

## 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: Distilling & Democratising External Cyber Threat Intelligence
- Bugcrowd's New Inside the Mind of a Hacker Report
- Article from Singapore Polytechnic
- SVRP 2022 Winner: Darren Ong

## Professional Development

## Membership

# NEWS & UPDATE

## New Partners

AiSP would like to welcome Clixer, CrowdStrike and Horangi Cyber Security as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

### New Corporate Partners



**HORANGI**  
CYBER SECURITY

## Continued Collaboration

AiSP would like to thank AZ AP, Onesecure, Scantist and Vectra AI for their continued support in developing the cybersecurity landscape:



## News & Updates

### GovWare Focus on 18 July

Leading to GovWare SG 2023, Image Engine organised the GovWare Focus on 18 July 23. Our AiSP President, Mr Johnny Kho was the moderator for the Panel on “A Zero-Trust Pitstop” i.e., an Evaluation of what Zero-Trust & XDR means today in the current landscape – is it still just a product pitch?”. It was a fruitful session as the speakers and audience shared insights and key takeaways on Zero-Trust.



### People's Association Community Spirit Merit Award on 25 July

AISP was awarded the prestigious People's Association (PA) Community Spirit Merit Award on 25 July 2023 to mark the recognition of AISP contribution to the community. This award is presented to organizations who have made significant contributions in driving sustainable projects and collaborations with People's Association. This recognition reflects the collective efforts of AiSP, corporate partners and supporting organizations such as the People's Association - Emergency Preparedness Division demonstrating unwavering commitment to creating a safer cyber landscape for everyone. Since the launch of AiSP Cyber Wellness Programme on 1 November 2021, AiSP has reached out to more than 15,000 people in the community. This is the first time AiSP was recognized for the continuous efforts and contributions in promoting good cyber hygiene habits and digital wellness to the masses. The award was presented to AiSP President, Johnny Kho by Deputy Chairman of PA, Mr Edwin Tong, Minister for Culture, Community & Youth and Second Minister for Law.

Upon receiving the award, Mr Johnny Kho, AiSP President expressed his heartfelt appreciation and dedication to the cause, stating, "We are truly humbled and honored

[back to top](#)

to receive the People's Association Community Spirit Award. This recognition reflects the collective efforts of our team, corporate partners and supporting organizations demonstrating unwavering commitment to creating a safer cyber landscape for everyone. We will continue to contribute and emphasize on the crucial importance of promoting cyber wellness and digital responsibility in our current society."

We would also like to extend our heartfelt gratitude to our esteemed DFL (Digital for Life) partners, whose unwavering support and collaboration have been instrumental in the success of the AiSP Cyber Wellness Program. Trend Micro, Huawei, Contifinity, Grab, Acronis, RSM Singapore, and Cisco have played pivotal roles in driving positive change within the digital space and empowering our community with the necessary tools to navigate the digital landscape safely. Thank you Temasek Polytechnic, Republic Polytechnic, Ngee Ann Polytechnic, Nanyang Polytechnic, Singapore Polytechnic and Institute of Technical Education, Singapore for providing student volunteers to help out at the events.

Furthermore, we extend our heartfelt appreciation to the individuals who played an important role in executing the AiSP Cyber Wellness Program. Ms Faith Chng, Ms Soffenny Yap, Mr Dennis Chan, Ms Sherin Y Lee, Ms Catherine Lee, Mr Tony Low, Mr Johnny Kho, Ms Wendy Ng, Mr Hoi Wai Khin, Ms Andrea Chea, Mr Breyvan Tan, Ms Judy Saw, Mr Beckham Lee and Mr Kenrick Yeo among others, have displayed exceptional dedication, passion, and hard work in sacrificing their weekends to share their insights with the community. It is through the collective efforts of such individuals that help AiSP to bring the programme to fruition.



## ITE West Security Summit on 28 July

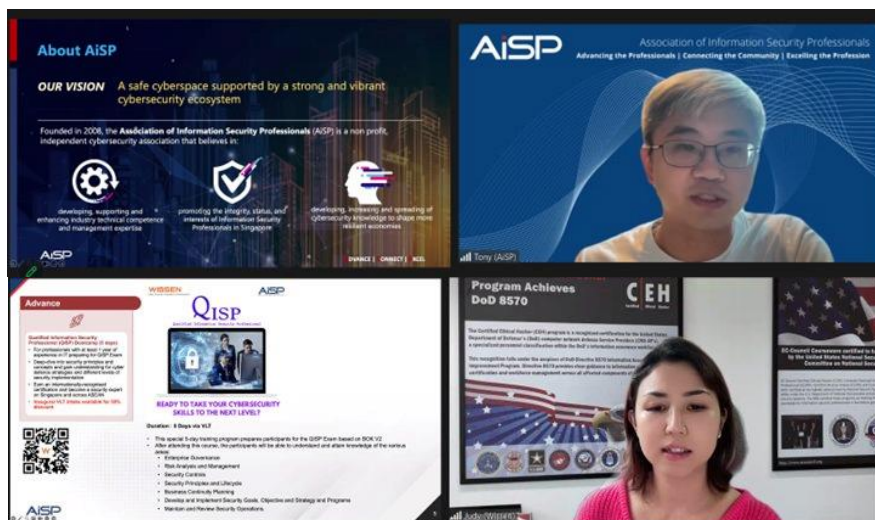
AiSP was invited by our Academic Partner, ITE West to set up a booth at the ITE Security Summit on 28 July to share with the students on our initiatives. AiSP Vice President Andre Shori and AiSP EXCO Member Alina Tan also did a sharing at the summit as well. Thank you ITE West for inviting us!



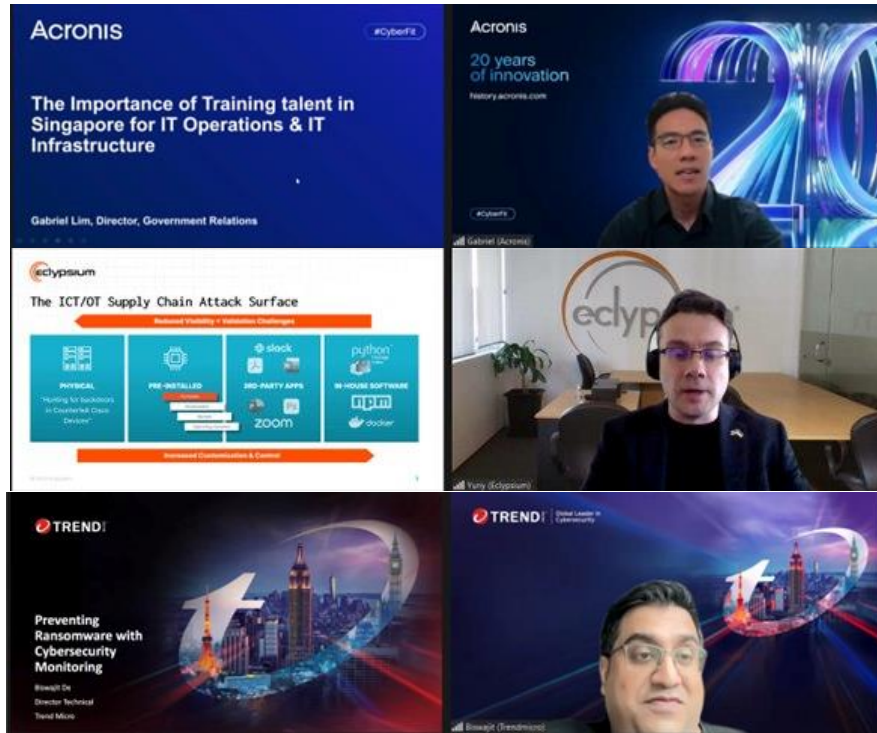
# Knowledge Series Events

## Operations & Infrastructure Security on 19 July

As part of Digital for Life Movement, AiSP organised the Knowledge Series today focusing on Operations & Infrastructure Security. Thank you to our Corporate Partners Acronis, Eclysium and Trend Micro for sharing insights with our attendees. Thank you AiSP Vice-President, Mr Tony Low for giving the opening address and Our Corporate Partner, Wissen for sharing on the cybersecurity courses.



[back to top](#)



## Upcoming Knowledge Series

IoT on 30 August



**AiSP Knowledge Series – Internet of Things**

**AiSP Knowledge Series**  
**Internet of Things**  
30 Aug 23 | 3PM - 5PM | Zoom



**Dave Gurbani**  
CEO  
Cybersafe



**Mike Henry**  
Chief Technology Officer  
CYFIRMA



**Raymond Ma**  
Regional Director, SSH  
APAC  
DTAsia



Organised by **AiSP** In support of **DIGITAL FOR LIFE**  
PLAY IT FORWARD

Supported by



[back to top](#)

In this Knowledge Series, we are excited to have Cybersafe, CYFIRMA and DTAsia to share with us insights on Internet of Things. 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.

