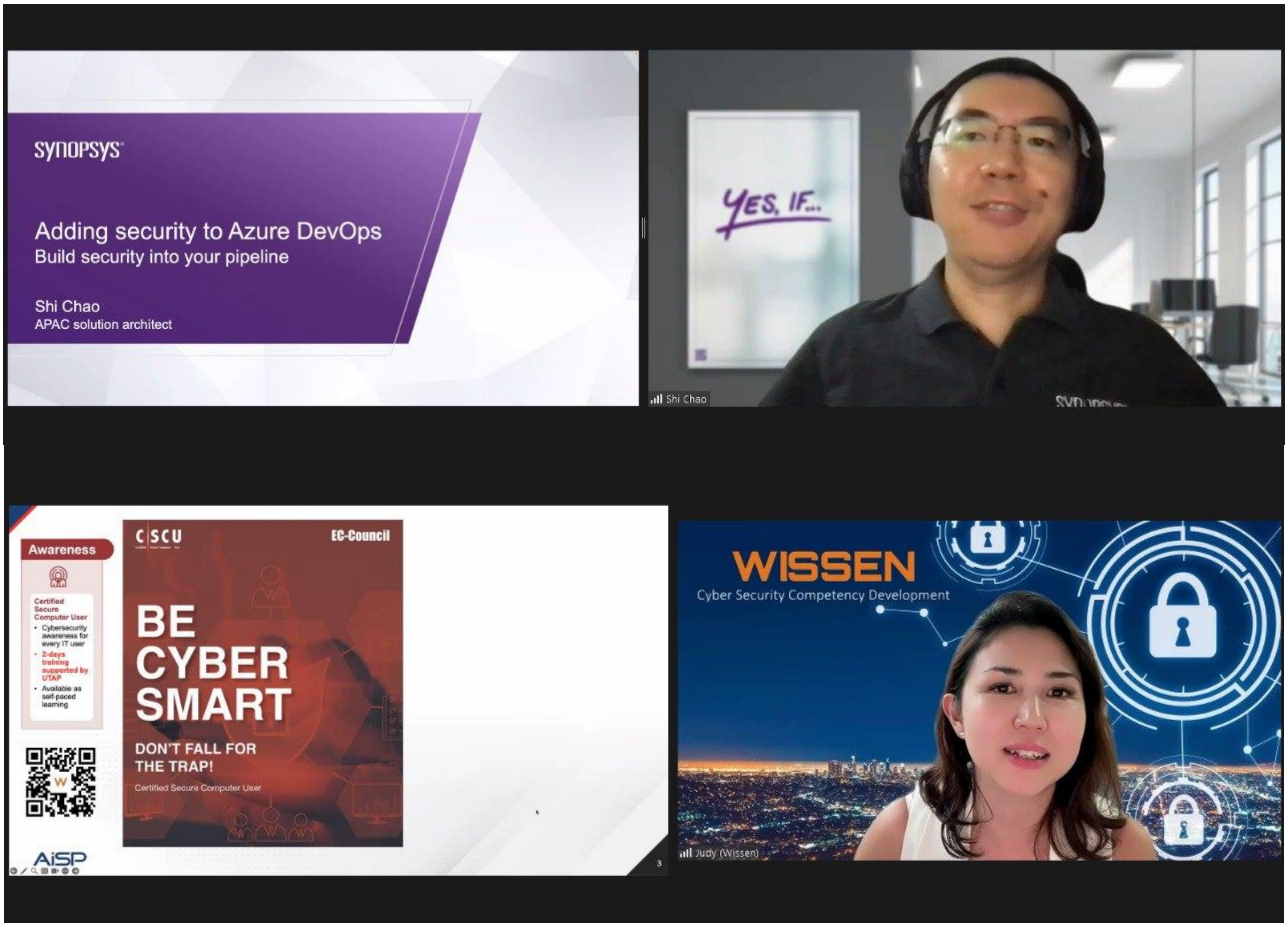
back to top

Knowledge Series Events

DevSecOps on 25 October

As part of Digital for Life movement, AiSP hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 25 October, AiSP organised the knowledge series focusing on DevSecOps, where our Corporate Partners, AZ Asia-Pacific, Responsible Cyber Pte. Ltd. and YesWeHack shared insights with our attendees.

Thank you AiSP Vice-President, Mr Andre Shori for giving the opening address. Shoutout to our Corporate Partner, Wissen International for sharing on the cybersecurity courses during the webinar.



synopsys

Adding security to Azure DevOps
Build security into your pipeline

Shi Chao
APAC solution architect

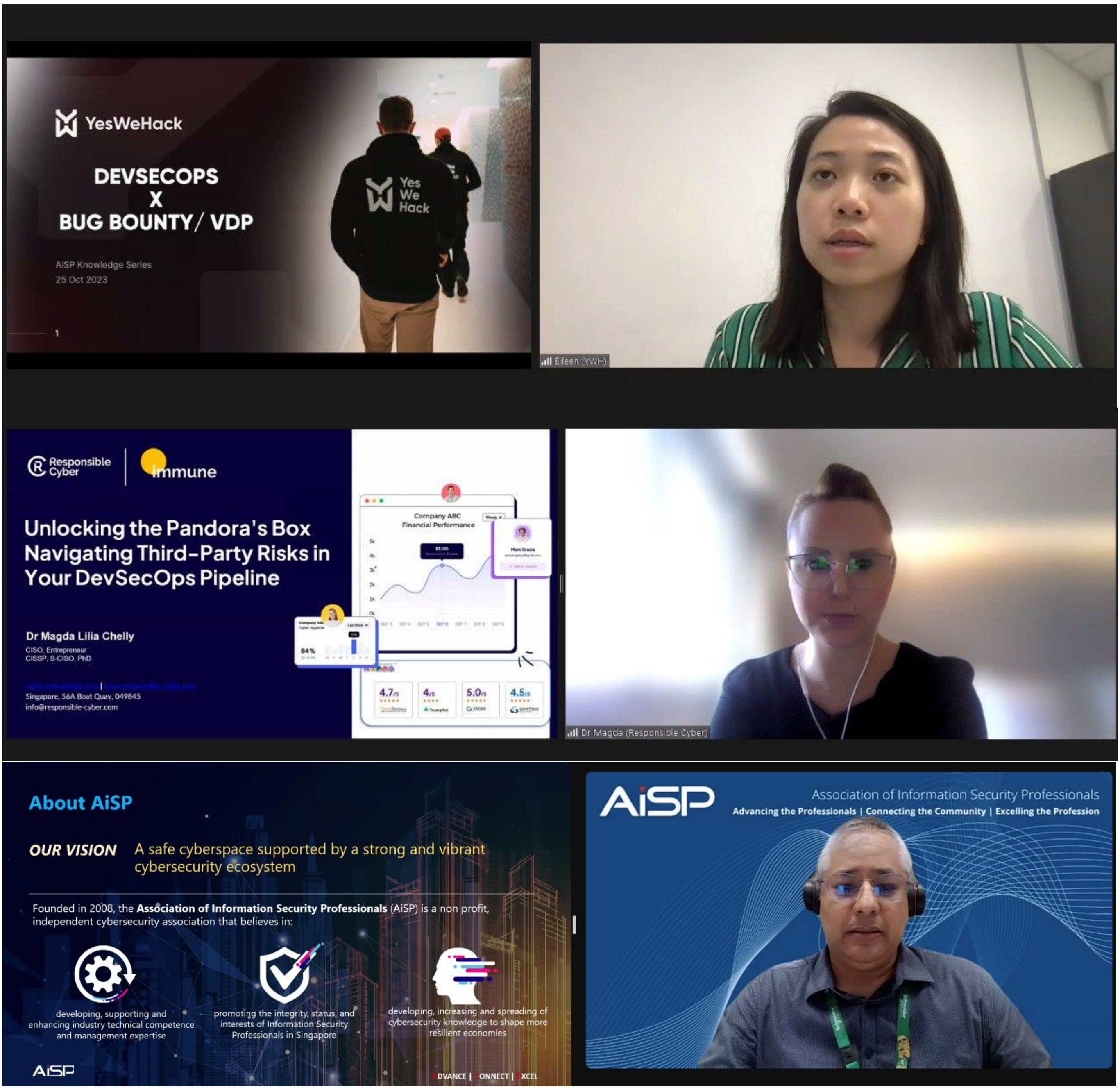
Awareness

Certified Secure Computer User
- Cybersecurity awareness for every IT user
- 2-days training supported by UTAP
- Available as self-paced learning

BE CYBER SMART

DON'T FALL FOR THE TRAP!

Certified Secure Computer User



YesWeHack

DEVSECOPS
X
BUG BOUNTY/ VDP

AiSP Knowledge Series
25 Oct 2023

Eileen (YWH)

Responsible Cyber | immune

Unlocking the Pandora's Box Navigating Third-Party Risks in Your DevSecOps Pipeline

Dr Magda Lilia Chelly
CISO, Entrepreneur
CISSP, S-CISO, PhD

Singapore, 56A Boat Quay, 049845
info@responsible-cyber.com

Dr Magda (Responsible Cyber)

About AiSP

OUR VISION A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem

Founded in 2008, the **Association of Information Security Professionals** (AiSP) is a non profit, independent cybersecurity association that believes in:

- developing, supporting and enhancing industry technical competence and management expertise
- promoting the integrity, status, and interests of Information Security Professionals in Singapore
- developing, increasing and spreading of cybersecurity knowledge to shape more resilient economies

AiSP Association of Information Security Professionals
Advancing the Professionals | Connecting the Community | Excelling the Profession

back to top

Upcoming Knowledge Series

AiSP
Advance Connect Excel

AiSP Knowledge Series – Cyber Threat Intelligence

CYBER THREAT INTELLIGENCE
KNOWLEDGE SERIES
22 November 2023
3PM - 5PM
Zoom
Julie Cabuhat
DFIR Specialist
Blackpanda
Ruevitzwan Isa
Sr Regional SE
Crowdstrike
Organised by
AiSP
Supported by
BLACKPANDA
CROWDSTRIKE

In this Knowledge Series, we are excited to have Blackpanda & Crowdstrike to share with us insights on Cyber Threat Intelligence. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

Shut Your Door on Cyber Threats
Speaker: Julie Cabuhat, DFIR Specialist, Blackpanda

In today's changing world, the presence of cyber threats is an unfortunate fact. It is crucial for any organisation to have an understanding of these threats and take measures to protect themselves. At the session, we will explore the use of cyber threat intelligence strategies in a cyber incident, and dive into the importance of utilising valuable data to empower organisations in their preparation for effective and speedy response from these cyber challenges.

Dissecting Ransomware: Analyzing Adversaries and Emerging Trends in Cyber Extortion
Speaker: Ruevitzwan Isa, Sr Regional SE, Crowdstrike

With ransomware continuing to wreak havoc on organizations globally, it's time to get on the front foot. Join Crowdstrike as we provide a deeper understanding into adversaries behind

back to top

recent major ransomware incidents, along with their motivations and tactics. Learn about the latest attack trends and our projection for the coming threats in 2023 and beyond.

