

## News & Update

- Knowledge Series
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Special Interest Groups
- CAAP
- The Cybersecurity Awards
- Digital for Life
- Regionalisation
- Corporate Partner Events
- AiSP x JTC Networking Event
- Upcoming Events

## Contributed Contents

- CTI SIG: A Threat Intelligence Analyst's Diaries
- Opentext: How AI Can Be Used as a Business Advantage

## Professional Development

## Membership

# NEWS & UPDATE

## New Partners

AiSP would like to welcome Sailpoint as our new Corporate Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

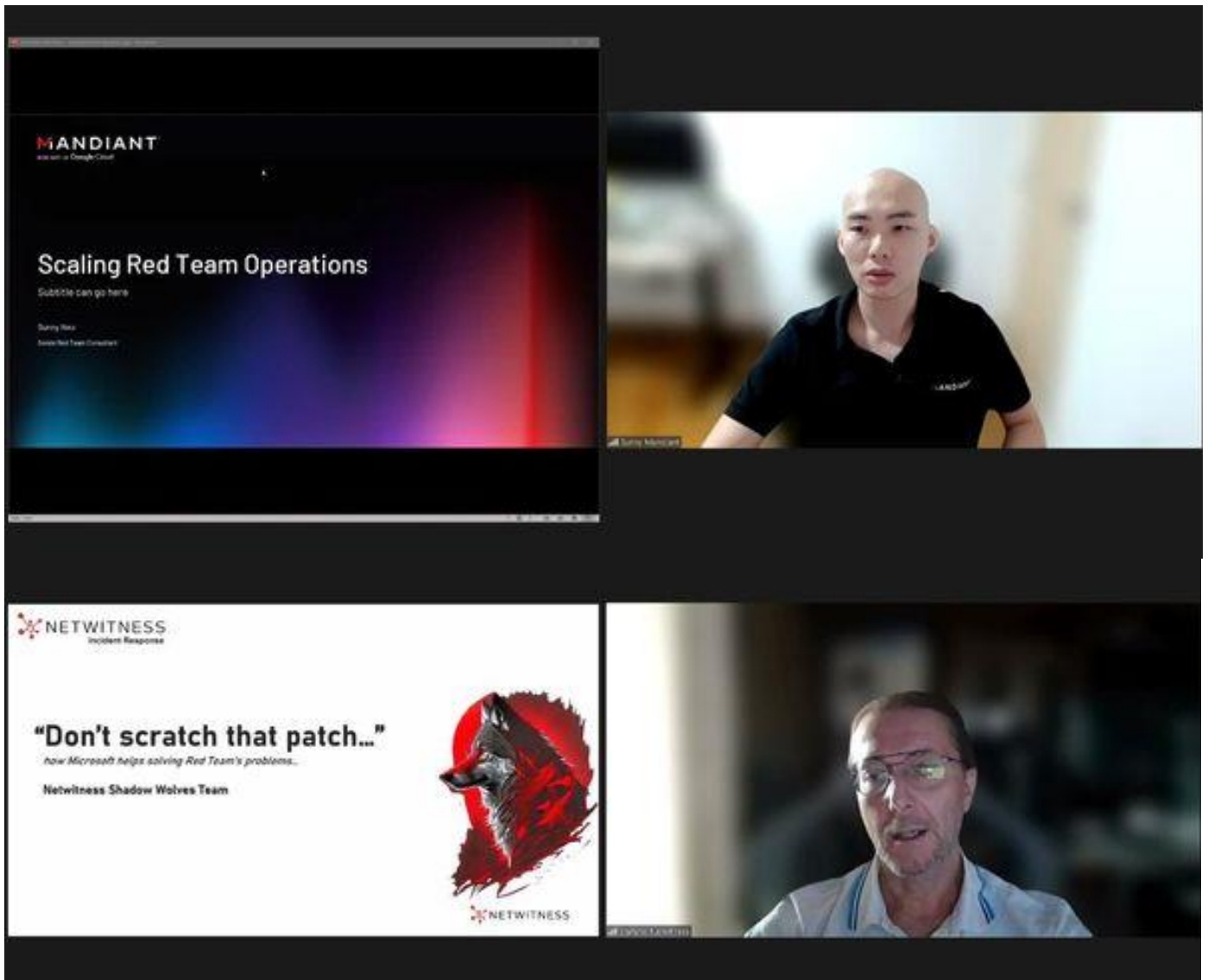
### New Corporate Partners

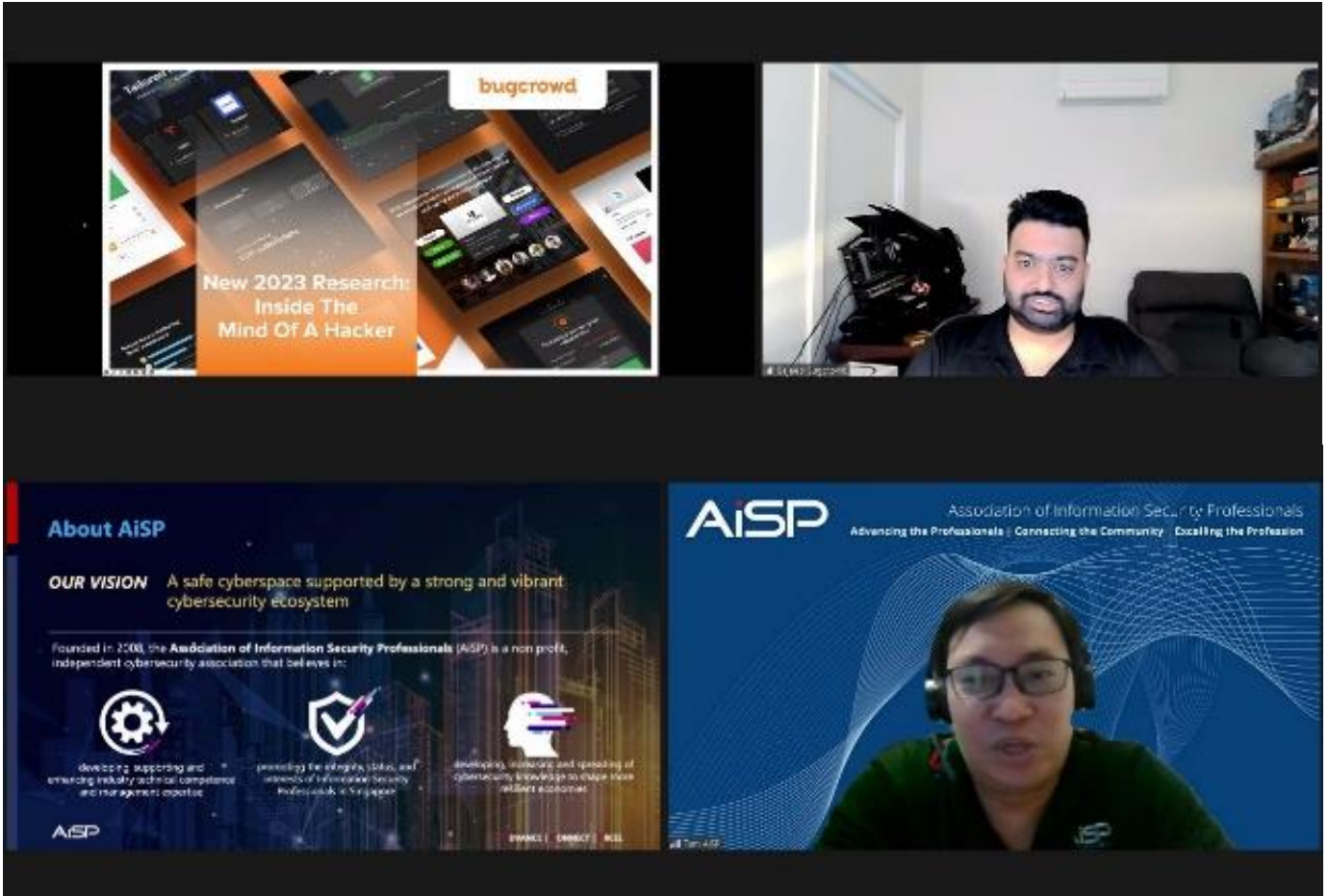


# Knowledge Series Events

## Red Team on 20 September

As part of Digital for Life Movement, AiSP organised the Knowledge Series today focusing on Red Team on 20 September. Thank you to our Corporate Partners Bugcrowd, Mandiant & NetWitness for sharing insights with our attendees. Thank you AiSP Assistant Secretary , Mr Tam Huynh for giving the opening address.





## Upcoming Knowledge Series

DevSecOps on 25 October



**AiSP**  
Advance Connect Excel

**AiSP Knowledge Series – DevSecOps**



**AiSP KNOWLEDGE SERIES**  
**DEVSECOPS**  
25 Oct 2023 | 3PM - 5PM | Zoom.



Shi Chao  
Solution Architect  
Synopsys



Dr Magda Lilia Chelly  
Managing Director, CISO  
Responsible Cyber Pte. Ltd.  
Co-Founder  
Women on Cyber



Eileen Neo  
APAC Regional Lead  
YesWeHack



Organised by    In support of



