

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

- Cloud Security SIG: Distilling & Democratising External Cyber Threat Intelligence
- DT Asia: The Anatomy of Active Directory Attacks
- Developing the Next Generation of Cybersecurity Talent : Interning at Confinity
- Wizlynx: Zero Trust Framework: Bolstering Cloud Security in the Remote Work Era
- Parasoft: Compliance is a Pain! I need a painkiller
- SVRP 2022 Winner: Claudia Chan

Professional Development

Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome Getvisibility and OPSWAT as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partners



News & Updates

National Day Celebration hosted by Cyber Security Agency of Singapore on 4 August

On 4 August, our AiSP CPP and APP members had an early celebration for National Day with Cyber Security Agency of Singapore (CSA) over a time of wine and canapes. Thank you AiSP Advisory Chair, Commissioner of Cybersecurity and Chief Executive, Cyber Security Agency of Singapore, Mr David Koh for hosting us and Mr Wong Choon Bong for sharing with our members on the upcoming initiatives in cyber!



Annual SME and Infocomm Commerce Conference (SMEICC) 2023 on 16 August

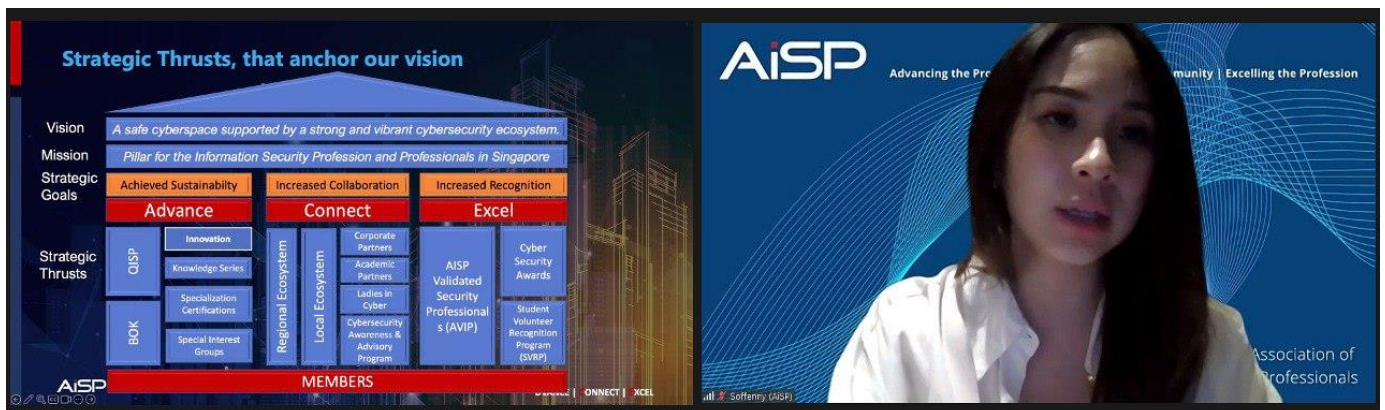
On 16 August, AiSP EXCO Member Freddy Tan did a sharing at 新加坡中华总商会 SCCC SMEICC, and moderated the panel discussion on Cybersecurity in the Digital Age: Protecting Your business from emerging threats.



Knowledge Series Events

IoT on 30 August


As part of Digital for Life Movement, AiSP organised the Knowledge Series on 30 August focusing on Internet of Things. Thank you to our Corporate Partners CyberSafe, CYFIRMA and DT Asia for sharing insights with our attendees. Thank you AiSP Secretary & IoT SIG EXCO Lead, Ms Soffenny Yap for giving the opening address and Our Corporate Partner, Wissen International for sharing on the cybersecurity courses.