### **IoT In Cybersecurity - Risk and Reward**

Speaker: Dave Gurbani, CEO, Cybersafe

In this presentation, Dave will be sharing insights into the risks and rewards associated with utilizing IoT in the context of cybersecurity. He will discuss common IoT devices found in business environments and shed light on how they can serve as vectors of attack. Dave will emphasize the importance of implementing robust security measures to protect organizations from potential vulnerabilities. Moreover, he will explore how strategic deployment of IoT technologies can effectively safeguard businesses when used correctly. Attendees can expect to gain practical knowledge and strategies for ensuring a secure and resilient business ecosystem amidst the evolving landscape of IoT.

### **How to Assess the Threat Landscape and Make Intelligence-Led Decisions in a Hyperconnected World**

Speaker: Mike Henry, CTO, CYFIRMA

A wise man once said: knowing your enemy and knowing yourself is key to winning a thousand battles. The same applies to war on the wire where the adversary operates in the dark and defenders need to adapt strategies in real-time to counter attacks. In this session, Mike will share the methods to gain visibility of the fast-evolving threat landscape, map out attackers' motives, uncover their attack techniques, and build an agile approach to managing cybersecurity.

### **Enhancing security by using Zero Trust approach for OT access**

Speaker: Raymond Ma, Regional Director, SSH APAC, DTAsia

The Zero Trust philosophy is continuing to gain momentum across the globe with various industries adopting and regulators imposing the best practices of using passwordless, just-in-time access. However, Zero Trust access has thus far been seldom mentioned or applied to OT/IoT access, despite the fact that the technology can enhance security for another layer. Therefore, Zero Trust access for OT/IoT will be introduced and explored.

Date: 30 Aug 2023, Wednesday


Time: 3PM – 5PM

Venue: Zoom

Registration:

[https://us06web.zoom.us/webinar/register/4716868205413/WN\\_3q7zvOj2SSaD2pTutmiVsQ](https://us06web.zoom.us/webinar/register/4716868205413/WN_3q7zvOj2SSaD2pTutmiVsQ)

## Red Team on 20 September




**AiSP**  
Advance Connect Excel

**AiSP Knowledge Series – Red Team**


# AISP KNOWLEDGE SERIES

## RED TEAM


20 Sep 2023 | 3PM - 5PM | Zoom




Sajeeb Lohani  
Global Head (Director)  
of Cybersecurity  
Bugcrowd





Sunny Neo  
Senior Red Team  
Consultant  
Mandiant, Google Cloud





Stefano Maccaglia  
Incident Response  
Manager  
NetWitness



Organised by  In support of 

Supported by


In this Knowledge Series, we are excited to have Bugcrowd, Mandiant & NetWitness to share with us insights on Red Team. 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.

**New Research: Inside the Mind of a Hacker**  
Speaker: Sajeeb Lohani, Global Head (Director) of Cybersecurity, Bugcrowd

For teams working to identify potential weaknesses within their organization's cyber defenses, technical skills aren't the only requirement. These teams must also put themselves in the shoes of both the adversary and the defender. What better way to do this than to step into the mind of a hacker?

Bugcrowd recently released the seventh edition of their flagship report, Inside the Mind of a Hacker. This report analyzes 1000 hacker responses to the most pressing cybersecurity questions. In this session, we'll cover some of the key takeaways from this report, including:

- Hacker demographics, trends, and motivations
- Ways hackers are leveraging generative AI
- How red, blue, and purple teams can use this information to strengthen their security posture

**Scaling Red Team Operations**

Speaker: Sunny Neo, Senior Red Team Consultant, Mandiant, Google Cloud

In recent years, there has been an uptrend of companies building internal red team to continuously test their organization's cybersecurity defense. However, red teaming is a laborious process that requires skilled technical testers to overcome evolving security controls and deliver fruitful results. Thus, scaling red team operations is a challenging issue exacerbated by shortage of skilled talents in the industry.

Based on publicly available information, this talk aims to explore how threat actor groups such as FIN7 and CONTI overcame the talent shortage, and how Mandiant is supporting ~160 proactive consultants globally to execute their operations effectively.

**Don't scratch that patch: how Microsoft helps to solve Red Team problems...**

Speaker: Stefano Maccaglia, Incident Response Manager, NetWitness

With "Patch Tuesday" Microsoft usually addresses various security vulnerabilities and issues by providing patches and updates for their software products. However, for malicious actors, Patch Tuesday can be a valuable resource for identifying new exploits.

In time, noticing this mechanism in the cybercriminal ecosystem, we adopted a similar approach to support our Red Team and our investigations.

In a nutshell, we industrialized a process where our Threat Intel team harvest exploits linked with the Patch Tuesday from the dark web, while our team reverse engineer the updates looking for code we could use during our Red team activities.

The result is an extended set of potential exploits we can reliably integrate with our arsenal when we carry out simulated attacks. This improves our test effectiveness and allows us to extend our options against our customers' defense mechanisms. By using the newly acquired knowledge about the vulnerabilities, the Red Team can test whether these systems can detect or prevent exploitation attempts.

In our session, we will present our process and some examples where our newly acquired knowledge and exploits allowed our team to better test our customers' cybersecurity posture.

Date: 20 Sep 2023, Wednesday

Time: 3PM – 5PM

Venue: Zoom

Registration:

[https://us06web.zoom.us/webinar/register/3316905308124/WN\\_UwDKTY9fSRCuQlo0dBDLWQ](https://us06web.zoom.us/webinar/register/3316905308124/WN_UwDKTY9fSRCuQlo0dBDLWQ)

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. Red Team, 20 Sep
2. DevSecOps, 25 Oct
3. 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)

## AiSP Youth Symposium on 2 July

As part of Youth Day Celebrations, AiSP organised the second Youth Symposium on 2 July, where over 120 participated attended the symposium together with our AiSP Patron, Senior Minister of State, Mr Tan Kiat How.

Thank you to AiSP Secretary & SVRP EXCO Lead, Ms Soffenny Yap, Mr Choon Bong Wong from Cyber Security Agency of Singapore (CSA) and Mr Sean Lim from EC-Council for sharing insights with our youths. Thank you to AiSP Vice President, Ms Sherin Y Lee for giving the welcome address.

Thank you to our moderator AiSP EXCO Member, Mr Pengfei Yu as well as our panellists, AiSP Secretary & SVRP EXCO Lead, Ms Soffenny Yap, Mr Sean Lim from EC-Council and AiSP Patron, Senior Minister of State, Mr Tan Kiat How for the insightful panel discussion.



## Learning Journey to Singtel on 5 July for Republic Polytechnic

As part of Digital for Life Movement, AiSP organised a learning journey to our Corporate Partner, Singtel for our Academic Partner Republic Polytechnic. Thank you our Corporate Partner, Wissen International(EC-Council ASEAN) for providing the refreshments for the students.



## Learning Journey to AiSP Corporate Companies for Primary School Students

In support of CSA Peer Support Leader Programme for primary school students, AiSP facilitated a series of exciting learning journey for students from different Primary schools to different CPP companies. Thank you ASUS, Grab and RSM Singapore for hosting our primary school students and sharing insights with them!



# 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

### **AiSP Ladies in Cyber Annual Socials on 31 August**

AiSP will be organising our AiSP Ladies in Cyber Annual Socials on 31 Aug 23 at Bar Bar Q as part of the International Cyber Women Day Celebrations held every year on 1 Sep. We would like to invite you and your female friends to join us in the event.

Objective : Networking, Inspiration and Career Development

Join us on 31 August 2023 for an empowering Ladies in Cyber Socials Event dedicated to supporting and celebrating women in the Cybersecurity & Tech industry. This event will feature a Tech and Tunes Networking session that provides an opportunity to connect with like-minded individuals, expand your professional network, and foster valuable connections. Engage in quick, dynamic conversations with professionals from various sectors of the Cyber & tech industry and make lasting connections. Don't miss out on this exciting opportunity to support the advancement of women in the field.

Date: 31 August 2023 (Thu)

Time: 6PM - 8.30PM

Venue: Bar Bar Q at 3 Temasek Boulevard #01-602

Suntec City Tower 4, Singapore 038983

Dress Code: Casual

# AiSP Ladies in Cyber Annual Socials on 31 Aug 23 (Thu)

Bar Bar Q located at 3 Temasek Boulevard #01-602  
Suntec City Tower 4, Singapore 038983

Sharing by Keynote Speakers on Career Development  
and Inspiration.

Join us for a night of networking with finger food & free flow of drinks. Bring a female friend along and join our AiSP Ladies in Cyber Team and hear what our AiSP President and our Vice President & Founder for Ladies in Cyber Charter on their upcoming plans and activities for 2023 & 2024.