Date: 22 November 2023, Wednesday
Time: 3PM – 5PM
Venue: Zoom
Registration: https://us06web.zoom.us/webinar/register/3916981121845/WN_ERqXm7vAT4-wtclE6B8JFw

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its **Information Security Body of Knowledge 2.0** topics. Our scheduled topics for webinars in 2023 are as follows (*may be subjected to changes*),

1. CTI, 22 Nov

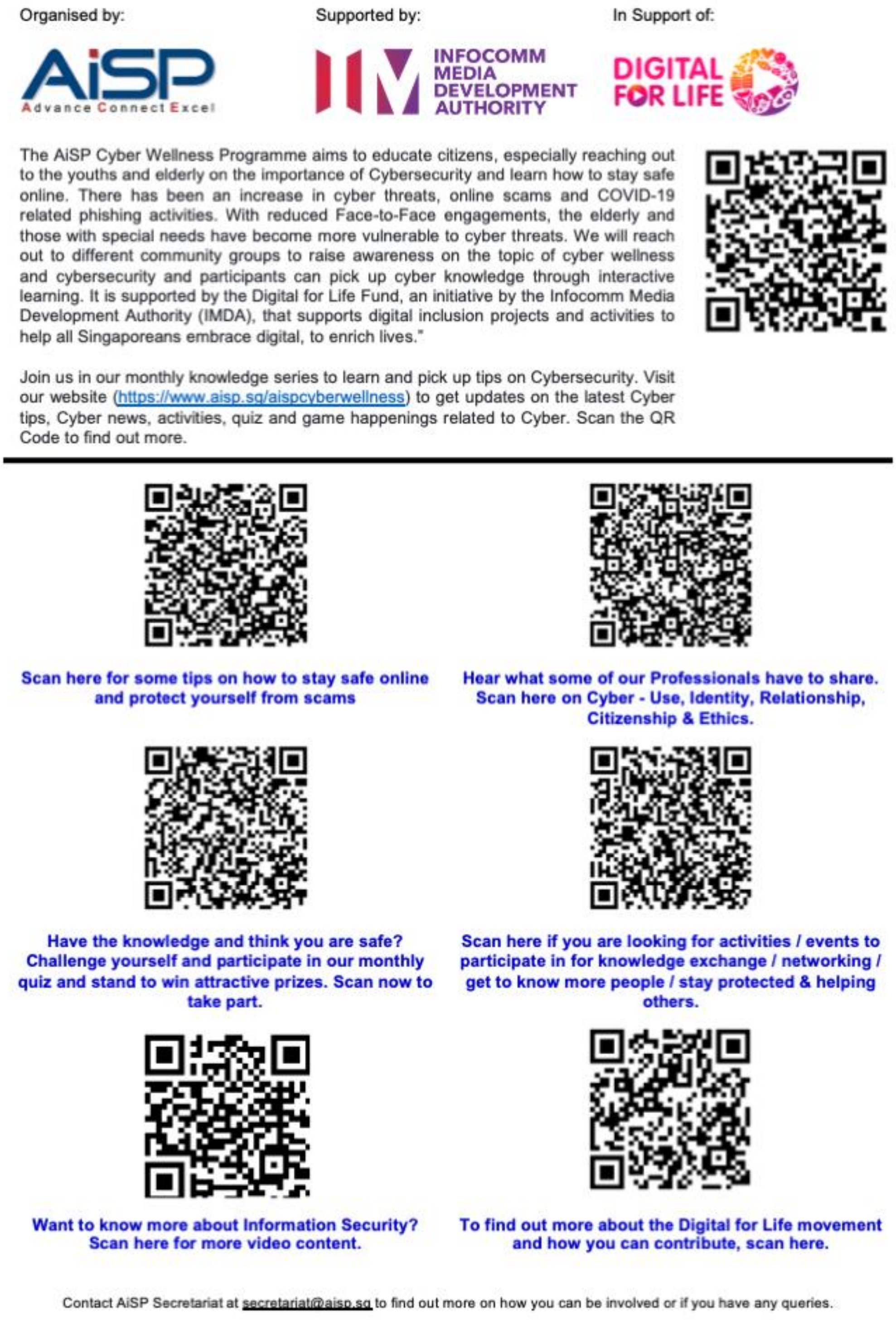
Please let us know if your organisation is keen to provide speakers! Please refer to our scheduled 2023 webinars in our event calendar.

Student Volunteer Recognition Programme (SVRP)

Learning Journey to Acronis on 10 October

As part of Digital for Life movement, AiSP brought 50 students from our Academic Partner, Republic Polytechnic on a learning journey to our Corporate Partner, Acronis on 10 October.

AiSP Cyber Wellness Programme



Organised by: Supported by: In Support of:

The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."

Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website (https://www.aisp.sg/aispcyberwellness) to get updates on the latest Cyber tips, Cyber news, activities, quiz and game happenings related to Cyber. Scan the QR Code to find out more.

Scan here for some tips on how to stay safe online and protect yourself from scams

Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship & Ethics.

Have the knowledge and think you are safe? Challenge yourself and participate in our monthly quiz and stand to win attractive prizes. Scan now to take part.

Scan here if you are looking for activities / events to participate in for knowledge exchange / networking / get to know more people / stay protected & helping others.

Want to know more about Information Security? Scan here for more video content.

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

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

Click here to find out more!

back to top

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 Advance Connect Excel SIG CLOUD SECURITY

AiSP Advance Connect Excel SIG CYBER THREAT INTELLIGENCE

AiSP Advance Connect Excel SIG DATA AND PRIVACY

AiSP Advance Connect Excel SIG INTERNET OF THINGS

AiSP IOT Security Sharing at NTU 2023 on 3 November

Organised by
AiSP
Supporting Partners
CSCIS
Nanyang Technological University Singapore
Supporting Agency
CSA Singapore
Sponsors
ARMIS
CISCO
eclypsium
FORTINET
softScheck
VECTRA

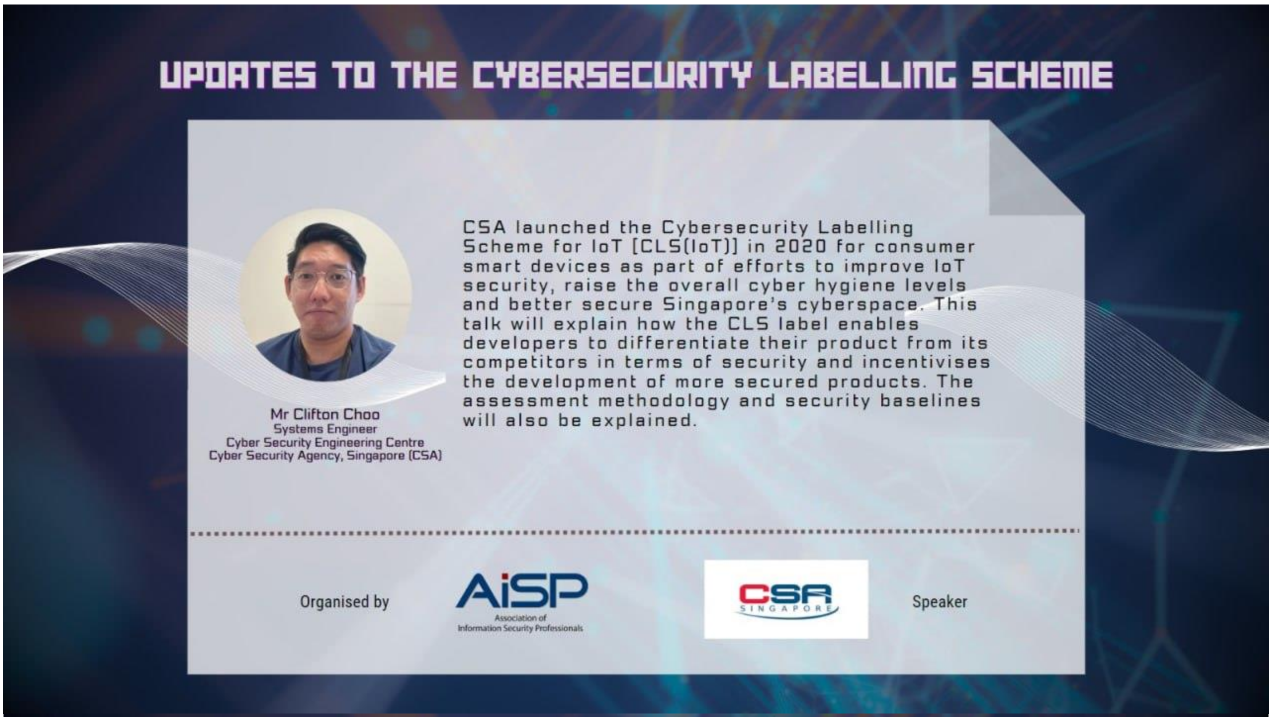
AISP IOT SECURITY SHARING AT NTU 2023

EMPOWERING TOMORROW'S IOT: UNVEILING THE SHIELD OF INNOVATION AND IGNITING LIFELONG LEARNING

03 NOV 2023 | 9:30AM - 2:00 PM
NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE

Guest of Honour: Dr Janil Puthucheary
Senior Minister of State, Ministry of Communications and Information & Ministry of Health

back to top



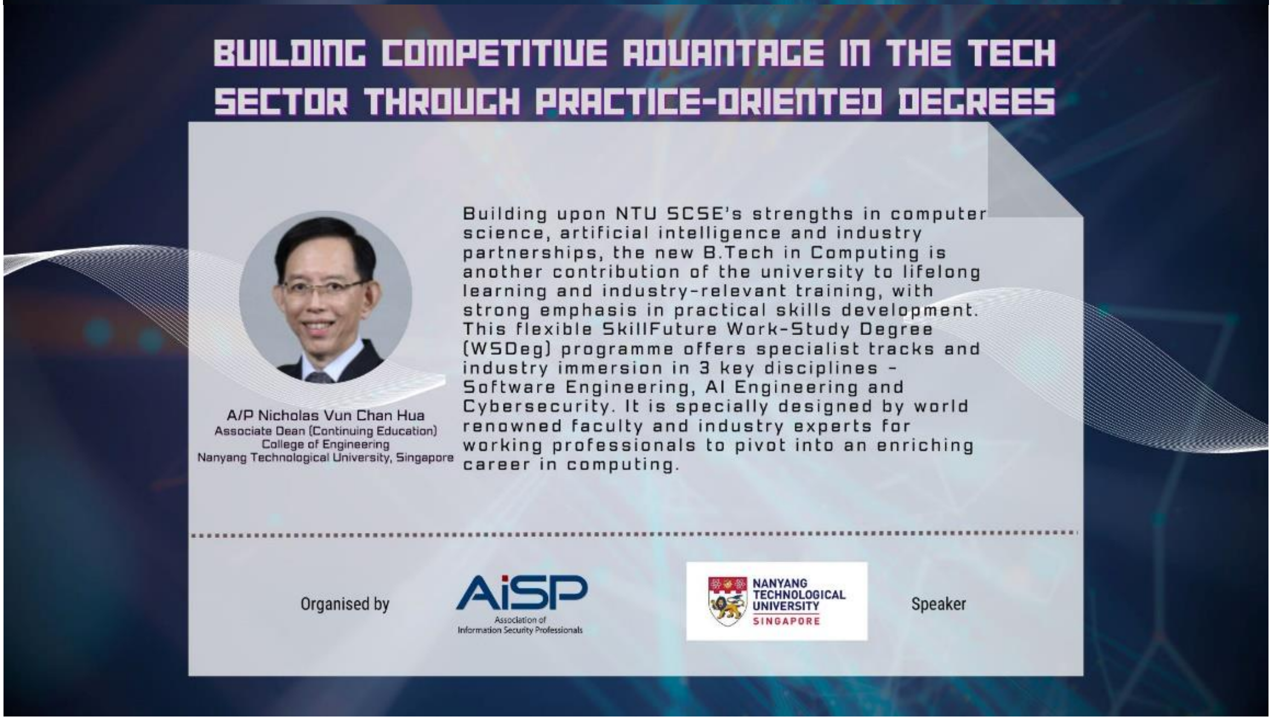
UPDATES TO THE CYBERSECURITY LABELLING SCHEME

CSA launched the Cybersecurity Labelling Scheme for IoT [CLS(IoT)] in 2020 for consumer smart devices as part of efforts to improve IoT security, raise the overall cyber hygiene levels and better secure Singapore's cyberspace. This talk will explain how the CLS label enables developers to differentiate their product from its competitors in terms of security and incentivises the development of more secured products. The assessment methodology and security baselines will also be explained.