<p>Foundation</p> <p>Cybersecurity Essentials</p> <ul style="list-style-type: none"> For those who are new to information security, need an introduction to the fundamentals of security and may be considering a career change Gain understanding in cybersecurity concepts such as Network Defense, Ethical Hacking and Digital Forensics No pre-requisites necessary 2 days training supported by UTAP <p>EC-Council</p> <p>Essentials Series</p> <p>Essential Skills for Tomorrow's Entry-Level Cybersecurity Careers</p> <p>Network Defense (NDE) Ethical Hacking (EHE) Digital Forensics (DFE)</p>	<p>Program Achieves DoD 8570</p> <p>CEH Certified Ethical Hacker</p> <p>The Certified Ethical Hacker (CEH) program is a recognized certification for the United States Department of Defense's (DoD) Computer Network Defense Service Providers (CND SPs), a specialized personnel classification within the DoD's information assurance workforce.</p> <p>This recognition falls under the auspices of DoD Directive 8570 Information Assurance Improvement Program. Directive 8570 provides clear guidance to information assurance certification and workforce management across all affected components of the U.S. DoD.</p> <p>EC-Council Courseware certified to have by the United States National Security Committee on National Security</p>
<p>CYBERSAFE</p> <p>First, we've got to understand classifies as IoT? Networking, Data Exchange, and Automation</p> <p>WAN, LAN Connections?</p> <p>What access is required for Automation?</p> <p>What data is sent? E.g. Audio? Files? PII Info?</p>	<p>CYBERSAFE YOUR SECURITY. OUR PRIORITY</p> <p>Bill Dave (CyberSafe)</p>
<p>PIONEER</p> <p>EXTERNAL THREAT LANDSCAPE MANAGEMENT PLATFORM ETLM</p> <p>UNIFIED VISIBILITY OF YOUR EXTERNAL THREATS AND RISKS</p> <p>Founded in 2017 by ex-government intelligence head and CISO</p> <p>AJML enabled, cloud native SaaS products - DeCTR and DeTCT</p> <p>Partners: RICOSS, btpt, NEC, Mitsubishi Corporation, ZILKHA, SUBARU</p> <p>Analysts: FORRESTER, Gartner, IDC</p>	<p>Remove Pin</p> <p>CYFIRMA DECODING THREATS</p> <p>Bill Mike (Cyfirma)</p>
<p>Enhancing security by using Zero Trust approach for OT access</p> <p>How to secure IT, OT and IoT accesses, transcend VPNs and adopt JIT/JEP Zero Trust?</p> <p>Raymond Ma Regional Director SSH Communications Security</p> <p>SSH.COM</p>	<p>Remove Pin</p> <p>SSH.COM</p> <p>Bill Raymond (DTasia)</p>

Upcoming Knowledge Series


Red Team on 20 September




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

[back to top](#)

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

Page 5 of 56

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

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*),

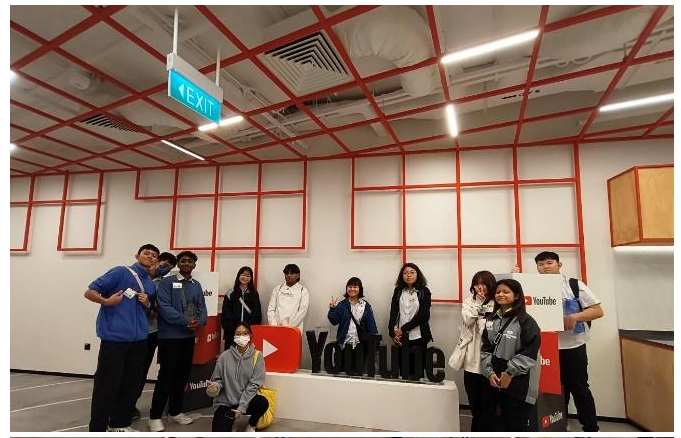
1. DevSecOps, 25 Oct
2. CTI, 22 Nov

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 Google on 2 August

As part of Digital for Life Movement, AiSP brought 80 students from our Academic Partner, ITE West, on a learning journey to Google office on 2 August. The students had a great time hearing from the professionals on the career prospects and toured the office premise. Thank you Mandiant (now part of Google Cloud), our Corporate Partner for hosting us.