Supported by



In this Knowledge Series, we are excited to have AZ Asia-Pacific, Responsible Cyber & YesWeHack to share with us insights on DevSecOps. 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.

**Build secure, high-quality software faster in Microsoft Azure**  
Speaker: Shi Chao, Solution Architect, Synopsys

Every business is a software business. Digital transformation is reshaping the way organizations operate. Whether you're one of the thousands of companies that sell software, or one of the millions that use software to run your business, your ability to innovate and deliver value to your customers is powered by secure, reliable software.

Join us and discover how you can easily manage risk throughout your Software Development Lifecycle with extensions for Azure DevOps, bring testing to IDE and integrate automation into your software pipeline.

**Unlocking the Pandora's Box: Navigating Third-Party Risks in Your DevSecOps Pipeline**  
Speaker: Dr Magda Lilia Chelly, Managing Director, CISO, Responsible Cyber Pte. Ltd.; Co-Founder, Women on Cyber

[back to top](#)


© 2008 – 2023 Association of Information Security Professionals. All rights reserved.


Page 4 of 44

Are you aware that your DevSecOps pipeline could be a ticking time bomb? With third-party components embedded at almost every stage of the software development cycle—from source code repositories and build tools to cloud services and monitoring tools—the risks are pervasive and often under the radar.