Mr Clifton Choo
Systems Engineer
Cyber Security Engineering Centre
Cyber Security Agency, Singapore (CSA)

Organised by AiSP Association of Information Security Professionals

CSA SINGAPORE Speaker



BUILDING COMPETITIVE ADVANTAGE IN THE TECH SECTOR THROUGH PRACTICE-ORIENTED DEGREES

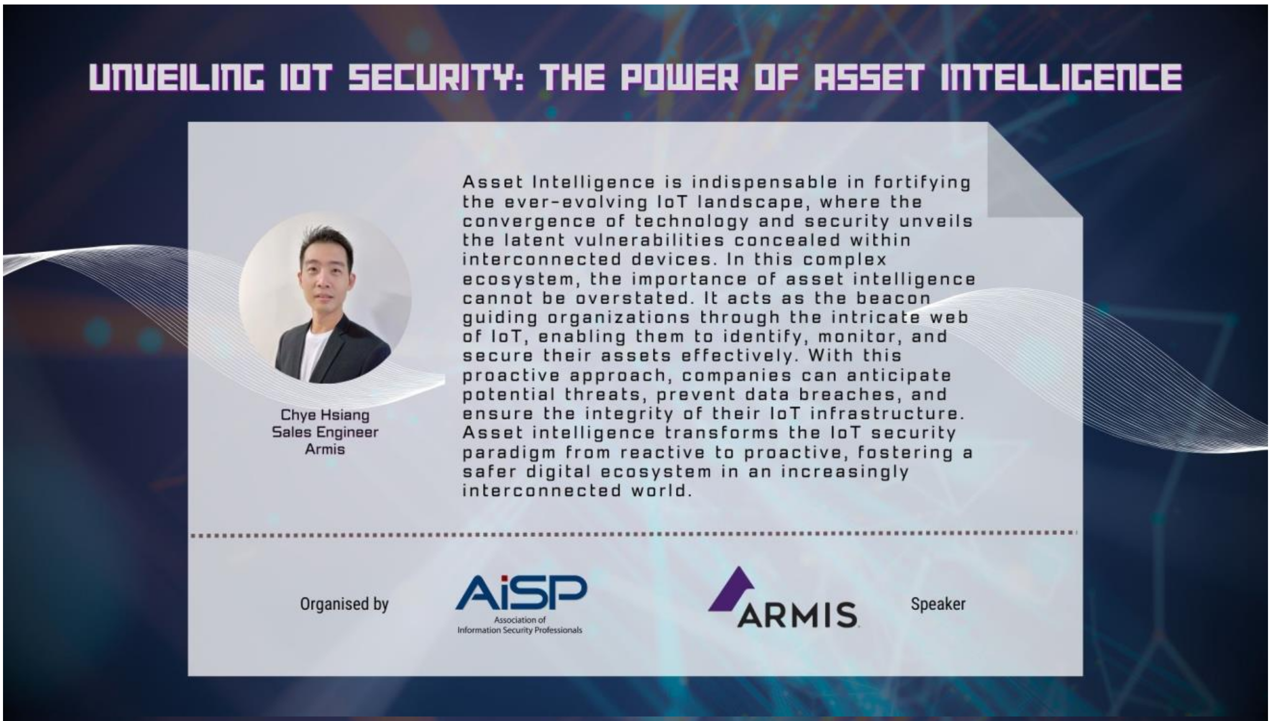
Building upon NTU SCSE's strengths in computer science, artificial intelligence and industry partnerships, the new B.Tech in Computing is another contribution of the university to lifelong learning and industry-relevant training, with strong emphasis in practical skills development. This flexible SkillFuture Work-Study Degree (WSDeg) programme offers specialist tracks and industry immersion in 3 key disciplines - Software Engineering, AI Engineering and Cybersecurity. It is specially designed by world renowned faculty and industry experts for working professionals to pivot into an enriching career in computing.

A/P Nicholas Vun Chan Hua
Associate Dean (Continuing Education)
College of Engineering
Nanyang Technological University, Singapore

Organised by AiSP Association of Information Security Professionals

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE Speaker

back to top



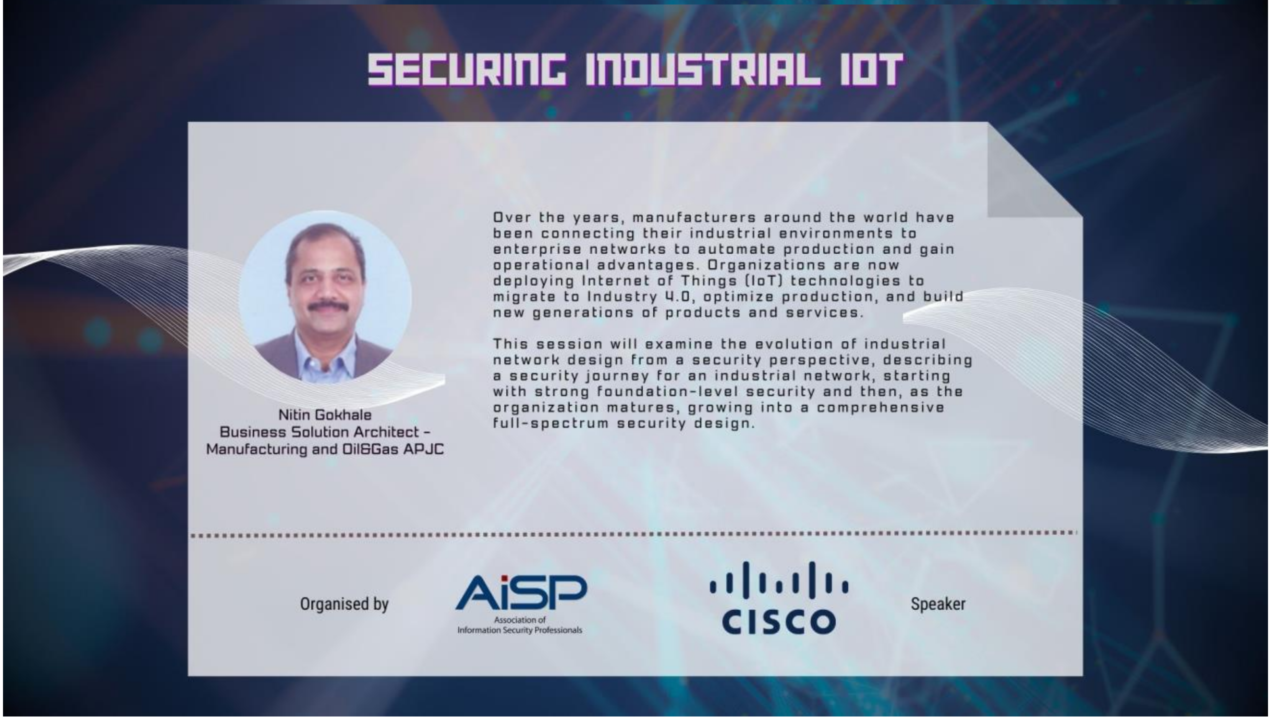
UNVEILING IOT SECURITY: THE POWER OF ASSET INTELLIGENCE

Chye Hsiang
Sales Engineer
Armis

Asset Intelligence is indispensable in fortifying the ever-evolving IoT landscape, where the convergence of technology and security unveils the latent vulnerabilities concealed within interconnected devices. In this complex ecosystem, the importance of asset intelligence cannot be overstated. It acts as the beacon guiding organizations through the intricate web of IoT, enabling them to identify, monitor, and secure their assets effectively. With this proactive approach, companies can anticipate potential threats, prevent data breaches, and ensure the integrity of their IoT infrastructure. Asset intelligence transforms the IoT security paradigm from reactive to proactive, fostering a safer digital ecosystem in an increasingly interconnected world.

Organised by AiSP Association of Information Security Professionals

ARMIS Speaker



SECURING INDUSTRIAL IOT

Nitin Gokhale
Business Solution Architect -
Manufacturing and Oil&Gas APJC

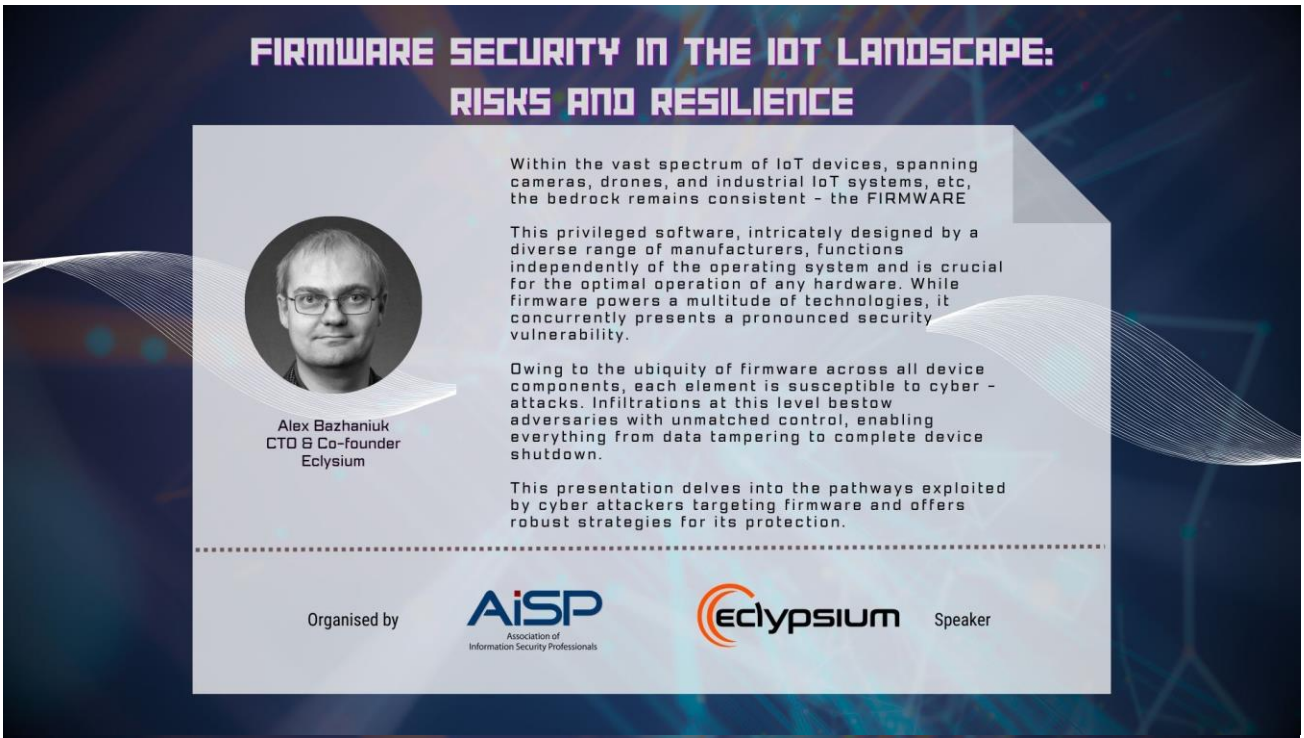
Over the years, manufacturers around the world have been connecting their industrial environments to enterprise networks to automate production and gain operational advantages. Organizations are now deploying Internet of Things (IoT) technologies to migrate to Industry 4.0, optimize production, and build new generations of products and services.

This session will examine the evolution of industrial network design from a security perspective, describing a security journey for an industrial network, starting with strong foundation-level security and then, as the organization matures, growing into a comprehensive full-spectrum security design.