[back to top](#)

AiSP Cyber Wellness Programme

Organised by:



Supported by:



In Support of:



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



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



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



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



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



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



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



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

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

Click [here](#) to find out more!



Ladies in Cybersecurity

AiSP Ladies in Cyber Career Sharing and Networking on 31 August

It was fun and insightful evening with food and drinks at AiSP Ladies in Cyber Career Sharing and Networking session in celebration for International Women in Cyber Day.

Thank you Ms Tham Mei Leng, Ministry CISO at Ministry of Sustainability and the Environment for sharing her personal experience on career development and the value of continued learning and certifications in cybersecurity and AiSP Vice President, Ms Sherin Lee for the closing address. We also extend our heartfelt gratitude to all attendees for joining us on 31 August.

AiSP would like to wish all ladies a Happy International Women in Cyber Day!



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-Isames
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

SEACC Forum on 16 October



The banner features a large QR code on the left side. On the right, the text reads 'SEA CC FORUM 2023' in large white letters. Below this, a box indicates the event is on 'MONDAY | 16 OCTOBER 2023 | 9AM - 1PM'. A list of topics is shown with green circular markers: 'SEA CC WEBINAR - DATA & PRIVACY', 'SEA CC WEBINAR - CLOUD SECURITY', 'SEA CC LADIES IN CYBER WEBINAR', and 'SEA CC FORUM 2023'.

ORGANISED BY



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](#)

[back to top](#)

Special Interest Groups

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

- Cloud Security
- Data and Privacy
- Cyber Threat Intelligence
- IoT

We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together. If you are keen to be part of a SIG, please contact secretariat@aisp.sg



Cloud Security Summit on 17 August

What an insightful time it has been at the AiSP Cloud Security Summit held on 17 August! The energy, enthusiasm, and knowledge shared throughout the event were truly inspiring.

With the theme "Simplifying Cloud for a Safer Future," we delved into the complexities of cloud security, uncovering ways to make it accessible and robust. The discussions were enlightening, and the connections made were invaluable. A major highlight was the signing of the Memorandum of Understanding (MoU) with Cisco Networking Academy. This collaboration marks a pivotal step towards empowering cybersecurity education, and we couldn't be more thrilled about the possibilities it holds!

We extend our heartfelt gratitude to our sponsors, Bugcrowd, Cisco Systems, CrowdStrike, Minecast, Contfinity Pte Ltd, Parasoft, Horangi and wizlynx group and our supporting agencies, Cyber Security Agency of Singapore (CSA) and Govtech Singapore who made this event possible. Your support has been instrumental in creating an environment where innovation and knowledge flourish. Thank you to our AiSP Vice President and AiSP Cloud SIG Lead, Mr Tony Low for the welcome address and moderating the panel discussion and SMS Tan Kiat How for gracing the event as our AiSP Patron!

To all the participants, speakers, and partners, you've made this summit a resounding success. Let's take the lessons learned and connections forged to continue championing

a safer digital future together. We looked forward to meeting you in our Cloud Security Summit 2024.



[back to top](#)



Cybersecurity Awareness & Advisory Programme (CAAP)

SME Cybersecurity Conference 2023

AISP
Association of Information Security Professionals

SME CYBERSECURITY CONFERENCE 2023

27 NOV 2023 9.30AM - 2PM CAPITAL TOWER

GUEST OF HONOUR: MS YEO WAN LING, MEMBER OF PARLIAMENT FOR PASIR RIS-PUNGGOL GRC AND NTUC U SME DIRECTOR

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 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

Enterprises

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

Students

4. Students

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

TCA2023 Sponsors & Partners



Organised by



Supported by



Supporting Associations



Platinum Sponsors



Gold Sponsors



Silver Sponsors



Digital for Life

Booth at Pasir Ris Town Park on 5 August

As part of Digital of Life Movement, AiSP and our Corporate Partner, RSM Singapore had a booth at the Pasir Ris Town Park on 5 August. Thank you Senior Minister Teo Chee Hean and Member of Parliament Sharael Taha for visiting our booth



Jalan Kukoh Community Day on 12 August

As part of Digital for Life Movement, AiSP had a booth on 12 August at Jalan Kukoh Community Day to share cyber hygiene tips with the residents. Thank you Minister Josephine Teo for visiting our booth.