JOINTLY ORGANISED BY:



**LADIES  
IN CYBER**

Scan the QR  
Code to  
register for  
the event.



You can sign up at <https://forms.office.com/r/c1rmAYwHGz> or scan the above QR Code. Registration will close 31 July 23.

[back to top](#)

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



**SEA CC Webinar – Ladies in Cyber**



Jackie Low  
AiSP



Ts. Nur Amirah Fatin bt Abdul Aziz  
MBOT



Cpt. Mariel Mascarinha-Isaacs  
WISAP

# SEA CC WEBINAR LADIES IN CYBER

THURSDAY | 7 SEPTEMBER 2023 | 3PM - 5PM (SGT)

- SEA CC WEBINAR - DATA & PRIVACY
- SEA CC WEBINAR - CLOUD SECURITY
- SEA CC LADIES IN CYBER WEBINAR
- SEA CC FORUM 2023



ORGANISED BY










The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2023. The third webinar will be focusing on Ladies in Cyber where speakers will be sharing on empowering women in the ASEAN's cybersecurity sector.

**Importance of Cyber Literacy and Resilience**  
 Speaker: Jackie Low, AiSP Ladies in Cyber Co-Lead & EXCO Member and CISO, Ensign InfoSecurity [Association of Information Security Professionals]

Digitalization Initiatives and their Impact on Digital Natives and Immigrants  
 Moving from Literacy to Focused Cybersecurity Career Options

**Redefining Risk: Women Powering Cyber Resilience for a Secure Tomorrow**  
 Speaker: Ts. Nur Amirah Fatin bt Abdul Aziz, MBOT Professional Technologist Ts. in Utilities and Energy sector [Malaysia Board of Technologists]

Empowering role of women in risk management, highlighting their ability to redefine and strengthen cyber resilience for a secure future. It emphasizes the transformative impact women have in managing risks and shaping the landscape of cybersecurity.

**Breaking Barriers: Cyber Battalion's Remarkable Journey Towards Gender Equality and Inclusion**

Speaker: Cpt. Mariel Mascariña-Ibañez, Company Commander, Incident Response and Active Defense Company, Cyber Battalion, ASR, PA [WiSAP (Women in Security Alliance Philippines)]

Cpt. Mariel will be discussing the brief history of Cyber Battalion, its mission, task organization and organizational employment. She will also be presenting the roles of the women personnel of Cyber Battalion in the Philippine Army and its impact.

Date: 7 September 2023, Thursday

Time: 3PM – 5PM (SGT)

Venue: Zoom

Registration:

[https://us06web.zoom.us/webinar/register/4716890000439/WN\\_8Saf3IVcQQSejIP1R\\_8FWA](https://us06web.zoom.us/webinar/register/4716890000439/WN_8Saf3IVcQQSejIP1R_8FWA)

## 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)





Cloud Security Summit on 17 August

# AiSP

## CLOUD SECURITY SUMMIT 2023

17 AUG 2023 | 9.30AM - 2PM  
SUNTEC CONVENTION CENTRE, SUMMIT 1

THEME:  
SIMPLIFYING CLOUD FOR A SAFER FUTURE

Supporting Partners

Organised by

Supporting Agencies

Gold Sponsors

Silver Sponsors

Bronze Sponsor

**Guest of Honour: AiSP Patron, Mr Tan Kiat How**  
Senior Minister of State, Ministry of Communications and Information & Ministry of National Development

---

## SECURE CLOUD FOR THE FUTURE

Explores the importance of secure cloud practices, addressing security challenges, key strategies and emerging trends to ensure data protection in a digitally connected world.

Organised by

Speaker

## SIMPLIFYING THE SECURE CLOUD ARCHITECTING APPROACH



**Bernard Tan**  
Director,  
Cyber Security Group,  
GovTech

Cloud is a powerful and key enabler for any business to accelerate their digitalisation efforts. Hence, it is important to not underestimate the importance of securing cloud implementation as there are many different security archetypes, each with their own unique security considerations.

This session will share some tips to simplify the decision making process by: identifying the challenges, finding the sweet spots for possible deployment mode(s), and leveraging security architecting principles to navigate through the implementation journey.

Organised by  
**AISP**  
Association of Information Security Professionals

Speaker  
**GOVTECH**  
Government Technology

---

## BREAKING THE CLOUD ILLUSION: DOCKER DILEMMAS AND OPEN-SOURCE OVERSIGHTS IN SUPPLY CHAIN SECURITY



**Sajeeb Lohani**  
Global Head (Director) of  
Cybersecurity  
Bugcrowd

Most organisations have started diving deep into areas of supply chain security, but have they looked at the impact such issues may have on their cloud environments? This talk shines a light on the security challenges cloud environments face, particularly in the use of Docker images and open-source software supply chains. Contrary to common belief, not all Docker images are safe to use, and we'll discuss practical DevSecOps strategies for protection, detection, and response in these scenarios.

We'll also examine the potential vulnerabilities within the software supply chain that could affect your DevSecOps processes & cloud security. To bring these risks to life, we'll delve into real-life scenarios, including handling rogue authors, to highlight their potential business impact.

Finally, we'll offer advice on communicating these risks effectively to your board. Join us as we debunk common misconceptions and guide you towards a more secure cloud-oriented future.

Organised by  
**AISP**  
Association of Information Security Professionals

Speaker  
**bugcrowd**

---

## SECURING CLOUD NATIVE APPLICATIONS : THE FINAL FRONTIER



**Jatin Sachdeva**  
Global Principal Security Architect  
Cisco

Applications are the center of any business and rapidly evolving from workloads to containers and microservices. As environments transition their applications to the cloud, some get re-hosted or re-platformed from on-prem to cloud and others get re-factored or re-architected to use more cloud native technologies. The hybrid nature of transitioning applications today requires us to re-think security. In this session, we will look at the problem space and bring together various controls in the Cisco arsenal, that help us secure the modern application pipelines, runtimes as well as the underlying cloud native technologies and cloud infrastructure.

Organised by  
**AISP**  
Association of Information Security Professionals

Speaker  
**CISCO**

## THINK IT, BUILD IT, SECURE IT. CLOUD SECURITY REIMAGINED.



Valerian Rossigneux  
Sales Engineering Director, Asia  
CrowdStrike

The architecture of cloud-native applications requires its own unique approach to security in terms of policies and contents. Beyond meeting the challenge of maintaining consistent security across their data center and the public cloud environment where their applications are deployed, IT must also contend with a lack of mature tools for securing containers, API vulnerabilities and other issues.

In this presentation, Val will showcase how CrowdStrike Cloud Security provides continuous posture management and breach protection for any cloud in the industry's only adversary focused Cloud Native Application Protection Platform (CNAPP) powered by holistic intelligence and end-to-end protection from the host to the cloud, delivering greater visibility, compliance and the industry's fastest threat detection and response to outsmart the adversary.



## LEARN HOW TO WORK PROTECTED IN TODAY'S DIGITAL AGE



Garrett D'Hara  
Senior Director, Solutions Engineering  
APAC  
Mimecast

Email and collaboration are where work happens - they're also where risk is concentrated. Mass consolidation on a handful of cloud platforms like Microsoft 365 and Google Workspace has created irresistible targets; malicious actors target them relentlessly, using the top attack vector - email - to deliver everything from phishing to ransomware. And, they count on employees to make mistakes. It's no surprise that 91% of cyberattacks start with email or that 94% of successful breaches involve some form of human error.

How has the security industry responded to these challenges? By creating a complex web of point products designed to address critical areas of risk. However, this approach has generated a level of complexity that's untenable. Put simply, IT and security teams are spending more time managing technology than risk.

This session will delve into the importance of working protected against cyber attacks at the intersection of people, communications, and data. Additionally, it will explore how leveraging API/Mesh integration can simplify your cyber security stack and enhance your overall cyber resilience.



## PANEL DISCUSSION



Tony Low  
Moderator  
AiSP Vice-President &  
Cloud Security SIG Lead



Mr Tan Kiat How  
AiSP Patron  
Senior Minister of State, Ministry  
of Communications and Information



Jon Lau  
CSCIS Cloud Security  
Chairman



Jonathan Kok  
Partner, Intellectual  
Property and Technology  
WITHERS KHATTARWONG



The AiSP Cloud Security Summit 2023 is an important event of the year, organised by the AiSP Cloud Security Special Interest Group. The programme schedule comprises of key notes, solutions, panel discussion and workshop. The theme for the summit is Simplifying Cloud for a Safer Future. This event is organized for anyone with an interest or wish to find out more or understand more on the landscape of Cloud Security.