Join us for this eye-opening presentation where we unravel the complexities of third-party risks in your DevSecOps pipeline.


But worry not! This isn't a tale of doom and gloom. Instead, it's your guide to fortifying your DevSecOps process against potential weak links.

 Learn how third-party code can be a Trojan Horse in your system.

 Get insights into the hidden vulnerabilities in CI/CD tools, container images, and even your trusted security scanning software.

 Discover how cloud services could be your Achilles' heel.

 Understand why even your monitoring tools need monitoring!

 Equip yourself with actionable strategies to secure every phase of your DevSecOps pipeline.

Don't leave your DevSecOps process exposed. Seal the cracks, strengthen your defenses, and build with confidence. Register now to become part of the solution to one of DevSecOps' most pressing challenges!

### **Bug Bounty and VDPs as drivers of DevSecOps**

Speaker: Eileen Neo, APAC Regional Lead, YesWeHack

Traditional pentesting requires a lot of coordination and scheduling, which makes it antithetical to DevSecOps, where testing must be agile and launchable at short notice. Learn how Bug Bounty and VDPs ensure that vulnerabilities are continuously surfaced and evaluated, in alignment with a DevSecOps approach, powered by a global community of testers.

Date: 25 Oct 2023, Wednesday

Time: 3PM – 5PM

Venue: Zoom

Registration:

[https://us06web.zoom.us/webinar/register/2816956971013/WN\\_6ORozfDcTYeN3pBaXHF5SQ](https://us06web.zoom.us/webinar/register/2816956971013/WN_6ORozfDcTYeN3pBaXHF5SQ)

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 Brunei from 11 September to 15 September

Supported by National Youth Council Singapore, AiSP brought students on an overseas learning journey to Brunei, from 11 - 15 Sep. They visited University of Technology Brunei, Brunei Shell Petroleum Co. Sdn. Bhd, Progresif, BIBD Bank Islam Brunei Darussalam, Cyber Security Brunei & Information Technology Protective Security Services (ITPSS) and AITI. AiSP would like to thank University of Technology Brunei, Brunei Shell Petroleum Co. Sdn. Bhd, Progresif, BIBD Bank Islam Brunei Darussalam, Cyber Security Brunei & Information Technology Protective Security Services (ITPSS) and AITI for hosting the students and Brunei Cybersecurity Association (BCSA) for coordinating the trip.







# 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](mailto: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!





## Ladies in Cybersecurity

### SEA CC Webinar – Ladies in Cyber on 7 September

On 7 September, the third webinar leading up to the SEACC forum was held with our speakers sharing on ladies in Cyber. Thank you, AISP Vice President & Founder for Ladies in Cyber Charter Sherin Lee, Ladies in Cyber Co-Lead Jackie Low, Deputy of WTC Malaysia Board Of Technologists, Ts. Ellis Yap, MBOT Professional Technologist, Ts. Amirah, WiSAP Chairman & President, Mel Migriño and Cpt. Mariel Mascariña-Ibañez for sharing insights for the attendees.



# 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](mailto:secretariat@aisp.sg)



## AiSP IoT Security Sharing at NTU 2023 on 3 November

Organised by	Supporting Partners	Supporting Agency	Sponsors

# 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

## UPDATES TO THE CYBERSECURITY LABELLING SCHEME



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

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.

Organised by



Speaker

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



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

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.

Organised by



Speaker



## 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



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



Speaker



## FIRMWARE SECURITY IN THE IOT LANDSCAPE: RISKS AND RESILIENCE



Alex Bazhaniuk  
CTO & Co-founder  
Eclysium

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.

Organised by



Speaker

## NEXT GEN BUILDING MANAGEMENT SYSTEM - IOT CYBERSECURITY, A CRUCIAL FACTOR



Jonathan Chin  
Business Development Director  
Fortinet

IOT and IIOT systems are highly leveraged in today's next gen cybersecurity. These systems, while they provide immense value in optimising resources and achievement business objectives, open a new avenue of cybersecurity risks to the organisation. This Webinar seeks to expose the risks, and explore strategies to secure Next Gen Building management systems in an automated, integrated and simplified fashion.

Organised by



Speaker

Click [here](#) to register.

# Cybersecurity Awareness & Advisory Programme (CAAP)

## SME Cybersecurity Conference 2023



Organised by the Association of Information Security Professionals (AiSP), SME Cybersecurity 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”.

Objectives of the conference include:

1. The importance of Cybersecurity for business growth and Innovation
- What are the trends that are forcing customers to look for new ways to work and drive businesses
  - How are businesses using technology to guide enterprises to securely
2. The latest cybersecurity trends and tools available to protect your business from cyberattacks
  - What is the software that you can introduce into the organization
    - Areas to look out for
3. Cybersecurity best practices for SMEs and staff
  - Awareness
4. Getting support from the government to sustain Growth Enterprise Innovation Scheme

- Areas to get help from the government in supporting developing innovative solutions, where Security can be built in rather than bolted later
  5. The future of Cybersecurity
    - GenAI's Impact on Security

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.

Email us at [secretariat@aisp.sg](mailto:secretariat@aisp.sg) to find out more on the sponsorship package.