Celebrate Digital @ East Coast Appreciation Nite 2023 on 22 August

A great evening of networking over food and drinks at the Celebrate Digital @ East Coast Appreciation Nite 2023 on 22 August where AiSP Patron & Grassroot Advisor for East Coast GRC Senior Minister of State Tan Kiat How presented Certificate of Appreciation to all the partners that involved in the Celebrate Digital @ East Coast.

Thank you to our AiSP Corporate Partner - Acronis, Contfinity Pte Ltd, DBS Bank, Grab, Huawei Singapore & Trend Micro who setup activities at the event to share with the residents of East Coast on the importance of Digital and beware of scams.

Also thank you to our Academic Partner - Temasek Polytechnic for providing 200 student volunteers to support in the event.



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

ENTICE event at Kuala Lumpur on 15 August

AiSP was invited to MBOT ENTICE 2023 at Hilton Kuala Lumpur on 15 August. Thank you Nurul Huda from Xcellink Pte Ltd and Minister of Science, Technology and Innovation YB Tuan Chang Lih Kang for visiting AiSP Booth. Thank you MBOT for inviting us to the event!



CYBER DSA on 16 August

AiSP was at Cyber DSA on 16 August at KLCC Convention Centre. Thank you BG Edward Chen, Cyber DSA for inviting AiSP. Big shoutout to our CPP Votiro for hosting us too!



SEACC Webinar on 23 August 2023


On 23 August, the second webinar leading up to the SEACC forum was held with our speakers sharing on cloud security. Thank you, AiSP Vice President, Tony Low and Ye Thura Thet from Myanmar Information Security Association (MISA), for sharing the insights with our attendees!

The screenshot displays a webinar interface with the following elements:

- Slide Content:**
 - Title:** Mitigation
 - Left Column:**
 - Threat Modelling
 - Assets
 - Adversaries
 - Attack Techniques
 - Mitigations
 - Right Column:**
 - Crypto mining
 - Ransomware
 - Data Theft
- Top Right Video Feed:** A man with glasses, identified as Ye MISA, speaking from a home office.
- Bottom Left Video Feed:** A promotional slide for the webinar titled "SEA CC Cloud Security" by Tony Low, dated 23 August 2023. It features a cityscape at night with glowing network lines and the AiSP logo.
- Bottom Right Video Feed:** A man with glasses, identified as Tony AiSP, speaking against a blue background with abstract network patterns.

Upcoming Event

Czechia – Singapore CyberSecurity Online Meetup on 19 September




AiSP
Advance Connect Excel

Czechia – Singapore CyberSecurity Online Meetup


CZECHIA - SINGAPORE
CYBERSECURITY ONLINE MEETUP

TUESDAY
19TH SEP 3PM - 5PM (SGT)


LIVE STREAM




Richard Kadlčák
Special Envoy for Cyber Space, Ministry of Foreign Affairs of the Czech Republic




David Čermák
CEO, Blindspot



Tesvin Choon
Senior Business Devt Manager, Cloud, Fortinet Singapore




Dr. Ondřej Ryšavý
Associate Professor, Faculty of Information Technology, Brno University of Technology




Dr. Yang Liu
Professor, Nanyang Technological University

Organised By



Supported By



AiSP, Embassy of the Czech Republic in Singapore, CzechTrade and CzechInvest Singapore bring together specialists from various fields of cyber security to share their knowledge of countering the ever-rising threat of cyber-attacks. The aim is to promote innovative solutions, engage inspiring professionals and build a united front against cyber threats. Our shared vision is to create a safer digital environment for individuals, organizations, and nations, ensuring the integrity, availability, and confidentiality of data and systems worldwide.