Cloud computing has become an integral part of modern businesses and organizations. The cloud offers a wide range of benefits, including increased flexibility, scalability, and accessibility. However, many users still struggle to navigate the complex landscape of the cloud and face security concerns. This summit aims to simplify the cloud experience and make it safer for everyone. Experts in cloud computing will share their insights and best practices for utilizing the cloud in a straightforward manner while maintaining security.

This event is organized for anyone with an interest or wish to find out more or understand more on the how to simplify and secure their cloud operations and reap the benefits of the cloud with confidence. We are expecting 150 attendees at this physical event. We have invited AiSP Patron - Senior Minister of State, Ministry of Communications and Information & Ministry of National Development Mr Tan Kiat How, to be our distinguished Guest of Honour for the opening. We will also be engaging CISOs, reputable services providers and vendors to present key development of Cloud Security.

Event Date: 17 Aug 2023

Event Time: 9.30AM – 2PM

Event Venue: Suntec Convention Centre

Guest of Honour: AiSP Patron - Senior Minister of State, Ministry of Communications and Information & Ministry of National Development Mr Tan Kiat How

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.**

### Professionals

1. Hall of Fame
2. Leader
3. Professional

### Students

4. Students

Please email us ([secretariat@aisp.sg](mailto:secretariat@aisp.sg)) if your organisation would like to be our sponsors for The Cybersecurity Awards 2023! Only Silver sponsorship packages are available.

### Enterprises

5. MNC (Vendor)
6. MNC (End User)
7. SME (Vendor)
8. SME (End User)

**TCA2023 Sponsors & Partners**

**THE CYBERSECURITY Awards 2023**

Organised by

**AiSP**  
Advance Connect Excel

Supported by

**image engine**      **SFA** SINGAPORE FINTECH ASSOCIATION

Supporting Associations

**CSCIS** CENTRE FOR CYBER SECURITY INTERAGENCY STUDIES      **CSA** cloud security alliance SINGAPORE CHAPTER      **HTCIA**      **SANS**      **Singtel**      **wizlynx group**

**ISACA** Singapore Chapter      **ISC** SINGAPORE      **OT-ISAC**

**SINGAPORE COMPUTER SOCIETY**      **SGTECH** WHERE TECH MEETS      **THE LAW SOCIETY IN SINGAPORE**

**Platinum Sponsors**

**BeyondTrust**      **CISCO**      **ENSIGN** INFOSECURITY

**HUAWEI**      **ST Engineering**      **TREND**

**Gold Sponsors**

**DBS**      **DSTA** Defence Science & Technology Agency      **FORTINET**

**Silver Sponsors**

**PCS SECURITY**      **SIT** SINGAPORE INSTITUTE OF TECHNOLOGY

# Digital for Life

## Library Learning Journey on 14 July

As part of Digital for Life movement, AiSP went to Bukit Panjang Library for the learning journey to library to share with the elderly on how to use the library app on 14 July. Our past year AiSP SVRP winner Chea Le Xin Andrea who is now working in our CPP - RSM Singapore did a sharing on the importance of stay safe online and beware of scams.



[back to top](#)

## Digital Club @ Ayer Rajah on 15 July

As part of the Digital for Life Movement, Team AiSP was invited to the Digital Club @ Ayer Rajah where we setup a booth to share with the public on how to stay safe online and beware of scams. Thank you our Corporate Partner Contfinity Pte Ltd for joining us and Grassroots Advisor for West Coast GRC - Minister Desmond Lee and Ms Foo Mee Har for visiting us at our booth.





## Skills for Good Festival 2023 from 28-29 July

As part of Skills for Good festival to promote continuous learning, AiSP and corporate Partner Wissen had a booth showcase at Bishan Junction 8 on 28-29 July to promote cybersecurity awareness. AiSP EXCO member Breyvan Tan did a sharing on Career Opportunities in Cybersecurity for the two days to the public.

On Day 2 of Skills for Good Festival, Mayor Denise Phua was the Guest of Honour and visited AiSP booth together with Mr Chong Kee Hiong, Advisor to Bishan-Toa Payoh Grassroots Organizations. Thank you AiSP President, Johnny Kho, AiSP EXCO Member, Breyvan Tan and Judy Saw from Wissen International for hosting them!



[back to top](#)

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

# SCAM AWARENESS AND DIALOGUE SESSION

## AiSP x PA x Huawei

With the theme of “elevating Cybercrime awareness”, this session aims to enhance the capabilities of the Leaders in identifying threats in the online space.

### Keynote Speakers

*Collaborative effort to maintain cybersafe*

*Common scam typologies, APPACT*



**Dennis Chan**

Country Cybersecurity and Privacy Officer, Huawei  
AiSP Cyberwellness Co-Lead



**Aileen Yap**

Assistant Director, Anti-Scam Command, Commercial Affairs Department, Singapore Police Force

### Panel Discussion



**SUN XUELING**

Panellist  
Minister of State in the Ministry of Home Affairs and Ministry of Social Family



**DENNIS CHAN**

Panellist  
Country Cybersecurity and Privacy Officer, Huawei  
AiSP Cyberwellness Co-Lead



**AILEEN YAP**

Panellist  
Assistant Director, Anti-Scam Command, Commercial Affairs Department, Singapore Police Force



**SOFFENNY YAP**

Moderator  
AiSP Secretary & Cyberwellness Co-Lead

### More Information


#### REGISTER NOW



<https://forms.office.com/r/CGQDee8qQt>

 26 Sep 2023

 6PM - 9PM

 Huawei AI Lab and DigiX lab  
51 Changi Business Park Central 2, Level 7  
The Signature, Singapore 486066

#### ORGANISED BY



#### IN SUPPORT OF



Register [here](#)

# Regionalisation

## CYDES from 10 – 13 July

AiSP went to Kuala Lumpur and set up a booth at CYDES from 10-11 July, We are pleased to have AiSP Advisory Chair, Mr David Koh to visit our booth at the event!



Upcoming Event

The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2023. The second webinar will be focusing on Cloud Security where speakers will be sharing insights on the best practices for cloud security.

**Challenges for Secure Cloud Adoption at scale in Singapore**

Speaker: Tony Low, AiSP Vice-President [Association of Information Security Professionals]

Will like to look at the trends in Cloud Adoption especially with security around the region. A look at some of the policies that Singapore government has rolled out how it has affected the organisations in drive cloud implementation. Meanwhile there have been a lack of talents in the space across the board, what are some of the initiatives that has been implemented with joint partnership with the private sector.

**Protecting Your Assets : Unravelling the Unique Security Deployment Requirements of On-Premise Vs. Cloud**

Speaker: Sutedjo Tjahjadi - Head of Cloud Computing Committee APTIKNAS [APTIKNAS]

The drive to move the workload into the cloud due the digital transformation adoption is significant. The cloud solution offers the simplification to the infrastructure operation because it offers as a service. One aspect which should not be overlook is Cyber Security.

We'll address questions such as: What are the key considerations for securing your cloud environment? How does on-premise security differ from cloud security? And what are the foundational elements required to implement a robust Zero Trust security model in the cloud?

**Risks and Mitigation Strategies for SMEs on Cloud IaaS**

Speaker: Ye Thura Thet, Principal Analyst, Kernellix [MISA]

Many SMEs today leverage cloud technology to enhance their business functions. While the cloud is no longer a new technology, technology teams with limited capacity tend to overlook some fundamental security controls when implementing a cloud computing model in SMEs. This presentation discusses common pitfalls for SMEs and presents a pragmatic approach to covering the basics.

**Serverless Security Model and Function Level Security**

Speaker: Rey Supan, Senior Solutions Architect [WiSAP (Women in Security Alliance Philippines)]

Understanding the security model of serverless computing and how it differs from traditional architecture and best practices for securing individual functions in a serverless architecture.

Date: 23 August 2023, Wednesday

Time: 3PM – 5PM (SGT)

Venue: Zoom

Registration:

[https://us06web.zoom.us/webinar/register/8216862079756/WN\\_C0gdnb9cTmKFQpAu0ZN\\_ig](https://us06web.zoom.us/webinar/register/8216862079756/WN_C0gdnb9cTmKFQpAu0ZN_ig)

## Corporate Partner Events

### Cyfirma Webinar on 5 July

Working with our corporate partner @CYFIRMA, AiSP has hosted the third Cyber Intelligence Briefing on the topic: SEO Poisoning and Typosquatting: Protecting Your Online Presence on 5 July. In the briefing, CYFIRMA researcher shared analysis of discovered remote access tool (RAT) called "VagusRAT" and its potential attribution to Iranian threat actors. The VagusRAT is deployed to victims through the exploitation of Google Ads.



## SOC 101 TRUST NO FILES! | Votiro BFSI Workshop on 12 July

As part of Digital for Life Movement, AiSP collaborate with our Corporate Partner, Votiro to organise an event on SOC 101 | Trust No Files on 12 July. Thank you AiSP President, Johnny Kho, Grace Chong, Mark Chan, George Seah & Paul Hadjy for sharing insights with the attendees.