## The Cybersecurity Awards



**Thank you for all your nominations**

**TCA 2023 Call for Nominations has ended on 14 May. TCA 2023 will be held on 13 October.**

### 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)

All sponsorship packages are taken up. Thank you for the support.

### TCA2023 Sponsors & Partners



Organised by



Supported by



Supporting Associations



Platinum Sponsors



Gold Sponsors



Silver Sponsors



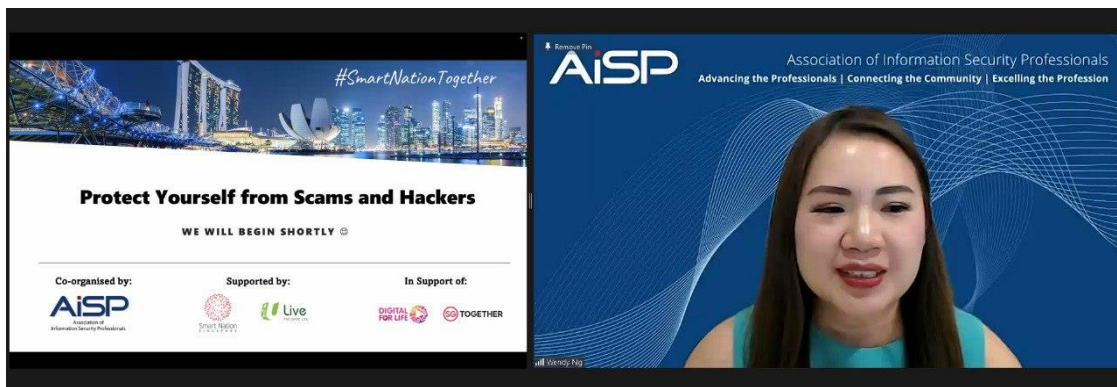
## Digital for Life

### Protect Yourself from Scams and Hackers Webinar on 20 September

AiSP & Smart Nation Office organised a lunch webinar with more than 300 attendees as part of Digital for Life Movement on 20 September.

Are you tired of hearing about scams in the news? Want to find out more about the different forms of scams and how they work? Discover the latest scam tactics and arm yourself with practical tips and strategies for staying scam-free.

Thank you AiSP EXCO Member, Wendy Ng & Smart Nation and Digital Government Office!





## **AiSP x PA x Huawei - Scam Awareness and Dialogue Session on 26 September**

As part of Digital for Life Movement, AiSP x Huawei Singapore x People's Association Emergency Preparedness Division organised the Scam Awareness and Dialogue Session on the theme of "Elevating Cybercrime Awareness" with Ms Sun Xueling, Minister of State in the Ministry of Home Affairs and the Ministry of Social and Family Development on 26 September. This session aims to enhance the capabilities of the Leaders in identifying threats in the online space.

We would like to thank our AiSP EXCO Co-Lead for Cyberwellness, Mr Dennis Chan for the sharing on the collaborative effort to maintain Cybersafe with the audience and Ms Aileen Yap from Singapore Police Force Anti-Scam Team who shared on the Common Scam Typologies, APPACT. Thank you to Huawei Singapore for hosting us and our AiSP President Mr Johnny Kho for moderating the dialogue session.

Together we can all ACT against scams by:

"Add" security features such as the ScamShield app and anti-virus/malware on your devices;

"Check" for scam signs and verify with official sources; and

"Tell" authorities, family and friends about scams.

Everyone of us have a part to play to ACT against scams.

Shoutout:

Interested to be part of the Celebrate Digital Events or sharing with elderly on the scam awareness, cyber hygiene tips or digital tips? Able to host a group of 40 to 50 Youths or Elderly in your office for a learning journey or some digital activities in your premises, contact the AiSP Secretariat to see how you can play a part in it. Together we will create a safe cyberspace supported by a strong and vibrant ecosystem for all Singaporeans.



# Regionalisation

## Brunei Cybersecurity Conference 2023 on 14 September

AiSP and Brunei Cybersecurity Association (BCSA) organized the inaugural Brunei Cybersecurity Conference 2023 graced with the presence of Singapore High Commissioner-designate Mr Laurence Bay and Pengiran Dato Seri Setia Shamhary bin Pengiran Dato Paduka Haji Mustapha Minister of Transport and Infocommunications. Thank you Brunei Cyber Security Association for coordinating. Our student, Rayden Leau also won the first prize for the competition.

Thank you our Corporate Partners, Huawei, Fortinet and Votiro and AiSP President, Mr Johnny Kho for sharing insights during the event. After the conference, there was an appreciation dinner for the guests to unwind and network with each other.







[back to top](#)





### Czechia – Singapore CyberSecurity Online Meetup on 19 September

In collaboration with Embassy of the Czech Republic in Singapore, CzechTrade and CzechInvest Singapore, AiSP bring together specialists from various fields of cyber security to share their knowledge of countering the ever-rising threat of cyber-attacks on 19 September. Thank you Johnny Kho, AiSP President and Richard Kadlčák, Special Envoy for Cyber Space, Ministry of Foreign Affairs of the Czech Republic for giving the opening remarks. Thank you David Čermák, CEO, Blindspot, Tesvin Choon, Senior Business Development Manager, Cloud, Fortinet Singapore, Dr. Ondřej Ryšavý, Associate Professor, Faculty of Information Technology, Brno University of Technology & Dr. Yang Liu, Professor, Nanyang Technological University Singapore for sharing insights with our attendees.