Organised by AiSP Association of Information Security Professionals

CISCO Speaker

back to top



FIRMWARE SECURITY IN THE IOT LANDSCAPE: RISKS AND RESILIENCE

Within the vast spectrum of IoT devices, spanning cameras, drones, and industrial IoT systems, etc, the bedrock remains consistent - the FIRMWARE

This privileged software, intricately designed by a diverse range of manufacturers, functions independently of the operating system and is crucial for the optimal operation of any hardware. While firmware powers a multitude of technologies, it concurrently presents a pronounced security vulnerability.

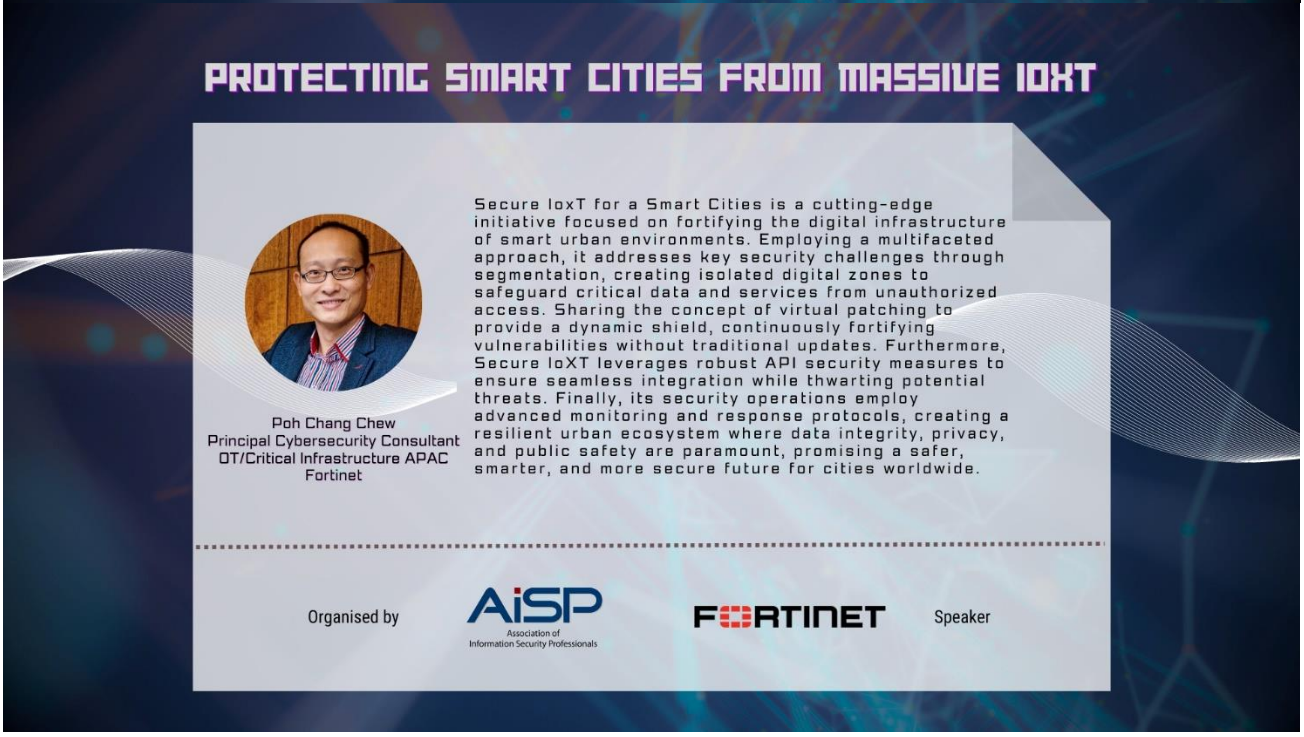
Owing to the ubiquity of firmware across all device components, each element is susceptible to cyber - attacks. Infiltrations at this level bestow adversaries with unmatched control, enabling everything from data tampering to complete device shutdown.

This presentation delves into the pathways exploited by cyber attackers targeting firmware and offers robust strategies for its protection.

Alex Bazhaniuk
CTO & Co-founder
Eclysium

Organised by AiSP Association of Information Security Professionals

eclypsium Speaker



PROTECTING SMART CITIES FROM MASSIVE IOXT

Secure IoxT for a Smart Cities is a cutting-edge initiative focused on fortifying the digital infrastructure of smart urban environments. Employing a multifaceted approach, it addresses key security challenges through segmentation, creating isolated digital zones to safeguard critical data and services from unauthorized access. Sharing the concept of virtual patching to provide a dynamic shield, continuously fortifying vulnerabilities without traditional updates. Furthermore, Secure IoXT leverages robust API security measures to ensure seamless integration while thwarting potential threats. Finally, its security operations employ advanced monitoring and response protocols, creating a resilient urban ecosystem where data integrity, privacy, and public safety are paramount, promising a safer, smarter, and more secure future for cities worldwide.

Poh Chang Chew
Principal Cybersecurity Consultant
OT/Critical Infrastructure APAC
Fortinet

Organised by AiSP Association of Information Security Professionals

FORTINET Speaker

Click here to register.

back to top

Cybersecurity Awareness & Advisory Programme (CAAP)

Safeguarding personal information and identity has become more critical in this digital age. AiSP Vice-President & CAAP EXCO Lead, Mr Tony Low, conducted a sharing to more than 100 attendees focusing on four key areas to raise awareness and empower attendees on 25 October. Through the sharing, attendees understood the importance of securing their personal phone information. They also learned about the actionable steps to safeguard against cyber threats, ensuring a safer digital environment.

AiSP Association of Information Security Professionals

Protecting Your Personal Information and Identity

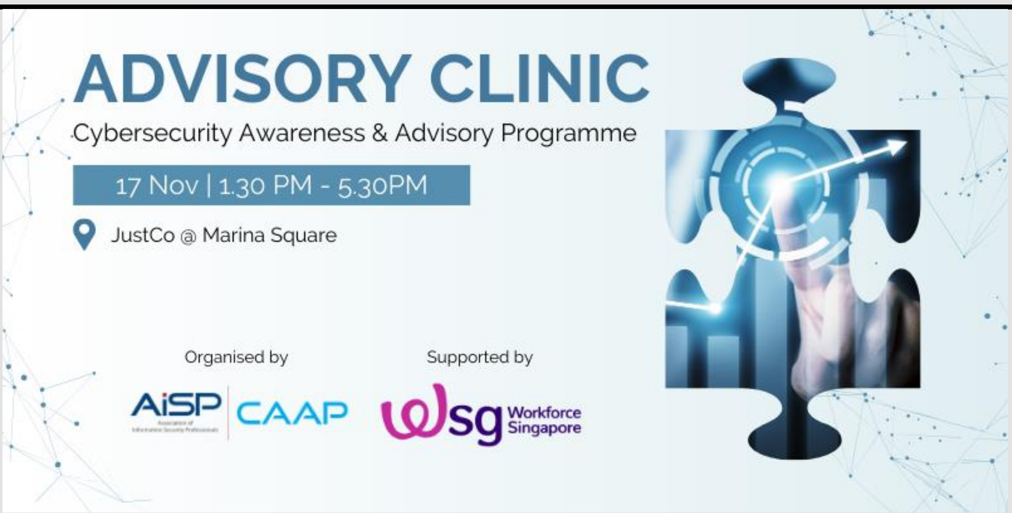
Tony Low, AiSP VP

Royalty-free image for Microsoft O365 subscribers

back to top

AiSP Advisory Clinic on 17 November

AiSP Advisory Clinic



ADVISORY CLINIC

Cybersecurity Awareness & Advisory Programme

17 Nov | 1.30 PM - 5.30PM

JustCo @ Marina Square

Organised by AiSP CAAP

Supported by Workforce Singapore

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

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

Date: 17 Nov 2023
Time: 1.30pm – 5.30pm
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/VHmFTR6Gg6

back to top

The Cybersecurity Awards

THE CYBERSECURITY Awards 2023

The Cybersecurity Awards (TCA) 2023 has officially concluded on 13 October 2023. Congratulations to all The Cybersecurity Awards (TCA) 2023 winners! AiSP would like to thank BeyondTrust, Cisco Systems, Cyber Security Agency of Singapore (CSA), Ensign InfoSecurity, Huawei International, ST Engineering Cybersecurity & Trend Micro for their kind sponsorship as Platinum Sponsors for TCA 2023. DBS Bank, DSTA, Fortinet, SANS, Singtel & wizlynx group for their kind sponsorship as Gold Sponsors for TCA 2023 and Athena Dynamics, Cybersafe Pte Ltd, PCS Security Pte Ltd and Singapore Institute of Technology (SIT), for their kind sponsorship as Silver Sponsors for TCA 2023. Thank you, all sponsors, for contributing to the Cybersecurity Ecosystem.

Sponsorship for The Cybersecurity Awards 2024 is now open, contact the AiSP Secretariat at secretariat@aisp.sg if you are interested in it.

back to top

THE CYBERSECURITY 2023 Awards
Opening Address
Guest of Honour
Mr Tan Kiat How
AiSP Patron,
Senior Minister of State for Communications an tion
AiSP

Digital for Life

People's Association (PA) – Prime Minister Lee Appreciation Reception 2023 on 10 October

On 10 October, Johnny represented AiSP to attend the People's Association (PA) – Prime Minister Lee Appreciation Reception 2023 at PA HQ.

back to top

I am Digitally Ready @ South West on 7 October

As part of the Digital for Life Movement, AiSP was invited to Hillview CC for I am Digitally Ready @ South West to share with the public on how to stay safe online and beware of scams on 7 October.

Thank you Minister of State Ms Low Yen Ling for visiting our booth.

Digital for Life Festival

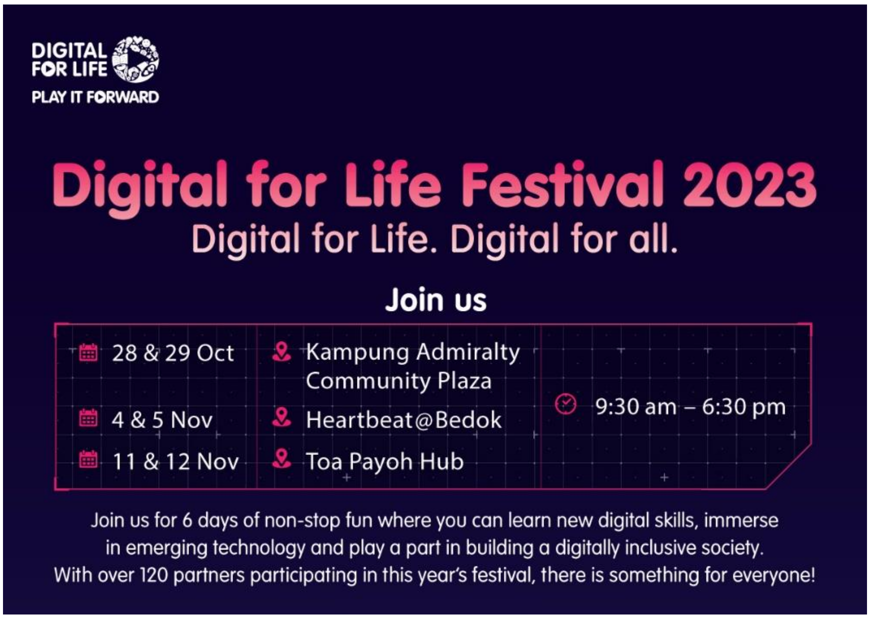
Digital for Life Festival on 28-29 October

The first edition was held at Kampung Admiralty from 28-29 October with our Corporate Partner, Grab. AiSP would like to thank Minister Ong Ye Kung, Minister Gan Kim Yong and Mr Zhulkarnain Abdul Rahim, Grassroots Advisor of Chua Chu Kang GRC for visiting our booth during the two days.