Welcome Words

Speaker: Richard Kadlčák, Special Envoy for Cyber Space, Ministry of Foreign Affairs of the Czech Republic

Collaborative Resilience: Strengthening National Defenses Against DDoS Threats

Speaker: David Čermák, CEO, Blindspot

With the increasing integration of digital technologies into all areas of society, distributed denial of service (DDoS) attacks pose a huge challenge to the security and reliability of critical infrastructure and other digital services. This presentation explores the broad spectrum of DDoS threats, their potential impacts, and the importance of national resilience. It also highlights the role of national policies and public-private partnerships in driving collective defense mechanisms.

This presentation provides a comprehensive overview of the DDoS threat landscape, emphasizing the importance of national resilience. It goes beyond the technological aspects of DDoS protection to discuss the role of state policies and public-private partnerships, offering a multifaceted perspective on the issue. It is designed to resonate with a wide audience, from technology professionals to policy makers, and aims to stimulate insightful discussions on enhancing national cybersecurity defenses. The talk subtly suggests the need for advanced DDoS mitigation solutions, setting the stage for potential follow-up discussions and engagements.

Top 5 Use cases for Securing Your Cloud Network

Speaker: Tesvin Choon, Senior Business Devt Manager, Cloud, Fortinet Singapore

Maintaining consistent, secure networking across the ever changing infrastructure in dynamic and hybrid world-spanning cloud and on-prem infrastructures is more critical than ever. Network connectivity, security, and operations all play a critical role in the organization. In this session, we will share secure networking use cases offered by Fortinet for cloud customers.

Enhancing Cloud Security: Leveraging Active and Passive Network Monitoring

Speaker: Dr. Ondřej Ryšavý, Associate Professor, Faculty of Information Technology, Brno University of Technology

The talk will present a network monitoring based method for cloud applications to quickly identify availability and performance problems. In the event of a problem, it will be possible to determine whether it is caused by a fault in the local network, on the application side, or in the service provider's network. This is achieved by integrating active and passive monitoring techniques into a unique hybrid monitoring solution. The method is being researched in a joint industry/academia project.

AI and DevSecOps

Speaker: Dr. Yang Liu, Professor, Nanyang Technological University

DevSecOps entails the systematic integration of security testing throughout all phases of the software development process. The objective is to automate the security expertise of human professionals by employing tools, thereby enabling early identification and resolution of security concerns during the early phase of the development life cycle. However, the effectiveness of DevSecOps greatly relies on the capabilities of intelligent tools to simulate or potentially replace security experts. With the emergence of Artificial Intelligence and Generative Computing (AIGC), a new means to accomplish this objective is now available. In this talk, I will discuss recent endeavors in utilizing AI within the realm of DevSecOps, specifically in the domains of Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Penetration Testing. Moreover, I will outline potential avenues for employing AIGC across diverse applications, including the construction of specialized large language models tailored to specific domains.

Date: 19 September, Tuesday

Time: 3PM – 5PM (SGT)

Venue: Zoom

Registration: https://us06web.zoom.us/webinar/register/4516916465206/WN_w7mx80ezTIW-mRH1UKAD8g

Corporate Partner Events

Cyfirma Webinar on 2 August

Working with our corporate partner CYFIRMA, AiSP has hosted the Cyber Intelligence Briefing on the topic: Defining Ransomware: Stages, Tactics, and Protection on 2 August. In today's digital landscape, the threat of ransomware looms larger than ever, and it's crucial to stay informed and prepared. Gain a better understanding of what is Ransomware, how it has evolved over the years, and more importantly, it's a time to adopt a more predictive, personalized, contextual, outside-in, and multi-layered insights to help you prepare against impending attacks.

Request for PowerPoint & Video [here](#)

What is ransomware?