**Blindspot**

**The DDoS Challenge: Major Impact on Modern Businesses**

- DDoS attacks are not the issue for all
- Are your online assets critical for daily operations?
- DDoS attack motivations know no bounds

High-risk customer segments	Customer exposure and protection
<ul style="list-style-type: none"> <li>Telecommunications</li> <li>Financial Services</li> <li>Media &amp; Entertainment</li> <li>Critical Infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>Gaming</li> <li>Betting</li> <li>E-Commerce</li> <li>Education</li> </ul>
	<ul style="list-style-type: none"> <li>Protected or falsely deemed protected</li> <li>Unprotected, high risk</li> <li>Unprotected, low risk</li> </ul>

**Securing people, devices, and data everywhere.**

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our security solutions are among the most deployed, most patented, and most validated in the industry.

Global Customer Base <b>680,000+</b> Customers	2022 Revenue <b>\$5.59B+</b> (as of Dec 31, 2022)	Market Capitalization <b>\$59.38B</b> (as of June 30, 2023)
Broad, Integrated Portfolio of <b>50+</b> Enterprise Cybersecurity Products	Strong Analyst Validation <b>41</b> Enterprise Analyst Report Inclusions	Vertical Integration <b>\$1B+</b> Investment in ASIC Design & Development



## SEACC Forum on 16 October



In an increasingly interconnected world, the digital landscape is more dynamic than ever before. As Southeast Asia continues to thrive in the digital age, ensuring a safe and secure cyberspace is of paramount importance. With the rise of cyber threats and vulnerabilities, the need for collaboration, knowledge sharing, and innovative solutions is greater than ever.

Join us for a pivotal forum where South East Asia Cybersecurity Consortium converge to address the pressing issues surrounding the safety of our digital ecosystem. This gathering serves as a catalyst for comprehensive dialogue, fostering cooperation, and forging a path toward a safer cyberspace for our region.

Register [here](#)

# Corporate Partner Events

## Securing Critical Infrastructure in an AI-Powered Era on 21 September

Thank you to Christopher Anthony from Cyber Security Agency of Singapore (CSA), Nathaniel Callens from Grab and Leon Tan from BeyondTrust for the sharing in our AiSP Event on Securing Critical Infrastructure in an AI-Powered Era on 21 September. The audience have a great time in the discussion and sharing.





# AiSP x JTC Networking Event

Our AiSP x JTC PDD event has concluded on 8 September with our speakers and panellists. Big thanks to Member of Parliament for Pasir Ris- Punggol GRC Ms Yeo Wan Ling, Director of JTC Ms Yap Eai-sy, AiSP President Mr Johnny Kho and AiSP Immediate Past President and Director of SIT, Prof Steven Wong for sharing insights with the attendees! Attendees also had the exclusive first peek into how the Punggol Digital District would look like. Counting down to 1 year to PDD TOP!



# Upcoming Activities/Events

## Ongoing Activities

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

## Upcoming Events

Date	Event	Organiser
1 Oct	Learn Digital Carnival @ Bukit Panjang	Partner
2 Oct	Cyber Trade Delegation to Singapore	Partner
5 – 6 Oct	Japan IC-AJCC	Partner
7 Oct	I'm Digital Ready@South West	Partner
10 Oct	<a href="#">LJ to Acronis for RP</a>	AiSP & Partner
11-12 Oct	Cloud Expo 2023	Partner
13 Oct	<b>TCA 2023 Gala Dinner</b>	AiSP
16 Oct	<b>SEA CC Forum</b>	AiSP
17 – 19 Oct	SICW/Govware	Partner
17 – 19 Oct	AISA's Australian Cyber conference Melbourne	Partner
24 Oct	Sailpoint Navigate Singapore 2023	Partner
24 Oct	Sailpoint Women in Security Lunch	Partner
25 Oct	Awareness Webinar for EY	Partner
25 Oct	<a href="#">Knowledge Series - DevSecOps</a>	AiSP & Partner
26 Oct	Event with Votiro	AiSP & Partner
28 – 29 Oct	DFL Festival – Kampung Admiralty	Partner
3 Nov	<b>IoT Security Sharing at NTU 2023</b>	AiSP & Partner
4 – 5 Nov	DFL Festival – Bedok	Partner
10 Nov	<b>SVRP 2023 Awards Ceremony</b>	AiSP & Partner
11 – 12 Nov	DFL Festival - TPY	Partner
15 – 17 Nov	Singapore FinTech Festival	Partner
18 Nov	Sharing at Kallang CC	Partner
21 - 22 Nov	CISO Auckland	Partner
22 Nov	<a href="#">Knowledge Series - CTI</a>	AiSP & Partner
27 Nov	<b>SME Cybersecurity Conference</b>	AiSP
29 Nov	CISO Indonesia	Partner
29 – 30 Nov	CDIC 2023	Partner

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

# CONTRIBUTED CONTENTS

## Article from CTI SIG

### A Threat Intelligence Analyst's Diaries

#### Introduction

Cyber Threat Intelligence (CTI) is not a new term and has been around for at least two decades according to the Forum of Incident Response and Security Teams (FIRST).<sup>1</sup> However, in recent years the term has evolved significantly into a discipline. The reason behind this advancement can be attributed to the "Red Queen effect," a coevolutionary hypothesis proposing that species must constantly adapt and evolve to survive against ever-evolving opposing species. Relating this hypothesis to cybersecurity, attackers and defenders are perpetually in a game of cat-and-mouse. In this game of "one-upmanship," attackers devise novel tactics and techniques to bypass protections, prompting network defenders to implement stronger defensive measures, processes, and tools. As such, organizations have begun to establish new roles focused on CTI as part of their overall cybersecurity strategy.