Thank you AiSP EXCO Johnny Kho, Dennis Chan and Catherine Lee for joining us at the event as well.

back to top

As part of Digital for Life movement, AiSP will be participating in the Digital for Life Festival from 28 Oct - 12 Nov.



DIGITAL FOR LIFE
PLAY IT FORWARD

Digital for Life Festival 2023

Digital for Life. Digital for all.

Join us

28 & 29 Oct	Kampung Admiralty Community Plaza	9:30 am – 6:30 pm
4 & 5 Nov	Heartbeat@Bedok	
11 & 12 Nov	Toa Payoh Hub	

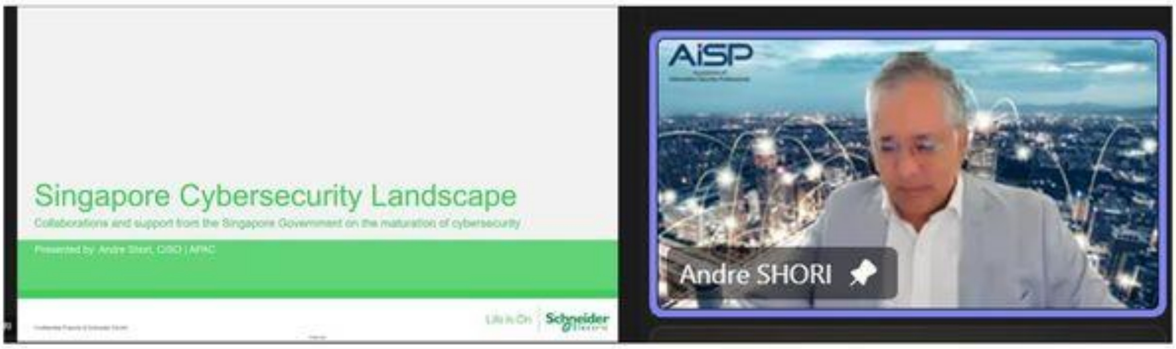
Join us for 6 days of non-stop fun where you can learn new digital skills, immerse in emerging technology and play a part in building a digitally inclusive society. With over 120 partners participating in this year's festival, there is something for everyone!

back to top

Regionalisation

UK Cyber Security Trade Delegation Mission Trip on 2 October

AiSP Vice-President for Partnership, Mr. Andre Shori, had the honor of representing AiSP on 2 October during the briefing organized by the British High Commission Singapore as part of the UK Cyber Security Trade Delegation Mission Trip. He shared invaluable insights on the topic of 'Fostering a Resilient Cybersecurity Ecosystem: The Synergy of Government, Industry Leaders, and Professional Associations'. We extend our heartfelt gratitude to the British High Commission Singapore for this honorable invitation to AiSP. It's an opportunity we greatly cherish to share and collaborate for a safer digital future.


Singapore Cybersecurity Landscape
Collaborations and support from the Singapore Government on the maturation of cybersecurity
Presented by: Andre Shori, CISO | APAC
Life Is On Schneider Electric
AiSP
Andre SHORI

back to top

ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023) on 5 October

AiSP Corporate Partners – Armis, Vectra AI, Wizlynx Group and Acronis Asia joined AiSP in the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023) from 5 to 6 October 2023 where they showcased their services at the conference and participated in the business matching at the event. Mr Leow Kim Hock from wizlynx also attended the conference. Together with AiSP, Armis, Vectra AI, Wizlynx Group and Acronis Asia also joined in the VIP dinner reception hosted by JNSA at Fuji-no-Ma at Meiji Kinenkan.

IC-AJCC
2023
International Conference on ASEAN-JAPAN Cybersecurity Community
5-6 OCTOBER 2023 MEIJI KINENKAN · TOKYO · JAPAN
50
NISC

back to top

ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023) on 5 October

AiSP President, Mr Johnny Kho was in Japan for the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023) on 5 October 2023 where he participated in a Panel Discussion on Collaboration for a Cyber-Safe ASEAN-Japan Community with Leaders of the Brunei Cybersecurity Association (BCSA), Information Sharing and Analysis Center - Cambodia (ISACCambodia), Indonesia Network Security Association (idNSA), Japan Network Security Association (JNSA), Malaysia CyberSecurity Community (rawSEC), Philippine Computer Emergency Response Team (PH-CERT), Thailand Information Security Association (TISA) and Vietnam Information Security Association (VNISA).

Mr Johnny Kho also shared on fostering collaboration within the region to create a thriving and dynamic international information and cybersecurity ecosystem. He emphasized the need for strong connections between governments, industries, communities, and individuals to strengthen our defenses and ensure a safer digital landscape for all.

IC-AJCC 2023
International Conference on ASEAN-JAPAN Cybersecurity Community
5-6 OCTOBER 2023 MEIJI KINENKAN - TOKYO - JAPAN
50 Year of ASEAN-Japan Friendship and Cooperation
AiSP
Collaboration for a Cyber-safe ASEAN-Japan Community
Association of Information Security Professionals

back to top

During the conference, AiSP joined hands with Brunei Cybersecurity Association (BCSA), Information Sharing and Analysis Center - Cambodia (ISACCambodia), Indonesia Network Security Association (idNSA), Japan Network Security Association (JNSA), Malaysia CyberSecurity Community (rawSEC), Philippine Computer Emergency Response Team (PH-CERT), Thailand Information Security Association (TISA) and Vietnam Information Security Association (VNISA) to form the ASEAN JAPAN Cybersecurity Communities Alliance or AJCCA to start exchanges between organizations promoting cross-border exchanges, fostering deeper mutual understanding and recognition among nations. This will help deepen mutual understanding and recognition across countries, allow the exchange of information about cyber security threats, incidents and their solutions in each country, and to promote cooperation between organization members in order to enhance security awareness and capacity building.

IC-AJCC 2023
International Conference on ASEAN-JAPAN Cybersecurity Community
5-6 OCTOBER 2023 MEIJI KINENKAN · TOKYO · JAPAN
50
NISC
COLLABORATION FOR A CYBER-SAFE ASEAN-JAPAN COMMUNITY

back to top

ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023) on 6 October

AiSP Vice-President, Mr Tony Low was in Japan for the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023) on 6 October 2023 where he shared with the participants on the Challenges in Building ASEAN Cyber Resilience. Tony also shared on the opportunity within ASEAN post-pandemic and a collective community effort by the ASEAN JAPAN Cybersecurity Communities Alliance (AJCCA).

IC-AJCC
2023
5-6 OCTOBER 2023 MEIJI KINENKAN - TOKYO - JAPAN
International Conference on ASEAN-JAPAN Cybersecurity Community
50
AiSP
Challenges in building ASEAN Cyber Resilience
Tony Low, AiSP VP

The International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023) came to an end on 6 October 2023 evening with a closed door dinner attended by the leaders of Brunei Cybersecurity Association (BCSA), Information Sharing and Analysis Center - Cambodia (ISACCambodia), Indonesia Network Security Association (idNSA), Japan Network Security Association（JNSA, Malaysia CyberSecurity Community (rawSEC), Philippine Computer Emergency Response Team (PH-CERT), Thailand Information Security Association (TISA) and Vietnam Information Security Association (VNISA).

AiSP Vice-President Mr Tony Low joined in the dinner and reaffirmed the support that AiSP will provide to the ASEAN JAPAN Cybersecurity Communities Alliance (AJCCA) and thanked JNSA for hosting the dinner and invited JNSA and all the other leaders to Singapore in 2024 for the Cloud Security Summit 2024.

back to top

SEACC Forum on 16 October

On 16 October, the second Southeast Asia Cybersecurity Consortium (SEACC) Forum was held at SIT@NYP with AiSP Patron SMS Tan Kiat How gracing the event as the GOH. All the 10 SEACC members were present which included representatives from Brunei Cybersecurity Association (BCSA), ISAC-Cambodia (InfoSec),Indonesian ICT Business Association (APTIKNAS), Malaysia Board of Technologist (MBOT), Myanmar Information Security Association (MISA), Thailand Information Security Association (TISA), Vietnam Information Security Association (VNISA) and Women in Security Alliance Philippines (WISAP).

During the forum, two MoUs were signed with AiSP to further the commitment of building a safer and resilient digital world beyond borders. AiSP signed an MoU with corporate partner Huawei to actively engage in cybersecurity training programs such as AiSP's Qualified Information Security Professional (QISP) certification, ensuring that a wider range of audience can upskill and increase certification opportunities in the field of cybersecurity.

AiSP is opening new doors with a joint MoU with Aptiknas and BCSA by translating AiSP Body of Knowledge book into Malay and Bahasa Indonesia. This initiative will help our friends in Brunei and Indonesia gain access to invaluable resources in their native language and applicable in their respective countries.

Thank you all who have contributed to another successful SEACC Forum!

back to top

SEA CC FORUM 2023
MiSA

SEA CC FORUM 2023
MiSA
VNISA

SEA CC FORUM 2023

SEA CC FORUM 2023
16 OCT 2023
SIT@N
Guest of Honour: A

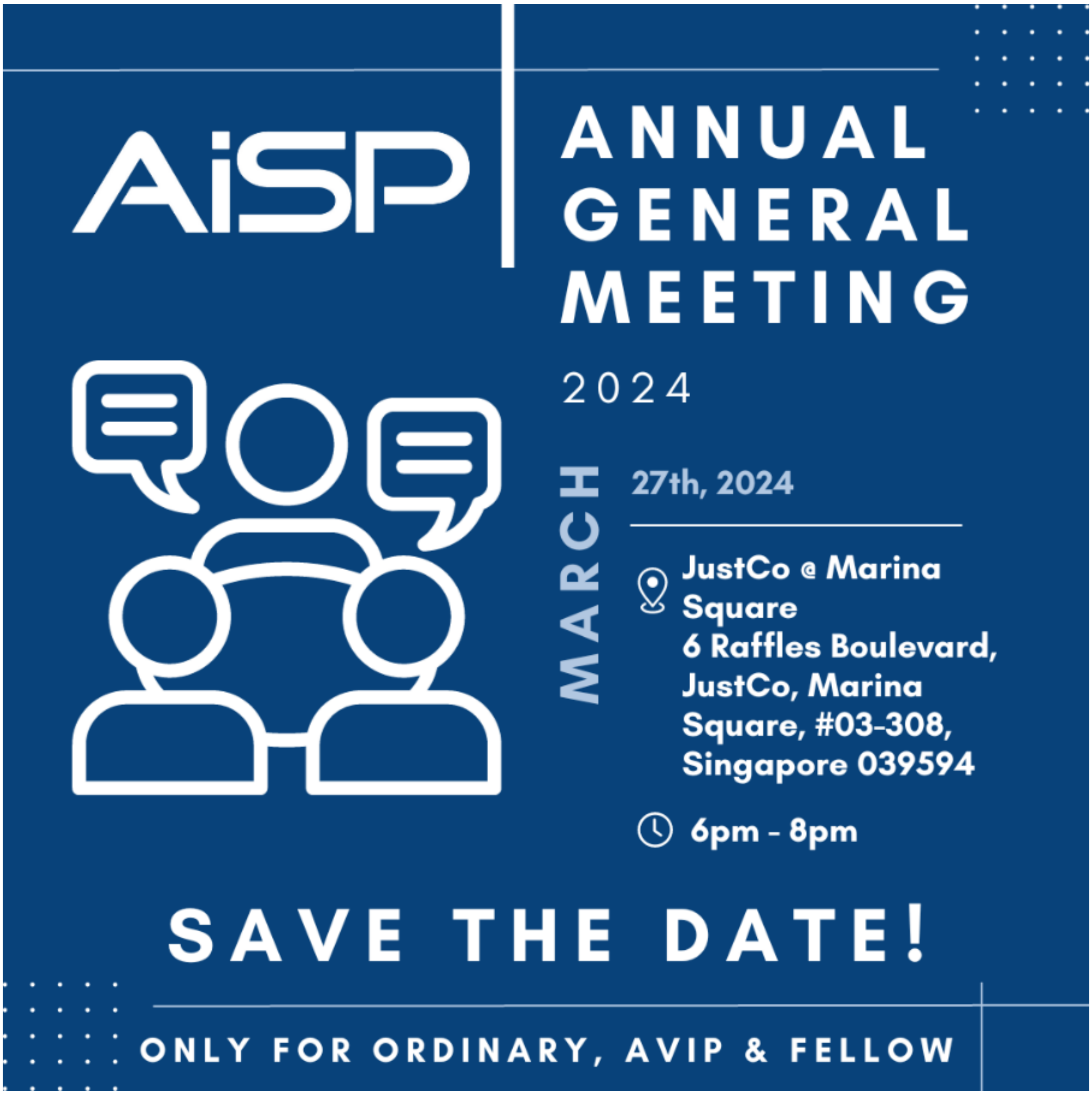
SEA CC FORUM 202
16 OCT 2023 | 9:30AM - 12:3
SIT@NYP Building
Guest of Honour: AiSP Patron, Mr Tan Kiat H
Minister of State, Ministry of Communica