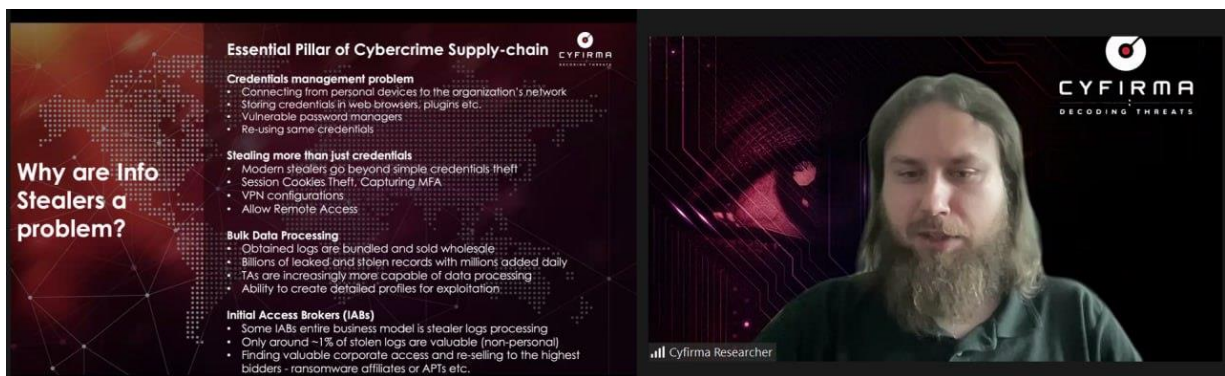


## Cyfirma Webinar on 19 July

Stealer malware is a type of malicious software that sneaks into computers, both personal and corporate, and steals valuable information. It does this by secretly communicating with a control center operated by cybercriminals. Information stealers are specialized malware used to steal account passwords, cookies, credit card details, and crypto wallet data from infected systems, which are then collected into archives called 'logs' and uploaded back to the threat actors.

Watch this video as CYFIRMA Cyber Researchers break down the details.

Watch the recording here -> <https://youtu.be/3Nw9GPxZm1s>



## Wissen CISO Alumni Gathering on 20 July

In support with our Corporate Partner, Wissen International (EC-Council ASEAN), we held a gathering with over 30 CCISO Alumni on 20 July. Thank you Aaron Ang, Audrey Teoh & Christopher Lek for sharing insights on Driving Business Growth and Building An Enterprise Security Culture: A Path to Success to the Alumni.



## Cyfirma Webinar on 26 July

Working with our corporate partner @CYFIRMA, AiSP has hosted the fifth Cyber Intelligence Briefing on the topic: Unmasking Wagner A Webinar on Russia's Controversial Mercenary Group. As concerned global citizens, it is imperative that we come together to understand the complex dynamics and potential dangers posed by this notorious private military company (PMC) and its ties to the Russian government. Watch this video as @CYFIRMA Cyber Researchers break down the details. #cyberintelligence #cybersecurity #situationalawareness #malware #infostealer #hacking Follow @CYFIRMARESEARCH to stay on top of the latest development in the world of cyber.

Watch the recording here ->

[https://us06web.zoom.us/rec/share/0uZviV-8T9iBWEkCNPqL-OQavCpG14A0Jqx\\_k07rNQiOHQpS75eQjgEUQaaU1hQ.Ab9yQDxUm93-0YQv?startTime=1690340113000](https://us06web.zoom.us/rec/share/0uZviV-8T9iBWEkCNPqL-OQavCpG14A0Jqx_k07rNQiOHQpS75eQjgEUQaaU1hQ.Ab9yQDxUm93-0YQv?startTime=1690340113000)

### Unmasking Wagner

A Webinar on Russia's Controversial Mercenary Group



stan.vitek@cyfirma.com



## Detecting the Undetected on 26 July

Together with our Corporate Partners, NetWitness & ONESECURE Asia Pte Ltd, we held an event on Detecting the Undetected on 26 July. Thank you Desmond Tan and Alvin Teo from ONESECURE Asia and Jolene Lim from NetWitness and AISP Data & Privacy EXCO Lead, Wong Onn Chee for sharing insights with the attendees.



Cyfirma Webinar on 2 August



**Cyber intelligence Briefings**  
**Defining Ransomware: Stages, Tactics, and Protection.**



Dear Cybersecurity Professionals,

We hope this email finds you well. We are excited to invite you to our upcoming webinar on the topic of "**Defining Ransomware: Stages, Tactics, and Protection.**" In today's digital landscape, the threat of ransomware looms larger than ever, and it's crucial to stay informed and prepared.

During this webinar, our expert speakers will delve into the following key areas:

- **Defining Ransomware:** Gain a comprehensive understanding of what ransomware is, how it works, and the impact it can have on individuals and organizations.
- **Different Stages of a Ransomware Attack:** Learn about the various stages that constitute a ransomware attack, from initial infection to encryption and ransom demands.
- **Tactics, Techniques, and Procedures (TTPs)** used by Ransomware Groups: Explore the sophisticated methods employed by ransomware groups to maximize their effectiveness and evade detection.

- **Recent Cyber-Attacks by Ransomware Groups:** Get insights into some of the most recent and high-profile ransomware attacks, understanding the modus operandi and their targets.
- **Protection Strategies:** Discover effective measures and best practices to protect yourself and your organization from falling victim to ransomware attacks.

Date: 2 August 2023, 11am SGT

Registration Link:

[https://us06web.zoom.us/webinar/register/4016841183809/WN\\_SQKml4mTQnupUt2PXQwRw](https://us06web.zoom.us/webinar/register/4016841183809/WN_SQKml4mTQnupUt2PXQwRw)

Our webinar will feature interactive sessions and an opportunity to ask questions directly to the experts. It is open to anyone concerned about cybersecurity, whether you're an individual looking to safeguard personal data or an IT professional responsible for securing your organization's network.

Don't miss out on this opportunity to enhance your knowledge and fortify your defenses against ransomware threats. Limited seats are available, so secure your spot now.

**Join us as we explore the inner world of these dangerous cybercriminals.**

## Operational Technology Cybersecurity Expert Panel Forum 2023 on 22-23 August



**OPERATIONAL TECHNOLOGY  
CYBERSECURITY EXPERT  
PANEL FORUM 2023**

EMBRACING NEW PERSPECTIVES  
AND STRENGTHENING CAPABILITIES

**DATE: 22 – 23 AUGUST 2023**  
**VENUE: RESORTS WORLD CONVENTION CENTRE,  
EAST BALLROOM**

Gain valuable insights into strategies and learn best practices for safeguarding OT systems against ever-evolving cyber threats. Catch our panel members in action as they share their knowledge and experiences on topics such as enhancing OT security through comprehensive assessment and do's and don'ts of OT penetration testing.

	<b>MS SALTANAT MASHIROVA</b> <i>Advanced Cybersecurity Architect, Honeywell Founder, Women in Cybersecurity (Kazakhstan)</i>		<b>MR JUSTIN SEARLE</b> <i>Director of ICS Security, InGuardians, Inc</i>
	<b>DR LIM WOO LIP</b> <i>Chief Technology Officer (Cyber) of ST Engineering</i>		<b>DR TERENCE LIU</b> <i>Chief Executive Officer, Trone Networks</i>

FIND OUT MORE AT [WWW.OTCEP.GOV.SG](http://WWW.OTCEP.GOV.SG)

**REGISTER NOW** 

FOLLOW US FOR THE LATEST EVENT UPDATES

 @CSASINGAPORE

 CYBER SECURITY AGENCY OF SINGAPORE (CSA)

HELD IN  **Singapore**  
Passion Made Possible

ORGANISED BY 

OTCEP Forum 2023 will be held from 22 to 23 August 2023 at Resorts World Convention Centre, East Ballroom.

The event will comprise of plenary presentations, industry participation, Capabilities Development Showcases, technical presentation and concurrent tracks in the domains on Operations, Engineering and Governance.

We are also pleased to share that all panel members will be physically in Singapore for OTCEP Forum this year.

We are now ready for registration to attend OTCEP Forum 2023. The broad programme outline is as follows:  
Day 1 - (22 August)

[back to top](#)

- Main Plenary Presentations and Panel Discussion
  - Capability development Showcase Day 2 - (23 August)
- Concurrent Track on Operations, Engineering and Governance Domains
  - Capability development Showcase

Please scan the QR code to register or visit us at <https://www.otcep.gov.sg> .  
See you at the event!