- 'Ransomware' is a type of malware that attempts to extort money from a computer user by infecting and taking control of the victim's machine, or the files or documents stored on it.
- Typically, the ransomware will either 'lock' the computer to prevent normal usage, or encrypt the documents and files on it to prevent access to the saved data.



Cyfirma Webinar on 11 August

Working with our corporate partner CYFIRMA, AiSP has hosted the Cyber Intelligence Briefing on the topic: The Ransomware Trends in the First Half of 2023 where industry experts will share invaluable data points & insights to help you stay ahead of the curve. With the rising cyber-attack trend, traditional CTI is no longer effective; you need intelligence-driven predictive insights to enhance your cybersecurity protocols.

Request for PowerPoint & Video [here](#)

- MAJOR RANSOMWARE ATTACKS IN 2023
- THE TOP 5 MOST PROLIFIC RANSOMWARE FAMILIES SINCE JANUARY 2023
- GEOGRAPHICAL DISTRIBUTION OF RANSOMWARE FROM JANUARY 2023
- TARGETED INDUSTRIES
- INDUSTRIAL TRENDS ANALYSIS OF H1-2022 & H1-2023
- THE EVER-ADAPTING THREAT: ON-GOING EVOLUTIONS OF RANSOMWARE ATTACKS-H1 2023
- NOTABLE NEW RANSOMWARE GROUP IN 2023
- NOTABLE VULNERABILITIES THAT WERE EXPLOITED BY RANSOMWARE FROM THE BEGINNING OF 2023.
- TRENDS COMPARISON OF H1 2022 & H1 2023.

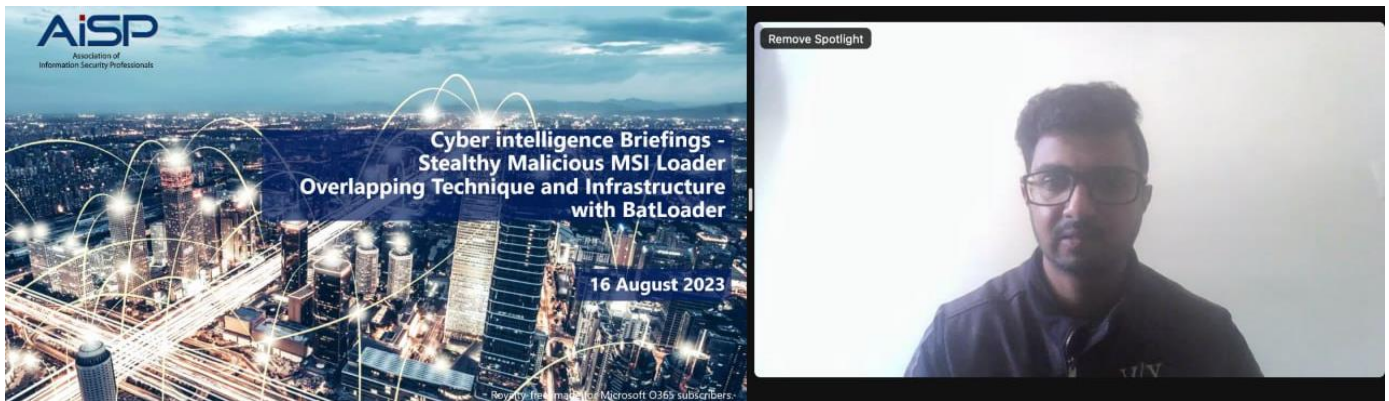


[back to top](#)

Cyfirma Webinar on 16 August

Working with our corporate partner CYFIRMA, AiSP has hosted the on the topic: Stealthy Malicious MSI Loader Overlapping Technique and Infrastructure with BatLoader, where the CYFIRMA Research team has recently discovered a disguised Stealthy MSI Loader being advertised in underground forums by Russian threat actors, showcasing its remarkable ability to evade detection by both Virus Total scan and Windows Defender.