How fast can a Qubit go?
Quantum Computing

AiSP

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

Ladies in Cyber

SailPoint in the Women+ In Identity Security Executive Lunch Roundtable on 24 October

AiSP is happy to support our CPP – SailPoint in the Women+ In Identity Security Executive Lunch Roundtable on 24 October held at Mandarin Oriental Marina Bay attended by 30 female leaders. AiSP Ladies in Cyber Mentor & Monetary Authority of Singapore (MAS) Agency CISO Ms Claudean Zheng together with our CPP – Temasek CISO Ms Cheri Lim joined Charmaine Valmonte in the roundtable session moderated by Ms Wendy Wu. Thank you Sailpoint for inviting AiSP and having us at the event.

SailPoint
Women+
in Identity Security
Moderator:
Wendy Wu
Chief Marketing Officer
SailPoint
Charmaine Valmonte
Chief Information Security Officer
aboitiz
Cheri Lim
Chief Information Security Officer
TEMASEK
MAS
Monetary Authority of Singapore
Claudean Zheng
Head of Cybersecurity, Agency CISO,
Monetary Authority of Singapore

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
3 Nov	**IoT Security Sharing at NTU 2023**	AiSP & Partner
4 – 5 Nov	DFL Festival – Bedok	Partner
10 Nov	**SVRP 2023 Awards Ceremony**	AiSP & Partner
11 – 12 Nov	DFL Festival – Toa Payoh	Partner
15 – 17 Nov	Singapore FinTech Festival	Partner
21 - 22 Nov	CISO Auckland	Partner
22 Nov	Knowledge Series - CTI	AiSP & Partner
29 Nov	CISO Indonesia	Partner
29 – 30 Nov	CDIC 2023	Partner
1 Dec	TCA 2023 Judges Appreciation	AiSP
3 Dec	Bukit Batok East Active Ageing Committee (AAC) - “ Wellness Day 2023”	Partner
9-10 Dec	STANDCON 2023	Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Data & Privacy SIG

Contributors
Ms. Qothrunnada Istiqamah & Ms CHUA Jia Ling
Reviewer / Advisor
Mr. HOI Wai Khin
Technology Compliance Team, RSM Risk Advisory Pte Ltd

IMPORTANCE OF HAVING A DATA BREACH RESPONSE / MANAGEMENT PLAN – AT WORK AND EVEN IN LIFE

With the rise in data breaches across all industries, we know that the negative impacts can take a costly toll on businesses, especially for small and medium-sized enterprises with limited resources. The importance of developing a robust data breach response plan and conducting regular exercises to evaluate the plan's effectiveness has been stressed by many experts, time and time again. And, as technology consultants, I couldn't agree more.

If you have been working in Singapore, there is a good chance that you have participated in annual fire drills in the workplace. To many, it was just another good excuse to skip work and chit-chat with friends while everybody all causally strolled to safe holding area or to the nearby coffee shop for a cup of coffee. It was all routine until a real fire broke out in the pantry.

Thankfully, the workplace's annual fire drills had indeed paid off and when a real crisis occurred, everyone was well-prepared. After the fire alarm went off, the appointed fire wardens remained calm and quickly guided everyone to the nearby stairs for evacuation. Upon further investigation, it was found that the fire had started from one of the microwave and with the swift response by well-trained staff, the flames were contained and extinguished without any casualties.

From this incident, it was recognised that it is crucial for every organisation to not just have a evacuation plan but to also get everyone else on board it. The regular fire drill training and rehearsals allowed staffs to become familiar with the escape routes and all necessary precautions to take during an emergency. These measures helped everyone to stay calm, allowing for a smooth, orderly and safe response to a potentially life threatening situation. The earlier fire drills also allowed the workplace to identify weak

back to top

spots to further strengthen the incident response preparedness and be better equipped for the real thing.

Similarly, in the business context, businesses are strongly advised to have a well-documented and regularly tested data breach response plan. The data breach management team and employees must be clear about their roles and responsibilities so that in the event of a security or data breach, they can quickly detect, respond and limit the consequences of any malicious cyber-attack.

The Personal Data Protection Commission on 15 March 2021 has updated a "Guide on Managing and Notifying Data Breaches Under the PDPA". The guidelines provided guidance on 3 areas; (1) Preparing for data breaches, (2) Responding to data breaches and (3) The data breach notification obligation.

The key takeaway for the guidelines are as follows;

(1) Preparing for data breaches	Ensure a data management plan is properly established and tested
(2) Responding to data breaches	Ensure management of data breach follows the C.A.R.E framework (Contain, Assess, Report, Evaluate)
(3) The data breach notification obligation	Ensure there is a process to report to PDPC Within 3 calendar days if there is a confirmed breach.

In today's digital world, data breaches and cyber attacks are an ever-present threat to organizations of all sizes and types. As such, data breach preparedness is not a luxury, but a necessity. It is not a matter of if a data breach will occur, but rather when it will strike your business.

To minimize the potential business disruptions, financial impact, and reputation damage that can result from a data breach, it is essential to have a robust plan in place. This plan should include clear guidelines on how to detect, respond to, and recover from a breach.

In conclusion, waiting until a data breach occurs before implementing a plan is not a viable strategy. By then, it may be too late to mitigate the damage caused. Instead, organizations must prioritize data breach preparedness by proactively developing and regularly testing their data breach management plans.

Author Bio

Wai Khin leads a team of professionals to manage the Firm's and clients' technology governance, risk, compliance ("GRC") programmes to meet legal, human resources, audit, IT, risk management and information security requirements. With significant experience in this sphere, he engages in the innovation of ideas to implement value-

back to top

added GRC programmes to support both the Firm's and the client's organisational objectives to build robust GRC frameworks that go beyond regulatory compliance.

Article from Corporate Partner, Sailpoint

Unpacking the Horizons of Identity Security 2023-24

Authored by Jaishree Submramania, Vice President Product Marketing

Historically, nautical explorers have often used the North Star as a guiding light, providing critical direction among vast and uncharted territories. Just as those explorers relied on that constant beacon, modern enterprises need a steadfast guide in the sprawling digital realm. Identity security is that guide, delivering organizations safely and securely to their innovative futures.

As our digital horizons expand, peppered with cloud innovations and looming cyber threats, charting the right course isn't a mere recommendation—it's essential. SailPoint, in collaboration with Accenture, recently published "The Horizons of Identity Security 2023-24" report, which extends upon last year's introduction of these key concepts and dives deeper into critical issues. This year's report offers comprehensive insights and action steps for organizations at various stages of identity security maturity.

The future of identity security

Identity Horizons: A revealing look at slow adoption rates

The 2023 report continues to build upon an insightful framework introduced in last year's Horizons of Identity" report, ranging from Horizon 1 (least mature) to Horizon 5 (most mature). Companies in Horizon 1 lack both comprehensive identity strategy and technology, whereas those in Horizon 5 employ next-gen technologies to blur the boundaries between enterprise and external identity controls. It's worth noting that 44% of the 375 companies surveyed are still at Horizon 1, missing out on the potential benefits that come with mature identity programs. However, about 8% of companies have successfully made the jump from Horizon 2 to Horizon 3.

Reaping the rewards: Real-world benefits of advanced identity security

For organizations that have advanced beyond the early stages of identity security, the tangible business benefits are impressive. Real-world examples showcase a large bank boosting its cloud migration speed by 15-20% and another financial services firm automating processes to reduce user access certifications by 80%. Moreover, a utility company dramatically shortened employee and partner onboarding from over two weeks to mere hours. Meanwhile, a prominent process manufacturer saved $1M in IT operations within a single year.

back to top

These success stories highlight the operational efficiencies and cost-saving opportunities a mature identity program can deliver. Importantly, data suggests that low-maturity companies shouldn't shy away from embracing advanced capabilities. While adoption rates differ, ranging from 15-90%, the actual usage of these capabilities remains steady at about 50-70%, regardless of the complexity or the maturity level of the company. This means that even less mature companies can achieve comparable success to their more mature counterparts when implementing and scaling advanced capabilities.

Making the business case: Tackling budget and boardroom hurdles in identity security

Across all maturity levels, the most significant barrier is a constrained budget, with 91% of survey respondents mentioning it as a primary obstacle. This lack of investment stems from the inability of security professionals to articulate the business value of identity programs, thus making it hard to gain executive sponsorship. Interestingly, 77% of respondents cited "limited executive sponsorship or focus" as another major hurdle, reinforcing the need for improved communication between security professionals and decision-makers. Overcoming these challenges is critical for companies to advance along the identity horizons and reap the benefits of operational efficiencies and risk mitigation.

From slow to go: Speeding up identity implementation with SaaS, AI/ML, and automation

Companies that utilize advanced technologies such as SaaS, AI/ML, and automation experience enhanced benefits, implementing new capabilities 20% faster and scaling them 37% quicker than those that don't. Additionally, these technologies improve the utilization of identity security capabilities across the organization. According to the report, these technological investments are pivotal in helping organizations leapfrog from lower maturity horizons, like Horizon 1 or 2, to more advanced stages, like Horizon 3, where identity capabilities are adopted at scale. These technologies not only speed up implementation but also contribute to broader coverage, including third-party and machine identities, ultimately fortifying the organization's overall security posture.

Driving to scale: Managing unique challenges in Identity Horizons

Even though a constrained budget is a common challenge across all horizons, the specific obstacles vary. For those at the earliest stages (Horizon 1), managing technical debt and developing a robust operating model are crucial for breaking the inertia. In contrast, mature companies, particularly those at Horizons 4 and 5, should focus on expanding the coverage of their existing capabilities to achieve holistic identity security programs. Interestingly, the report highlights that even companies with advanced identity capabilities often struggle to cover more than 70% of the identities in their organization. Therefore, mature companies need to not only scale but also aim for more comprehensive coverage, including third-party identities, machine identities, and data, to build a truly robust identity security program.

back to top

Industries and geographies: Who is at the forefront of identity security

When compiling this year's report, we noted a couple interesting takeaways.

- While the technology and banking sectors are at the forefront of identity security, utilities and manufacturing are making rapid strides, likely driven by the increasing complexity of their identity ecosystems and large attack surfaces.
- Geographically, North America and Europe lead in identity security maturity, with APAC presenting a mix of maturity levels.