## AiSP x JTC Networking Event

**ORGANISED BY:**

  **AiSP x JTC Networking Event**

Exclusive sharing by JTC on Punggol Digital District, Singapore's first smart and sustainable district, and partnership opportunities by AiSP and SIT

 08 Sep 2023  
Friday  5PM - 7PM

 L22 PDD Gallery at one north

  
Artist's Impression of Sky Terrace Gardens at Punggol Digital District. Credit: JTC

**Questions & Answers Segment**

 Ms Yeo Wan Ling Member of Parliament for Pasir Ris-Punggol GRC	 Mr Johnny Kho President, AiSP	 Ms Yap Eai-Sy Director, New Estates Business Development & Marketing Division and Info-Comm Media & Start- Up Cluster, JTC	 Prof Steven Wong Director, Projects, Office of the Provost, SIT
--	---	--	---

AiSP and JTC will once again be organising a networking session and updates on the Punggol Digital District on **8 Sep 23 (Fri) from 5pm to 7pm at Level 22 PDD Gallery at One North**. This year, we have the honour to have **Ms Yeo Wan Ling, Member of Parliament for Pasir-Ris Punggol GRC (Punggol Shore)** to also share her plans in Punggol and how partners like you can work with them. Speakers include AiSP President Mr Johnny Kho, Prof Steven Wong from Singapore Institute of Technology and Ms Yap Eai-Sy from JTC.

Register [here](#) by **11 Aug 23**.  
Admin instructions will be sent out 3 days before the event.

# Upcoming Activities/Events

## Ongoing Activities

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

## Upcoming Events

Date	Event	Organiser
2 Aug	Cyfirma Webinar	AiSP & Partner
2 Aug	Learning Journey to Trendmicro for Pri Sch	AiSP & Partner
<a href="#">2 Aug</a>	<a href="#">Learning Journey to Google for ITE West</a>	<a href="#">AiSP &amp; Partner</a>
4 Aug	<a href="#">National Day Celebration with Advisory Council</a>	AiSP
5 Aug	Pasir Ris Town National Day Celebration	AiSP & Partners
9 -10 Aug	CISO Exec Network Sydney	Partner
11 Aug	Cyfirma Webinar	AiSP & Partner
12 Aug	Jalan Kukoh Community Day	AiSP & Partner
15 - 16 Aug	SMEICC	Partner
15 Aug	MBOT ENTICE Event	Partner
16 Aug	Cyfirma Webinar	AiSP & Partner
16 Aug	ASEAN Bug Bounty	AiSP & Partner
17 Aug	<b>Cloud Security Summit</b>	AiSP
22 -23 Aug	CISO Singapore	Partner
23 Aug	<a href="#">SEA CC Webinar – Cloud Security</a>	AiSP & Partner
23 Aug	School Talk @ Westwood Sec	AiSP & Partner
24 Aug	ISACA Singapore GTACS Conference	Partner
25 Aug	ISC2 Workshop	AiSP & Partner
29 – 30 Aug	IndoSec 2023	Partner
29 Aug	Learning Journey to DBS for Pri Sch	AiSP & Partner
30 Aug	Learning Journey to Google for Pri Sch	AiSP & Partner
30 Aug	<a href="#">Knowledge Series - IoT</a>	AiSP
30 Aug	Cyfirma Webinar	AiSP & Partner
31 Aug	<a href="#">International Cyber Women Day Celebrations</a>	AiSP
5 – 6 Sep	CISO Brisbane	Partner
7 Sep	<a href="#">SEA CC Webinar – Ladies in Cyber</a>	AiSP & Partner
8 Sep	AiSP x JTC PDD Event	AiSP & Partner
11 – 15 Sep	<a href="#">Overseas Learning Journey to Brunei</a>	AiSP & Partner
12 Sep	Cisco Webinar: Well, That Escalated quickly: Prioritizing Alert to Minimize Impact	Partner
15 Sep	BCSA Conference	Partner
20 Sep	<a href="#">AiSP Knowledge Series – Red Team</a>	AiSP & Partner
21 Sep	<a href="#">AiSP x BT x CSA Event</a>	AiSP & Partner

[back to top](#)

26 Sep	<a href="#">AiSP x Huawei Scam Awareness event with MOS Sun Xueling</a>	AiSP & Partner
--------	---	----------------

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

# CONTRIBUTED CONTENTS

## Article from Cyber Threat Intelligence SIG

### **Distilling & Democratising External Cyber Threat Intelligence**

*Anthony Lim for AiSP, with thanks to Raymond Tan, ITnews.Asia.*

***We need to be aware about how cybercriminals can expose your digital assets by hijacking your brand, and take the measures to help preserve your customer trust and loyalty.***

The phenomena of the external cyber threat intelligence market is relatively new, coming to the fore only about five, less than 10 years ago. Today, we are seeing more players, be they from stand-alone solutions or from offshoots from a product (e.g. through an endpoint, firewall or other security solutions).

**Q: As a business leader, how do you know which threats matter and how important are they when you plan out your organisation's cyber security requirements?  
How would you describe cyber threat intelligence and its importance?**

As the name implies, external cyber threat intelligence (or TI for short) seeks to provide enterprise tech users with up-front intelligence about threats that may pertain to their IT network, service and assets, so they can ensure in place the appropriate defenses, or minimise the vulnerabilities or exposures, as best as they can, to mitigate the risks therein.

These specifically are threats external to the enterprise IT infrastructure – we call it 'outside the wire'. It is not so much a direct 'brute force' hacking of the IT network or servers etc. Rather, it's about the organisation's digital footprint and digital assets – including its web site, IP addresses, pieces of data that is sitting somewhere outside, even defending the organisation's brand, and also the digital elements and identities of their VIPs (key officers – Chairman, C-Level, board of directors, senior management).

**Q: How does 'defending the organisation's brand?' involve cyber-security, or vice versa?**

Cybercriminals today use your brand against you. For instance, they can impersonate your social media accounts, develop rogue mobile apps, sell stolen and counterfeit products, and hijack your brand to run scams.

External visibility and control over these brand threats are critical to safeguarding your valuable portfolio of trademarks, logos, and products. So, the organization needs to be able to protect what's theirs. But it goes one step further – they also need to protect their customers, and perhaps also some of their key digital ecosystem partners.

It's not just your organisation they want. Hackers impersonate your brand to steal your customers' data – to sell, abuse, impersonate etc.

You need to know about brand hijacking attempts, and take the measures to bring down the rogue sites – and help organisations preserve customer trust and loyalty.

At the same time, there are malicious apps and scams that needs to be dismantled. Companies have to detect, prioritise, and take down external threats to their brand across the clear, deep, and dark web – eliminate fake mobile apps, knockoff scams, brand misuse, the spread of misinformation and leaked intellectual property.

**Q: What about phishing? The damage from phishing is often not well known or misunderstood.**

Of course when we talk about cyber threats, we also need to look at phishing. We have to prevent phishing early in the attack chain. We must not 'bait the hook'.

Phishing remains the easiest, most popular, and most reliable technique for threat actors to trick vulnerable employees and customers into revealing sensitive data. It's critical to identify potential phishing attacks as early as possible to shut them down before human assets become attack vectors.

There are steps organisations can take, one of the most critical is being able to identify early signs of phishing weaponisation.

I know it's starting to sound more scary, but you need to monitor for common phishing tactics — domain spoofing, look-alike domains, typosquatting, homoglyphs, and more — that use countless permutations of your legitimate domains and subdomains.

These are all obvious tricks of the perpetrator – but we keep getting hit. Act on early warnings.

You need to be able to continuously track suspicious domain xChanges - monitor and correlate changes to domain attributes, including Whois info, MX and/or A record changes, IP reputation, and SSL certificate updates, to gain the full context and risk behind suspicious domains. You must keep a close eye on domains.

Organisations leverage the external cyber TI service provider's remediation team and robust ecosystem of partners to accelerate rogue domain takedown requests, block domains on perimeter devices, and shut down phishing attacks before they're launched.



The provider nowadays in turn needs to collaborate with trusted industry experts and value-add partners to make this happen.

Any advantage you can gain over your cyber adversaries is worth having. External TI can help you identify new cyber threats early, but this intelligence is only useful if you know how you're impacted and can act quickly.

The first step in this journey is to find out if – and where – you're exposed. You need immediate visibility into how your organisation is being targeted based on assessing your domain for threats that lurk across the clear, deep, and dark web.

### **Q: What does external threat protection and digital footprint protection entail?**

Firstly – you identify and lock down leaked sensitive information, and you instantly retrieve the leaked data.

Data leakage is one of the most significant threats to companies because it gives threat actors instant access to sensitive data or internal systems. If credentials or confidential data are leaked online, including in public repositories like GitHub, it's critical to identify, validate, and remediate the exposure as quickly as possible.

Secondly, you discover and reset exposed employee credentials and similarly lock them down.