Request for PowerPoint & Video [here](#)



Cyfirma Webinar on 30 August

Working with our corporate partner @CYFIRMA, AiSP has hosted on the topic: Singapore and Southeast Asia Threat Landscape, where we uncover trends in the SEA's threat landscape, covering nation-state and financially motivated APTs, phishing, and industry-specific threats with data-driven insights.

Request for PowerPoint & Video [here](#)



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



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 **4 Sep 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
6 – 7 Sep	ISMG's SEA Summit September	Partner
7 Sep	SEA CC Webinar – Ladies in Cyber	AiSP & Partner
8 Sep	AiSP x JTC x SIT PDD Event	AiSP & Partner
11 – 15 Sep	Overseas Learning Journey to Brunei	AiSP & Partner
12 Sep	Cisco Webinar: Well, That Escalated quickly: Prioritizing Alert to Minimize Impact	Partner
14 Sep	BCSA Conference	Partner
19 Sep	AiSP x CzechTrade Webinar	AiSP & Partner
20 Sep	SmartNation Webinar	AiSP & Partner
20 Sep	AiSP Knowledge Series – Red Team	AiSP & Partner
21 Sep	AiSP x BT x CSA x Grab CII Event	AiSP & Partner
26 Sep	AiSP x Huawei Scam Awareness event with MOS Sun Xueling	AiSP & Partner
27 Sep	Czech-Singaporean CyberSecurity Online Meet-Up	AiSP & Partner
28 – 29 Sep	Protect 2023	Partner
1 Oct	Learn Digital Carnival @ Bukit Panjang	Partner
5 – 6 Oct	Japan IC-AJCC	Partner
7 Oct	I'm Digital Ready@South West	Partner
10 Oct	LJ to Acronis for RP	AiSP & Partner
13 Oct	TCA 2023 Gala Dinner	AiSP
16 Oct	SEA CC Forum	AiSP
17 – 19 Oct	SICW/Govware	AiSP & Partner
25 Oct	Awareness Webinar for EY	Partner
28 – 29 Oct	DFL Festival – Kampung Admiralty	AiSP & Partner

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

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

Cloud Services, Digital Transformation & Security Transformation

Anthony Lim for AISP, with thanks to Fortinet.

Cloud services innovation, deployment and consumption are proliferating at a runaway rate today, for all the good reasons of opex cost management, storage, staging, business continuity, scalability, agility et al.

New services like FinTech, IOT, mobile apps, SD-WAN etc. all use the cloud infrastructure, and at the core of it, the datacenters, which host and run the storage, switches, networking, compute power, as well as the service reliability and robustness.

Digital transformation in the past several years have contributed significantly to the feverish adoption of cloud services (see the proliferation of cloud service provider and datacenters in the region) and the 2.5-years pandemic lockdown have accelerated this in no small way too, given the sudden need for work-from-home remote access, distributed computing, e-commerce and online order-delivery services of almost anything and everything.

Even when the lockdown has eased today, many organisations and staff continue to prefer a hybrid work model with partial (if not full still) WFH, thus continuing to feed to cloud services boom.

Digital transformation drives foundational change in how an organization operates, optimizes internal resources, and delivers value to customers. Cloud technologies provide the foundation for becoming more agile, collaborative, and customer-focused.

Digital transformation is when an organization takes advantage of new technologies to redesign and redefine relationships with their customers, employees, and partners. Digital transformation for business covers everything from modernizing applications and creating new business models to building new products and services for customers.

Organizations choose digital transformation frameworks as a way to reimagine themselves staying competitive in their respective businesses and industries.

There are security and governance concerns, primarily regarding data and availability, given that cloud is an outsourced model and the consumer tends to lose visibility and control.

[back to top](#)

Hence it is paramount to consider and comply with nationally and internationally established security and trust frameworks and certifications, such as from ISO, CSA and also some local ones from monetary authority, government, etc – as at least a next-best assurance and trust reference, that certain processes, policies and methodologies are in place to ensure the cyber security of the cloud services

As the drive towards digital transformation gathers momentum, this is an appropriate time for organizations to pause and reflect for a moment on their security strategies.