Navigating your identity journey: An adoption assessment tool

Charting your organization's identity security progress in is no easy task. To aid companies in pinpointing their current position and potential growth areas, we've developed an adoption assessment tool. The adoption assessment tool will:

-Help you determine where you currently stand in your identity journey

-Gauge your capability utilization against competitors in your sector

-Discover common obstacles faced by similar businesses and identify tailored solutions to overcome your unique challenges

By understanding the value proposition of an effective identity program and investing wisely, you'll be ready for stronger security and business growth. You'll uncover more insights than you think.

Ready for the future?

To succeed in today's digital world, companies must prioritize identity security, not just as a protective measure but as a business enabler.

Don't just adapt; lead the way in identity security and set your organization up for a future where you're not just surviving, but thriving.

Ready to secure your identity landscape? Download the SailPoint Horizon's of Identity Security report for more information, or schedule a conversation to discuss your identity security environment today.

For any enquiries, please contact Ms Winnie Parsons at winnie.parsons@sailpoint.com

back to top

Article from TCA 2023 Sponsor, DSTA

Adversarial Robustness through Adversarial Training

With the proliferation of AI systems, the Defence Science and Technology Agency (DSTA) has looked into the area of adversarial AI, where adversaries exploit the vulnerabilities in AI models to bypass them or to extract sensitive information. Upon understanding these vulnerabilities, DSTA's cybersecurity programme centre then builds defences to strengthen the agency's AI models. Adversarial training is one such defence used to improve the robustness of these AI models.

Introduction

Adversaries can carry out adversarial attacks on AI models by tricking them with deceptive data inputs to produce unintended and incorrect results. The example of an adversarial attack on an image classification model below is one such case. An adversary could take the image of a cat and apply small, calculated perturbations or 'noise'. To the human eye, the two images seem the same – even if one of them was slightly grainier, they both still definitely showed a cat. To the AI model, however, its prediction has changed from a cat to a dog. Weird, huh?

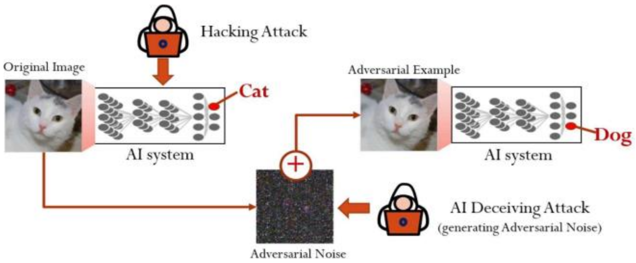


Figure 1: Adversarial attack on an image of a cat.
Real-Time Adversarial Attack Detection with Deep Image Prior Initialized as a High-Level Representation Based Blurring Network. Accessed on 18 Sep 2023, https://www.mdpi.com/2079-9292/10/1/52.

This has become a growing threat to AI, especially in the area of safety and security. Imagine a self-driving vehicle which uses an image recognition model to determine its actions. Upon seeing a red light, it should stop. If an attacker could somehow perturb the image and cause the model to misclassify it as a green light, the results could be devastating.

Targeted Retraining

To defend against such attacks, a common approach would be to retrain the model against adversarial samples by populating the dataset with both clean and adversarial

back to top

samples. A common issue for adversarial retraining is a phenomenon called the Robustness Accuracy Tradeoff, characterised by the inverse relationship between clean and adversarial accuracy. However, increasing adversarial accuracy comes at the expense of clean accuracy.

To minimise this impact, we explore targeted retraining, where the model is retrained with adversarial samples of a critical class, and clean samples from the remaining classes. The rationale behind this is if a less important class is wrongly classified, it would result in a false alarm. On the other hand, if a critical class is wrongly classified, the repercussions would be severe as it may result in a potential threat being undetected (e.g., a combat vessel being misclassified as a yacht). With targeted retraining, the aim is to enhance the robustness accuracy tradeoff as the model will not be exposed to too many adversarial samples.

Recently, an adversarial robustness benchmark called RobustBench which uses AutoAttack (AA) was created to benchmark models trained with adversarial attacks. We will use targeted AA adversarial samples to retrain a model and see how the results between standard and targeted training methods differ. The adversarial samples are generated from the Adversarial Robustness Toolbox, a python library for Machine Learning Security. The specifications and methodology for the training are shown below:

Model	Xception CV
Dataset	Vessels
Attacks used	AA, Projected Gradient Descent (PGD), Fast Gradient Sign Method (FGSM)
Samples/set	964

Table 1: Experimental Setup Specifications

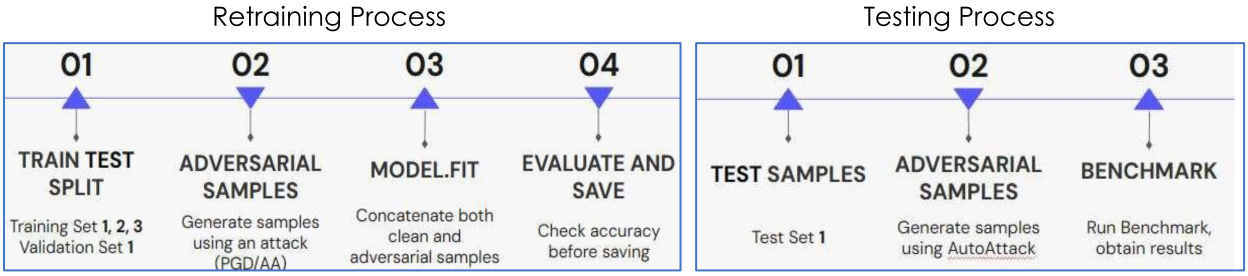


Figure 2: The retraining and testing processes

Due to limitations ranging from time to limited hardware resources, we will only be retraining three sets of clean and adversarial samples in total. One thing to note is that the samples chosen are all true positive, so the model would have classified all the samples correctly before retraining.

Results

back to top

As shown in Figure 3 below, when comparing targeted AA-retrained models (bottom graphs) to the untargeted ones (top graphs), we note the following:

- There is an increase in clean accuracies for both the general and target classes
- There is a decrease in adversarial accuracy for the general class, but an increase in adversarial accuracy of the target class
- While there was a greater decrease in clean accuracy of target class, there was also a greater increase in adversarial accuracy of the target class
- The improvement in adversarial accuracy for the target class using FGSM samples is the most significant
- One noticeable change is the huge increase in adversarial accuracy for FGSM attacks, which could suggest that AA might deal with FGSM-nature attacks. However, this might be a red herring, as the model may only be trained to defend against a specific epsilon value of FGSM, and might fail against other epsilon values.

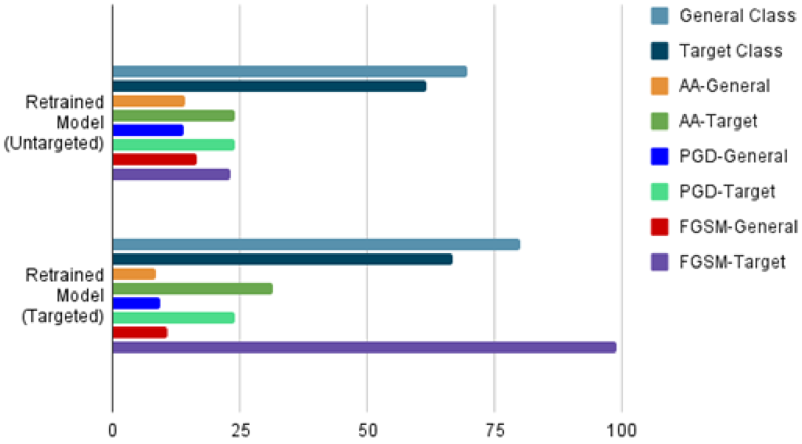


Figure 3: Performance (in terms of clean and adversarial accuracy) of untargeted and targeted AA-retrained models. Clean accuracies (for General Class and Target Class) refer to the model's accuracy on the unperturbed original samples. Adversarial accuracies (<Attack>-General and <Attack>-Target) refer to the model's accuracy on the samples perturbed using the corresponding attack.

Conclusion

There were several limitations when conducting this study, from the limited training provided to the models and testing size, to overfitting (which caused the model to be unable to distinguish between what is real and what is not when conducting adversarial training). More could also be done, such as fine-tuning the parameters to adjust the training loop to be more tailored to adversarial training, and exploring more forms of training methods. However, targeted retraining may still prove essential to improve robustness against a subset of critical classes. Optimising the robustness accuracy trade-off ensures that the AI models are robust for deployment, while maintaining a high level of accuracy.

back to top

Linus Yeong is a merit cyber scholar interning with the cybersecurity programme centre at DSTA. His work stints involve explorations in adversarial robustness, specifically designing a benchmark to evaluate the robustness of in-house models. Linus's curiosity was piqued when DSTA increased its usage in AI. He started analysing and finding exploits in various model file formats, and researching into solutions to ensure AI developers can utilise these model files safely.

Learn more about the work DSTA does at www.dsta.gov.sg.

Article from IoT Sponsor, Armis

Revolutionize Your Cybersecurity: See, protect and manage your entire environment with the AI-powered Armis Asset Intelligence Engine and Cybersecurity Platform

In the dynamic landscape of connected devices, ensuring the security of every asset is more critical than ever. With the proliferation of Internet of Things (IoT) devices, the attack surface for potential threats is expanding exponentially. The Armis Asset Intelligence Engine and Security Platform addresses the challenges posed by this with total deep asset visibility, contextualisation, segmentation and real-time monitoring.

Introducing Armis: A New Paradigm in OT/IoT Security

Imagine having the ability to see and secure every asset in your network, from traditional devices to IoT gadgets, regardless of their connectivity or location. Armis brings this visionary concept to reality. It offers an innovative approach that embraces a comprehensive, proactive strategy, enabling your organization to achieve cyber and operational resilience now and in the future.

The Power of Asset Intelligence

At the core of Armis lies the concept of Asset Intelligence. This means gaining a granular understanding of every device in your ecosystem, tracking their behaviors, vulnerabilities, and patch statuses throughout their lifecycle. In harnessing this intelligence, your organization can:

- **Gain Complete Inventory Visibility:** No asset goes unnoticed. Armis helps you identify and categorize every device, even those lurking in the shadows.

- **Continuous Risk Assessment:** Stay ahead of potential threats by identifying vulnerabilities and mitigating risks in real-time. Armis keeps an ever-watchful eye on device behaviors, ensuring a proactive response.

back to top

- **Efficient Patch Management:** Vulnerabilities are part of the game, but Armis ensures they don't stay that way for long. Prioritize and apply patches effectively, minimizing exposure.

- **Anomaly Detection:** Detect unusual device activities or unauthorized connections swiftly. Armis helps you spot breaches before they escalate.

- **Regulatory Compliance Made Easier:** Compliance is simplified with an accurate record of IoT devices and data flows, helping you meet data protection regulations seamlessly.

- **Swift Incident Response:** If a security incident occurs, Armis enables pinpoint accuracy in identifying affected devices, allowing you to contain threats quickly.

Embrace a New Era of IoT Security

With Armis, your organization can rise above the challenges of IoT security. The platform empowers you to navigate the limitations of traditional active scanning security models, creating an environment of trust, reliability, and longevity in your interconnected world. Embrace the future of cybersecurity and discover how Armis redefines the art of protection.

Ready to revolutionize your security strategy? Explore the world of Armis here.
[CTA Button] Request a Demo
CTA Link: https://www.armis.com/demo

Secure your assets. Protect your future. Manage with Armis.

For any enquiries, please contact Ms Nina Fomin at nina.fomin@armis.com

back to top

Updates from IMDA

Gain the Competitive Advantage and Build Consumer Trust with the Infocomm Media Development Authority's Data Protection Trustmark Certification!