Instantly discover and automatically lock down your leaked credentials on the clear, deep, and dark web using our continuous monitoring engine, extensive leaked credential database, and automated mitigation capabilities, including our unique integration with Active Directory.

Thirdly, you identify, secure and restore documents.

Continuously monitor black markets, closed hacker forums, paste sites, public repositories, and more to identify sensitive documents, secrets such as API keys, and new data dumps. Obtain data samples from threat actors, validate data legitimacy, and track down sources of leakage or data theft.

Finally, you can protect your customers by uncovering their compromised customer accounts. Monitor exposed or leaked credentials that may compromise customer PII, financial assets, or loyalty program rewards.

### **Q: What is the vision about democratising threat intelligence**

The idea is to find an external intelligence solutions and services that is easily accessible for organisations of any type or size, by synthesising complex signals captured from across the clear, deep, and dark web into contextualised, prioritised, and actionable intelligence.

Hence, “democratizing” of external cyber threat intelligence (TI) by enabling organisations of any type or size to gain the full benefits of external TI, no matter the scope or sophistication of their program. TI need not be this big, scary monolithic thing that only big enterprises and governments can benefit from.

Despite all the heightened awareness and need, our world is still chronically short of cyber security professionals. Democratising TI highlights simplicity of use and automating takedowns and remediations, which help smaller companies to quickly adopt TI solutions and services too, and thus help reduce their cyber risk to themselves and the overall ecosystem they play in, especially in today’s crazy world where hackers are attacking supply-chain partners and business eco-system members to get into their targeted company from.

**Q: When we speak of cyber security, TI or digital transformation, it's hard not to take into account the pandemic or the 'new normal'.**

As organisations move to remote work environments and face staff and budget cuts, they have to protect their businesses from threat actors looking to take advantage of the disruptions caused by the then-COVID pandemic, and even today when although the lockdown has since eased, there are still jitteriness and disrupted work patterns and workflows from back then still prevailing today, as we find our footing for the new normal.

They must be able to cover external threats across PaaS, SaaS, and IaaS. The ‘new normal’ requires new intelligence scenarios, which intelligence discovery capabilities need to be extended to include confidential documents, credentials from botnets, GitHub mentions, and many more.

They also have to accelerate their vulnerability prioritisation capabilities with bidirectional integrations and improve platform automation. Through extensive technology integrations, organisations will be better able to streamline their vendor risk assessments.

### Author Bio



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

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

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

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

## Article from Corporate Partner, Bugcrowd

### Bugcrowd's New Inside the Mind of a Hacker Report

The wait is finally over—Bugcrowd has released their seventh edition of [Inside the Mind of a Hacker](#)! When Bugcrowd first started releasing this annual report, it quickly gained popularity across the security industry as the gold standard for demographics, trends, and motivations within the hacker community.

This edition analyzed 1000 survey responses from hackers on the Bugcrowd Platform, in addition to millions of proprietary data points on vulnerabilities collected across thousands of programs.

It includes a special feature on security in the age of generative AI. The internet is full of fear-mongering articles covering the terrifying consequences AI could have on cybersecurity, but what about ways hackers can use AI to make the world a safer place? This report digs into how hackers are using AI technologies to increase the value of their work.

#### Key Learnings

##### 1. Even in an uncertain economy, the motivations of hackers remain altruistic.

There is a misconception that hackers, even the ethical kind, are only after money. For many of them, hacking is their full-time career, so of course financial factors are major motivators. However, time and time again, data shows that the

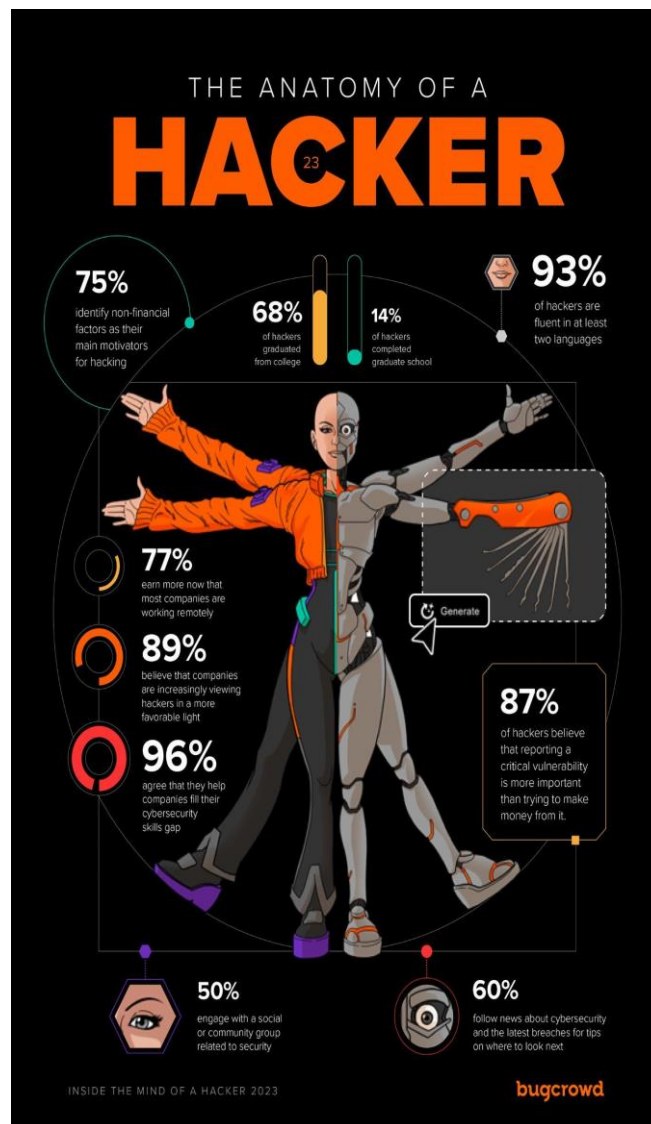
heart of hacking is much more complex. 75% of hackers identify non-financial factors as their main motivators to hack and 87% of hackers believe that reporting a critical vulnerability is more important than trying to make money from it.

**2. Top hackers consider generative AI as a tool to leverage, not a threat.**

72% of hackers do not believe AI will ever replicate their human creativity. Although some hackers are concerned about generative AI making their skills irrelevant, many of Bugcrowd's top hackers disagreed. According to Nerdwell, "If you're stagnant and don't grow your skills, then maybe you should be worried about AI, but if you embrace it and use it as a tool, then I believe you'll likely become even more valuable."

**3. CISOs are taking generative AI seriously.**

This edition spotlights two CISOs and surveys many others. We found that across the board, CISOs are already considering the potential cybersecurity risks of generative AI. They are approaching these concerns from a technical side, such as data poisoning and prompt injection concerns, and wider issues, such as implications on privacy and traceability.



Download [Inside the Mind of a Hacker](#) today to learn why organizations can trust hackers to secure their future with confidence.

## The Bugcrowd Security Knowledge Platform™

### Orchestrating data, technology, and human intelligence for crowdsourced cybersecurity

Bugcrowd has invested heavily in a SaaS platform that orchestrates data, technology, and human intelligence to help you quickly find, validate, prioritize, and remediate vulnerabilities uncovered by the Crowd, with the right trusted security researchers always brought into your workflows at the right time. And unlike alternatives, the Bugcrowd Platform lets you run multiple crowdsourced solutions in parallel at scale for a layered approach to cybersecurity.

Solutions on the platform include:

#### Penetration Testing as a Service

Bugcrowd PTaaS is the modern, streamlined approach to targeted security testing, helping to discover vulnerabilities across any target type continuously or on demand:

- Launch within days, not weeks
- Get 24/7 visibility into timelines, pen test findings and analytics, and methodology checklist progress
- Meet compliance objectives and go beyond them when needed

#### Managed Bug Bounty

Bugcrowd Managed Bug Bounty a highly efficient way to incentivize the discovery of emerging vulnerabilities that scanners miss, with scope and rewards pre-determined by you.

- Get end-to-end guidance based on best practices from 1000s of customer experiences
- Count on best-in-class triage from a global team of domain experts
- Continually adjust program parameters based on insights from data

#### Vulnerability Disclosure Programs

Bugcrowd VDPs invite the world to report critical vulnerabilities in your public-facing assets. Think of a VDP as a “neighborhood watch” program that helps you:

- Align with best practices such as NIST as well as industry regulations
- Build initial relationships with the security researcher community
- Demonstrate security maturity with a program that customers can see and value

#### Attack Surface Management

Bugcrowd ASM is the first solution to reduce risks of unknown attack surface by matching the effort and scale of attackers with the ingenuity and impact of the Crowd.