In this article, I'll share two key frameworks that are the "meat and potatoes" of CTI analysis and how they can be applied to a recent incident.

#### Cyber Kill Chain

Originally a military concept, the kill chain identifies the structure of an attack from the identification to the destruction of a target. It was later adapted by defense contractor Lockheed Martin to model computer network intrusions.<sup>2</sup> The cyber kill chain follows these sequential phases:

- 1. Reconnaissance** - The attacker first identifies their target, researches, and gathers information such as login credentials, network and operating system details, organization structure, etc.
- 2. Weaponization** - Based on the intelligence gathered from previous phase, the attacker creates an attack vector to exploit known vulnerabilities on the target.
- 3. Delivery** - The attacker then launches the attack typically via email or malicious website. In some cases, the attack might take place physically in the form of USB drives; for example, a USB Rubber Ducky.
- 4. Exploitation** - The attacker attempts to exploit vulnerabilities on the target's system.
- 5. Installation** - Malware or other malicious payloads are installed on the target's network or system.

<sup>1</sup> <https://www.first.org/global/sigs/cti/curriculum/cti-introduction>

<sup>2</sup> [https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining\\_the\\_Advantage\\_Cyber\\_Kill\\_Chain.pdf](https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf)



6. **Command and Control** - To maintain persistence access to the target network, the attacker deploys a remote access tool like Cobalt Strike to connect remotely to the attacker-controlled infrastructure.
7. **Actions on Objective** - Finally, the attacker carries out their intended goal such as data exfiltration, destruction, or encryption.

### Pyramid of Pain

The Pyramid of Pain is a conceptual model created by David J. Bianco to illustrate the relationship between the type of indicators used to detect an adversary's activities and the amount of pain inflicted on the adversary when it's denied. The figure on the right shows the type of indicators organized within the pyramid according to their value and their level of detection and response. The pyramid's exterior corresponds an indicator type with the amount of pain dealt to an adversary. At the base, hash values such as MD5, SHA1, and SHA256 are color-coded in blue representing the most accurate indicator type but causing a trivial amount of pain to an adversary. That's because the adversary can effortlessly change the hash value of a malicious file just by changing a single bit. As defenders advance upward the pyramid, the color changes to green, yellow, and ultimately red, depicting the level of difficulty in terms of detection and response. Situated at the pyramid's apex are an adversary's tactics, techniques, and procedures (TTPs) -- in other words, an adversary's behavior or modus operandi. When defenders can detect and respond at this level, adversaries are compelled to adapt their operations entirely. This can be challenging because old habits are more difficult to change. I'd recommend reading David J. Bianco's blog post that has greater details on the different levels of the Pyramid of Pain.<sup>3</sup>

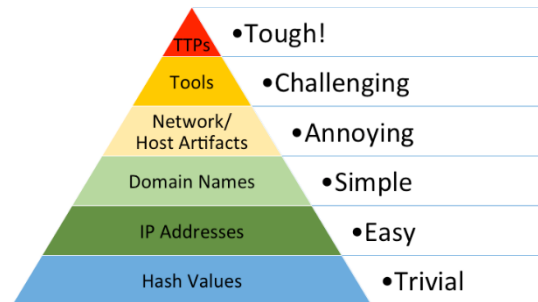


Figure 1: David J. Bianco's Pyramid of Pain

### Case Study of the 3CX and TT Cascading Supply Chain Attack

On March 29, 2023, cybersecurity vendors CrowdStrike and SentinelOne reported an active supply chain attack hitting organizations using 3CXDesktopApp, a softphone application from video conferencing firm 3CX.<sup>4,5</sup> Three weeks later, 3CX released an update detailing findings from Mandiant's investigation.<sup>6</sup> Mandiant identified the initial compromise began in 2022 when a 3CX employee installed the Trading Technologies X\_TRADER software on their personal computer. The trojanized software led to the deployment of VEILED SIGNAL malware that enabled the suspected North Korean threat

<sup>3</sup> <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

<sup>4</sup> <https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/>








<sup>5</sup> <https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/>

<sup>6</sup> <https://www.3cx.com/blog/news/mandiant-security-update2/>

actor (UNC4736) to initially compromise and maintain persistence on the employee's personal computer.<sup>7</sup>

With reference to Mandiant's report, I applied the two aforementioned frameworks in this case study as follows:

### Cyber Kill Chain

-  **Reconnaissance** - Considering the attack path, it appears that UNC4736 has initially identified Trading Technologies as their target.
-  **Weaponization** - In November 2021, UNC4736 used a legitimate digital certificate to sign a trojanized version of X\_TRADER.
-  **Delivery** - Prior to August 2022, the 3CX employee downloaded the trojanized software to their personal computer.
-  **Exploitation** - UNC4736 was able to gain elevated access to the 3CX employee's personal computer and subsequently harvested their 3CX work credentials.
-  **Installation** - The installation of trojanized X\_TRADER software led to the deployment of VEILED SIGNAL backdoor.
-  **Command and Control** - VEILED SIGNAL contains a C2 (command and control) module used to beacon to UNC4736's controlled infrastructure.
-  **Actions on Objective** - Due to ongoing investigations, it remains unknown what the intended goals of UNC4736 are.