The **Data Protection Trustmark (DPTM)** is a voluntary, enterprise-wide certification that is developed based on Singapore's Personal Data Protection Act (PDPA) & international standards, and serves as a badge of recognition that your institution adopts accountable & responsible data protection practices. Since the launch in 2019, more than 200 organisations have being certified, with many more undergoing assessment.

2 The DPTM will help you by:

i. Providing **assurance** – With a growing number of data breaches, the DPTM will help your business demonstrate PDPA compliance through a third-party validation of your data protection practices, uncover potential weaknesses and improve your data governance. The DPTM may also serve as a mitigating factor in the event of a data breach.

ii. Increasing **competitive advantage** – In a 2022 survey conducted by the PDPC, **4 in 5 companies** preferred to engage DPTM-certified companies – the DPTM will set you apart from your competitors! With a growing demand for DPTM-certified companies by both public & private sectors, being certified will greatly strengthen your reputation as a trusted company and increased your competitive advantage both locally and internationally.

Apply Now!

3 It pays to have the Data Protection Trustmark! **Apply for the DTPM** at www.imda.gov.sg/dptm. **Grants available for a limited time!**

4 For enquiries, please reach us at Data_Protection_Certifications@imda.gov.sg.

back to top

3 Business Benefits in 3 Steps with the Data Protection Trustmark

DATA PROTECTION ASSURED

Get your organisation certified with the Data Protection Trustmark (DPTM) for a competitive edge!

Gain customer trust

Customers know they can trust your organisation to safeguard personal data

Provide assurance to your organisation

You can be assured that your data protection practices will be sufficiently robust to minimise data risks

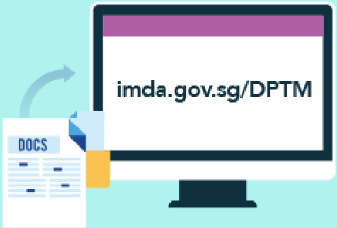
Do more with your data

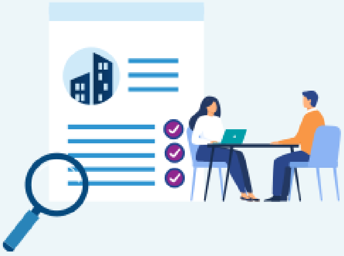
With accountable data management practices, you can make better use of your data to improve efficiency and customer experience

Your 1.2.3 to DPTM Certified

1 Application

Apply online at **imda.gov.sg/DPTM**





2 Assessment

Appoint an Assessment Body to have your organisation's data protection practices assessed

3 Certification

Get certified for three years with approval from IMDA

Certify your organisation today.

Grants support available.

back to top

www.imda.gov.sg/dptm Data_Protection_Certifications@imda.gov.sg

Jointly developed by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

In support of:

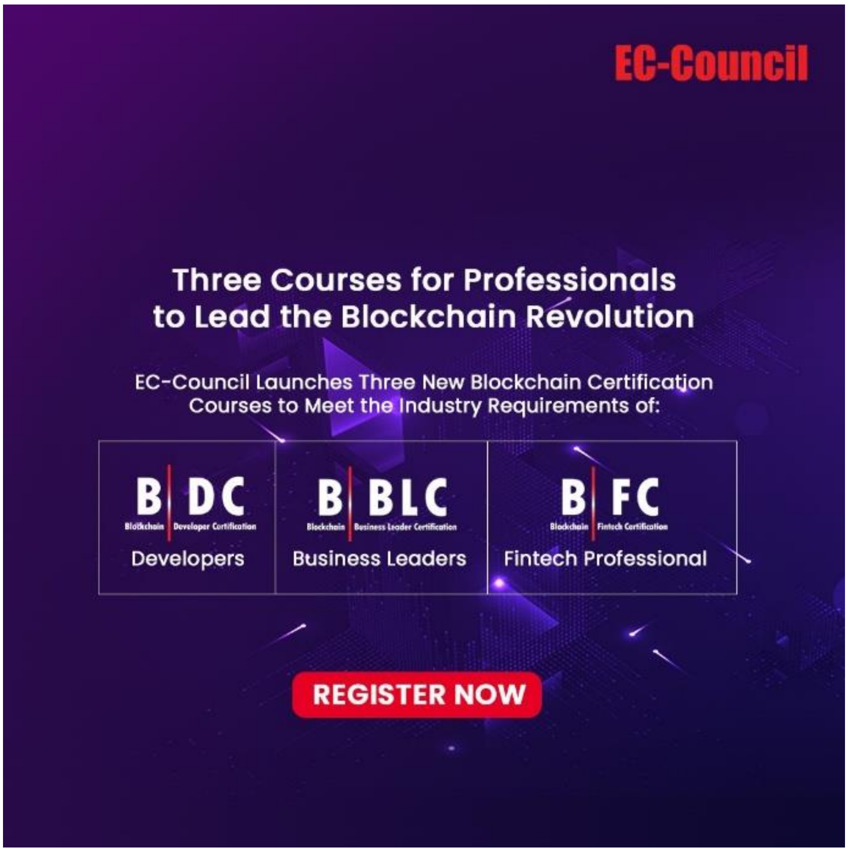
SG:D EMPOWERING POSSIBILITIES

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

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

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International



EC-Council

Three Courses for Professionals to Lead the Blockchain Revolution

EC-Council Launches Three New Blockchain Certification Courses to Meet the Industry Requirements of:

B DC Blockchain Developer Certification	B BLC Blockchain Business Leader Certification	B FC Blockchain Fintech Certification
Developers	Business Leaders	Fintech Professional

REGISTER NOW

back to top

EC-Council's Blockchain Certifications Overview

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

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

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

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

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

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

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

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

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

back to top

Listing of Courses by ALC Council

alc
ADVANCE YOUR CYBER CAREER
with world-class certification training
CISM® • CRISC® • CISA® • CGEIT®
SABSA® • NIST® • CISSP® • CCSP®

Stand out from the crowd

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

We offer the most in-demand cyber certifications including:

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

The right training makes all the difference

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

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

AiSP Member Pricing – 15% discount

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

back to top

Upcoming Training Dates

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

Special Offers.

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

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

Thank you.

The ALC team

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

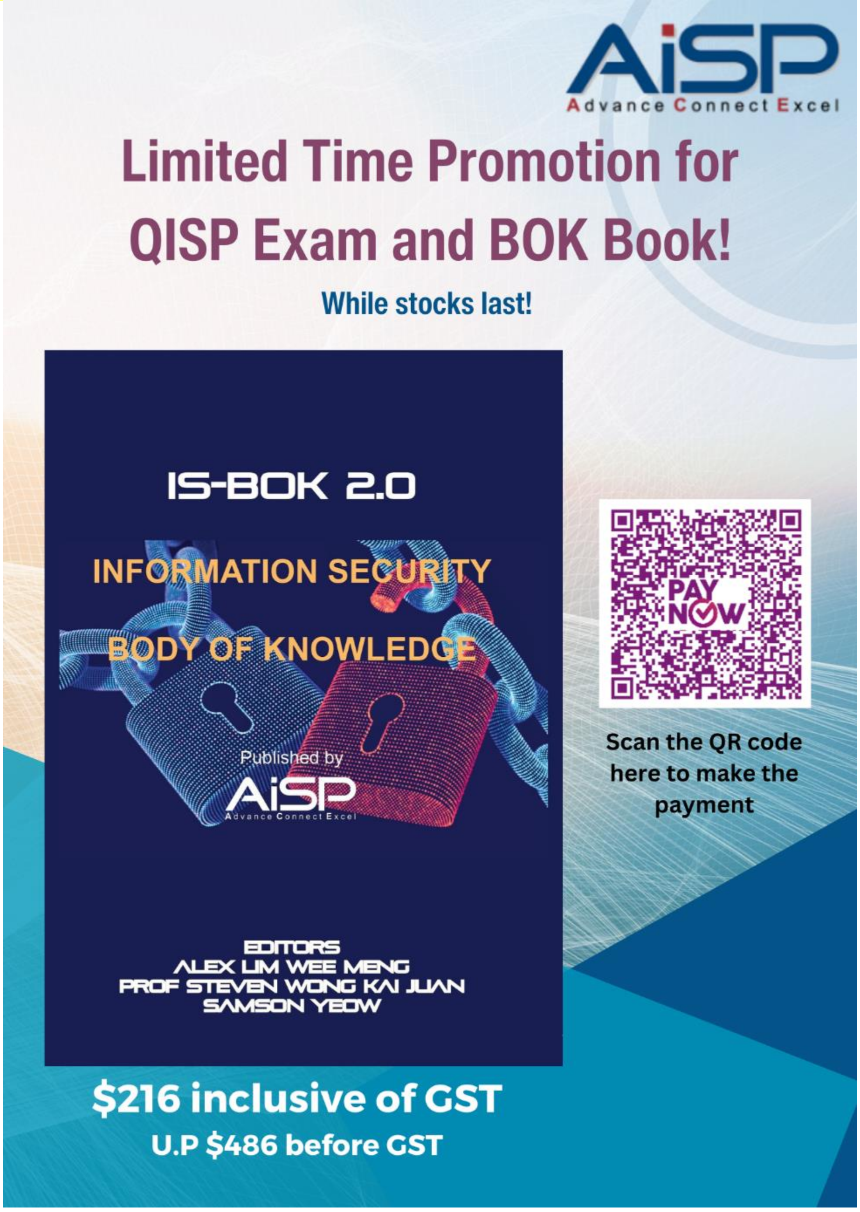
Advertisements placed on the AiSP website is in no way intended as endorsements of the advertised products and services. No endorsement of any advertisement is intended or implied by AiSP.

Qualified Information Security Professional (QISP®)

BUNDLE PROMOTION VALID TILL 30 NOVEMBER 2023

As part of SICW GovWare event, we are extending our promotion. Looking to advance your cybersecurity expertise? Exciting news – we've got the ultimate bundle for you!

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 **30 November 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

WISSEN
Cyber Security Competency Development
AiSP
Advance Connect Excel
QISP
Qualified Information Security Professional

READY TO TAKE YOUR CYBERSECURITY SKILLS TO THE NEXT LEVEL?

JOIN OUR VLT CLASS!

Enrol for QiSP inaugural VLT batch to enjoy 50% discount from the course fees!

Based on the latest version of BOK, this course will prepare you for QiSP exam.

Scan the QR code to find out more!

www.wissen-intl.com/qisp

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

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

back to top

AiSP Corporate Partners

ABPGROUP

Acronis

ARMIS

AZ ASIA-PACIFIC

ASUS

BD

BeyondTrust

BLACKPANDA

bugcrowd

CISCO

C8N+FINITY

CLIXER

CROWDSTRIKE

CSA SINGAPORE

CSIT Centre for Strategic Infocomm Technologies

CYBERSAFE YOUR SECURITY, OUR PRIORITY

CYBER SECURITY HUB

CYFIRMA DECODING THREATS

CzechTrade SINGAPORE

DBS

DETACK

DT ASIA Security with Confidence

eclypsium

ENSIGN INFOSECURITY

FERGUS CONSULTANCY GROUP

Fidelis Services Redefined

FORESCOUT Automated cybersecurity across your digital terrain

FORTINET

GETVISIBILITY own your data

GOVTECH SINGAPORE

back to top

Grab

HORANGI
CYBER SECURITY

HUAWEI

image engine

INTfinity

IT SEC ASIA

kaspersky

KnowBe4
Human error. Conquered.

LEARNCOLLAB

Lookout

MANDIANT

METASECURITY

opentext™

mimecast

ncs//

NETWITNESS
An RSA Business

OneSECURE®

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

back to top

ThriveDX Formerly Cybint

TREND MICRO

VECTRA

VOTIRO

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