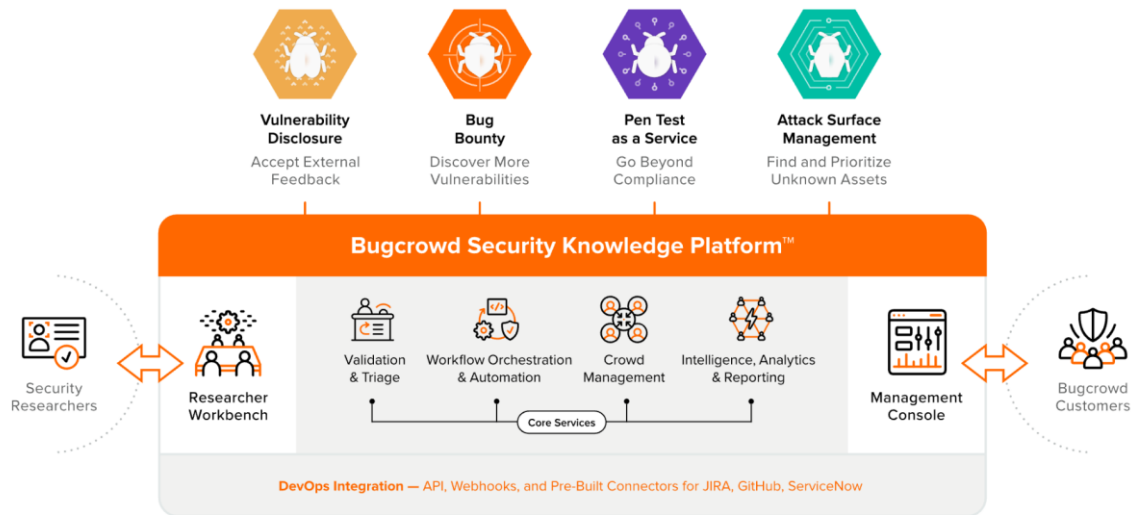
- Find and prioritize risk by combining live recon with data from our rich AssetGraph™ knowledge base
- Get customizable reports with full risk profiles, attribution methods, and recommendations
- Seamlessly migrate results to other solutions for targeted testing and continuous coverage

## Platform Overview

Organizations of all kinds need to do everything proactively possible to protect themselves, their reputation, and their customers from being blindsided by cyber attacks. The Bugcrowd Security Knowledge Platform™ finds hidden vulnerabilities before

[back to top](#)

attackers do by uniquely orchestrating data, technology, and human intelligence—including tapping into the global security researcher community (“the Crowd”)—for solutions that span Pen Testing as a Service, Vulnerability Disclosure, Bug Bounty, and Attack Surface Management.



**Best Security ROI from The Crowd**

We match you with the right trusted security researchers for your needs and environment across hundreds of dimensions using ML

**Instant Focus on Critical Issues**

Working as an extension of the platform, our global security engineer team rapidly validates and triages submissions, with P1s often handled within hours

**Contextual Intelligence for Best Results**

We apply accumulated knowledge from over a decade of experience across 1000s of customer solutions to your goals for better outcomes

**Continuous, Resilient Security for DevOps**

The platform integrates workflows with your existing tools and processes to ensure that applications and APIs are continuously tested before they ship

For any enquiries, please contact Hassan Alkaff at [hassan.alkaff@bugcrowd.com](mailto:hassan.alkaff@bugcrowd.com)

# Article from Academic Partner, Singapore Polytechnic



The School of Computing, Singapore Polytechnic is now sourcing for **Final Year Projects** (FYPs) for Diploma in Cybersecurity & Digital Forensics (DCPF). This is a full-time diploma that equips students with cybersecurity skills to counter offensive attacks, adopt defensive measures and implement investigative techniques. The Final Year Projects take place from **October 2023 to February 2024**.

The main difference between internship and FYP: for FYP, you have 4 to 5 students working as a team to develop a project for your organization, starting from requirements study to project completion. Unlike internship, the FYP teams do **not** work onsite, but will meet your team regularly either face-to-face or via MS Teams. All source code and documentations, if any, will be handed over to you when you accept and sign off the project. In short, if you have a project in mind or a cybersecurity technology to explore and want to a team to develop it in 4 months, let it happen on FYP.

Why not send your project idea to us, so we can evaluate and finetune it with you for FYP? Please download [this form](#) and write your idea, then send it to us by **8 Aug 2023**, or talk to us at our contacts below.

Like any school projects, SP SOC owns the right of FYP. Industry partner will pay SP SOC S\$3,000 for the right to use the project. But the good news is: if your project is meant for prototype, research or in-house use, **the payment is automatically waived**. Please contact us for a sample agreement. The project will commence when both parties have agreed on the project scope and signed the agreement.

Various government agencies and private companies have worked with our FYP students. You can view some of our past and completed FYPs at <https://www.sp.edu.sg/soc/soc-projects-showcase/Project-2021>

Thank you for your attention. Looking forward to working with you.

**Peter Lee Wai Tong**  
Lead (Student Development)

**SP** SCHOOL OF  
Computing

Email: peter\_wai\_tong\_LEE@sp.edu.sg

Office: 6772 1884

Mobile: 9757 0432

[back to top](#)

## Article from SVRP 2022 Winner, Darren Ong



It was such unexpected and delightful news when I received the news that I was a Gold Award winner and Valedictorian for the Student Volunteer Recognition Programme (SVRP) in 2022. I still recall that I was on a short tea break after long hours into my major project's meeting, when I read that specific email. Elated, I shared the news, where everyone in the meeting celebrated the award with me, and I immediately thanked my mentors and peers who had helped me along my journey. With a gratuitous heart, it was only a few months later that I was up on stage sharing my lived experience in cybersecurity and receiving the award from Minister Mr Tan Kiat How.

This award holds a strong place in my heart, not just because of its pride and accomplishment, but more so for what it creates and represents. With the gold award having a minimum criterion of at least 150 hours, it creates the purpose to have a passion not just to simply do cybersecurity - but to be involved in it and make a positive difference in Singapore's cyberspace.

An alumnus of Edgefield Secondary, I went into Temasek Polytechnic's Polytechnic Foundation Programme and entered the cybersecurity diploma. From being an organizing head for the Interpoly Capture the Flag competition along with the other 4 polytechnics, to competing for Singapore in WorldSkills and creating a research paper on Fully Homomorphic encryption, my experience in cybersecurity has been exciting!





I was first introduced to the Interpol Capture the Flag competition in 2021, when I was just elected as the President for the Temasek Polytechnic Cybersecurity interest group. This was an entirely new task for me, especially as I was newer to managerial roles. Albeit uncertainty, me and my co-president Russell Yap got the chance to collaborate with representatives across polytechnics, where we worked with industry partners involving of Division 0, Cyber Youth Singapore, and Cybersecurity Agency of Singapore. With the help of our members, we also set up capture-the-flag challenges and publicised the event. With the goal of inspiring and dedicating a continuous tradition of cybersecurity skillsets among youths, we managed to reach around 400 students from pre-tertiary institutions.

This experience alone drove my passion in cybersecurity and made me realise that I wanted to do much more for youths in cybersecurity. Starting from our roots, my team and I created workshops for cyber-hygienic practices for freshmen in the Polytechnic Foundation Programme at Temasek Polytechnic, after seeing the rise in scams in the past few years. This was further developed by cultural exchanges with Japanese students in Kumamoto, Japan, where we got to teach them about basic network administration and cybersecurity practices.

With this gained experience, I decided that I also wanted to dive into the academia and theoretical side in cybersecurity. Before my Year 3 even started, I decided to email a professor in Temasek Polytechnic, and after seeing my proactiveness, decided to undertake me on a project on “CUDA Enabled Fully Homomorphic Encryption”.



After a few tough months, we managed to publish the paper at IEEE in Guangzhou, China. This opened up several more opportunities for us where we presented our project at the Singapore International Cyber Week and IBM Think to executives and ministers, including DPM Heng Swee Keat.

This might sound surprising to some, yet normal to others, but the best parts of my journey were not the “high fly” moments such as going up on stage or being recognised for my achievements. Rather, I enjoyed the interactions so much more. I have met so many talented and unique people in conferences, events, and competitions, and have built up relationships where we talk more than work.

My success and achievements are not my own – rather, the combination of people who have encouraged and helped me along the way, and the leaders who have shaped and carved out the path for me. I am forever grateful for my student interest group members, Interpol representatives, seniors, juniors, teachers, mentors, and especially so to Russell Yap, my co-president, who have been with me not just in my highs but stuck by me even when at my lows. I would also like to thank AiSP for giving me the opportunity in the SVRP and even in this article. You have played an integral role in the development and growth of cybersecurity and technology in Singapore, and I know you will continue to do so in the future.

I believe that strong foundations build bright generations. My personal experiences and achievements in this community have utilised the built foundations from my seniors, and now, it is my turn to give back even more to the cybersecurity community in Singapore.

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®)

## QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

Online



# 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!

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.