### Pyramid of Pain

A complete list of indicators of compromise (IOCs) can be found on Mandiant's blog.<sup>8</sup>

- **TTPs** - Refer to the Technical Annex in Mandiant's blog
- **Tools** - Fast Reverse Proxy (frp) used for lateral movement
- **Network/Host Artifacts** - VEILED SIGNAL backdoor
- **Domain Names** - www[.]tradingtechnologies[.]com
- **IP Addresses** - 52[.]11[.]242[.]46 (Note the IP in question might not necessarily be malicious as it could resolve to other domains)
- **Hash Values** - MD5: ef4ab22e565684424b4142b1294f1f4d (X\_TRADER\_r7.17.90p608.exe)

<sup>7</sup> <https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise>

<sup>8</sup> <https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise>

## Biography



### **Jeremy Ang**

Jeremy is an information security professional with a decade of experience in the financial services, pharmaceutical and MSSP industries. He has a bachelor's degree in computer science and holds various industry certifications including CISSP, GCFA, GREM, GDAT, GCTI, GMON, and GCIH. Jeremy is a member of AiSP Cyber Threat Intelligence (CTI) Special Interest Group (SIG) and currently a Senior Threat Intelligence Analyst with Intercontinental Exchange, Inc., a Fortune 500 company that designs, builds and operates digital networks to connect people to opportunity.

Any views and opinions expressed in this article are solely those of the author and do not necessarily reflect the views and opinions of the author's employer.



# Article from Corporate Partner, Opentext

## How AI Can Be Used as a Business Advantage

By Matt Aldridge, Principal Solutions Consultant, OpenText Cybersecurity

Artificial intelligence has long dominated conversations in business and consumer technology, as well as in mainstream media, but the trend saw a major uptick with the release of Open AI's ChatGPT. As AI is becoming much more accessible, easier to use, and more refined, it is quickly being integrated into everyday life, bringing with it almost as many serious risks as it has advantages. Indeed, AI is a double-edged sword from many points of view, and cybersecurity is no exception.

### **AI: The good, the bad, and the ugly**

The bright side is that AI capabilities are helping security professionals expedite multiple workstreams, such as threat detection and security event processing. As a result, they are enhancing efficiency and liberating some of these professionals' time so they can dedicate their efforts to more labour-intensive aspects of their role, which require creative, critical, human thinking.

However, the increasing requirement for AI in a cyber professional's skillset is putting more pressure on both organisations and individuals, while greatly widening the already substantial cyber skills gap. In other words, AI is exposing the unrealistic expectations many businesses have. Recruiters often ask that candidates be familiar with standard sets of cybersecurity tools, but also know the latest threat landscape inside and out. On top of that, they are sometimes requiring several years of experience working with ChatGPT – even though the tool has only been around since November of last year!

We must also remember that the same AI tools that security professionals use are also readily available for bad actors. Always on the lookout for more evasive, more resilient tactics, cybercriminals rely on AI to elude detection and escape security systems. The use of generative AI for phishing purposes is an important, and alarming, example. Using AI, cybercriminals can more easily map and exploit the vulnerabilities of an organisation's infrastructure, and gain access to sensitive data or otherwise endanger the business. This is an endless game of cat and mouse which is set to get even rougher as time goes on, and as AI develops further.

### **You must fight AI with AI**

We have now seen that AI is changing the cyber landscape in many different and radical ways. It is also developing much faster than any other tech trend. ChatGPT took only an amazing five days to reach the landmark of one million users. By way of comparison, Facebook needed ten months, and Twitter two years, to achieve the same feat.

The only way to keep up with the speed at which this particular technology bandwagon is moving is to jump on it. You simply cannot throw anything else at the problem but AI itself. There are now increasingly sophisticated threats, powered by AI, which are getting

[back to top](#)

extremely difficult to filter out without it. The level of critical thinking and complex decision-making behind these evolving tactics is getting higher and higher. Organisations which aren't prepared to fight fire with fire are going to be increasingly vulnerable to a wide range of attacks.

### The bottom line

As it represents both significant development opportunities as well as risk factors, AI simply cannot be ignored. If businesses want to thrive, or even just survive, in the current technological climate, they need to be able to adapt AI in a way that is as speedy as it is comprehensive.

Some fears regarding AI, while understandable, are often ungrounded. It is highly unlikely that such a technology could ever fully replace humans, especially considering their generative and predictive nature, which still requires substantial human input. However, the way this technology is growing, it is far more likely to pose the threat of rendering non-AI-savvy businesses obsolete.

Humans will always have a place in the cyber sector, and they will not be completely replaced by AI. However, they might be replaced by people who can handle AI better. This is a game of the best AI and the most knowledgeable AI experts, and the sooner your business understands that, the better.

OpenText is one of the largest security solution providers in the industry. We help CISOs and their teams gain visibility across complex IT environments, quickly detect and prevent threats, respond quickly to internal and external threats to understand scope and impact, and comply with information security, regulatory and industry standards. Our solutions help organizations:

- **Reduce risk** with multi-vector protection against attack surfaces
- **Minimize business disruption** with ability to recover data within minutes
- **Investigate and analyze** threats to understand scope and impact
- **Gain rapid insights** leveraging real-time contextual threat intelligence



At the same time, we help them optimize resources and skillset shortages while addressing new and emerging threat vectors with high efficacy. Unlike other security providers, we provide the breadth and depth of comprehensive end-to-end security solutions – including brand names we’ve acquired such as Webroot, Carbonite and EnCase -- to address each step of an organization’s journey to enhance security and trust.

Of course, as the threat landscape continues to spiral, organizations must **strengthen their cyber resilience**. That means taking a three-pronged approach: first protecting against advanced threats to lower the overall risk of attack, then detecting threat actors in order to quickly eliminate their access to systems and data, and finally recovering from attacks and getting back to business as usual.

### About OpenText Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

Visit [OpenText Cybersecurity Cloud solutions](#) for more information.



**opentext™**

At OpenText, we believe future business growth is human centric, inclusive and sustainable. Bringing information and automation together, the OpenText Cloud solves complexities so businesses can re-invent through new digital fabrics, new rules and new ways to work. We elevate every person and every organization to be their best, so you can work smarter.

**SMARTER with OpenText**

**BUILD, AUTOMATE, CONNECT**      **SECURE, PREDICT, ACT**

Application Delivery & Quality      Cybersecurity

Application Modernization      Analytics & AI

Business Network      Content Management

IT Operations Management      Experience Management

**OpenText Quick Facts**

<b>25,000</b> EMPLOYEES	<b>125,000</b> ENTERPRISE CUSTOMERS	<b>180</b> COUNTRIES
<b>98</b> OF TOP 100 GLOBAL INDUSTRY LEADERS TRUST OPENTEXT	<b>11 MILLION</b> PUBLIC CLOUD USERS	<b>3,000</b> PRIVATE CLOUD DEPLOYMENT

For any enquiries, please contact Chua Ying Tze at [ychoa@opentext.com](mailto:ychoa@opentext.com)

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

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

# PROFESSIONAL DEVELOPMENT

## Listing of Courses by Wissen International



### EC-Council's Blockchain Certifications Overview

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

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](mailto:aisp@wissen-intl.com) for details!**

## Listing of Courses by ALC Council



### Stand out from the crowd

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

We offer the most in-demand cyber certifications including:

- CISM®, CRISC®, CISA®, CGEIT®, CDPSE®
- SABSA®, NIST®, ISO 27001
- CISSP®, CCSP®
- 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](mailto: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](mailto: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](mailto:learn@alctraining.com.sg) | [www.alctraining.com.sg](http://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 31 OCTOBER 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)**.

The banner features the AiSP logo at the top right. The main text reads "Limited Time Promotion for QISP Exam and BOK Book!" with a sub-headline "While stocks last! till 30 September 2023". Below this is a QR code with "PAY NOW" text. To the left of the QR code is an image of the book cover for "IS-BOK 2.0 INFORMATION SECURITY BODY OF KNOWLEDGE", published by AiSP, with editors Alex Lim Wee Meng, Prof Steven Wong Kai Juan, and Samson Yeow. At the bottom, the price is listed as "\$216 inclusive of GST" and "U.P \$486 before GST".

**AiSP**  
Advance Connect Excel

## Limited Time Promotion for QISP Exam and BOK Book!

While stocks last! till 30 September 2023

**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

Scan the QR code  
here to make the  
payment

**\$216 inclusive of GST**  
U.P \$486 before GST

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](mailto: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 **31 October 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](http://www.wissen-intl.com/qisp)



# 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](mailto:secretariat@aisp.sg)

For any enquiries, please contact [secretariat@aisp.sg](mailto:secretariat@aisp.sg)

## AVIP Membership

AiSP Validated Information Security Professionals (**AVIP**) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development, and career progression for our professionals.

## Membership Renewal

Individual membership expires on 31 December each year. Members can renew and pay directly with one of the options listed [here](#). We have GIRO (auto - deduction) option for annual auto-renewal. Please email [secretariat@aisp.sg](mailto: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](http://www.aisp.sg/membership.html)

## AiSP Corporate Partners



Acronis









Visit [https://www.aisp.sg/corporate\\_members.html](https://www.aisp.sg/corporate_members.html) to know more about what our Corporate Partners (CPP) can offer for the Cybersecurity Ecosystem.

## AiSP Academic Partners



## Our Story...

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

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

### Our Vision

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

### Our Mission

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

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

## AiSP Secretariat Team



Vincent Toh  
Associate Director



Elle Ng  
Senior Executive



Karen Ong  
Executive



[www.AiSP.sg](http://www.AiSP.sg)



[secretariat@aisp.sg](mailto: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.