It's beyond doubt that the integration of digital technology into all areas of a business can result in fundamental changes to how businesses operate and how they deliver value to customers.

Technologies typically associated with digital transformation include SD-WAN, IoT, and Cloud, and the changes they're driving are quite revolutionary.

However, without an accompanying Security Transformation strategy, any Digi-Trans effort can fall apart.

This presents a complication as Digi-Trans efforts move more data and systems to the cloud, and cyberattacks grow more sophisticated.

So, what is Security Transformation and why should you care about it?

It is the integration of security into all areas of digital technology, resulting in fundamental changes to how security is architected, deployed, and operated.

At the same time, Sec-Trans is more than just technology – it's also about changing how teams work.

With the wide range of different technologies being adopted under the banner of DX, the different teams associated with key projects – applications, networking, and security – all need to work together to achieve a common goal: a successful and secure Digital Transformation.

To understand why Sec-Trans is so vital, consider the ever-changing security threat landscape and its potential impacts on Digi-Trans technologies like Cloud.

The majority of organizations have adopted a multi-cloud strategy, including multiple IaaS providers and over a dozen different SaaS solutions. The expansion of data and workloads into a distributed cloud environment makes consolidated security prevention and detection difficult.

They best need an integrated virtual and physical cloud solution that extend seamless security across the distributed cloud deployment, including being the first to provide advanced security solutions for all five of today's top cloud service providers.

In a multi-cloud environment, for example, there are many security issues to consider, including how to manage access to cloud services from remote users and branch offices, multiple cloud vendors using different cloud platforms, managing the new and constantly evolving applications and workflows that span different environments, and establishing and enforcing consistent security policies across various cloud platforms that each have their own native controls and interfaces.

This complexity makes it impossible to monitor what's happening across all the clouds, properly manage risk, address regulatory compliance, and maintain consistent security policies across both on-premise and cloud environments.

Likewise, connecting next-gen branch offices to today's more dynamic and fluid networks requires adopting a more dynamic and fluid approach to building wide area networks.

SD-WAN, for example, through internet and cloud services, enables branch offices to easily connect to all resources, whether on-premise in a central data center or in any of an organization's multi-cloud environments. The challenge however is that most SD-WAN solutions do not have the necessary security capabilities to adequately protect the branch office.

It's also important to understand that the range of different digital technologies associated with Digi-Trans bring with them a range of security risks that IT teams can't afford to view in isolation.

Traditional or incumbent network infrastructure cyber security solutions cannot just be simply extended or shoe-horned to cover cloud services.

The fact that cloud environments tend to use unique controls and services that make integrated visibility extremely difficult only makes the problem worse.

To address these and similar challenges, organizations need to, where possible, step back before deployment and assess the situation with all of its associated risks in order to develop a comprehensive security strategy.

There is a need for collaboration between disparate teams to achieve a common goal is the essence of Sec-Trans and is a cyber-security best practice approach.

Without this initial planning and the full recognition and acknowledgement of the risks that a Digi-Trans strategy can entail, Digi-Trans objectives cannot be fully realized – and in the worst case, the Digi-Trans initiative could, as alluded to earlier, even fail.

The best response to increasingly complicated networked environments is simplicity. That requires a security transformation that can keep pace with the digital one.

Security transformation, to recap, involves the integration of security into all areas of digital technology, resulting in a consistent and holistic security architecture that enables an effective security life cycle that spans across the entire distributed ecosystem of networks.

This includes identifying the attack surface, protecting against known threats, detecting unknown threats, rapidly responding to cyber events in a coordinated fashion, and providing continuous trust assessments.

An effective security transformation strategy needs to include collaborative intelligence and system integration so local and global threat intelligence can be shared between devices and responses can be coordinated between solutions; the orchestration of unified security policies and enforcement; intelligent segmentation across physical and virtual environments for deep visibility into traffic moving laterally across the network, even across multi-cloud environments, and to quickly identify and quarantine infected devices; and automation to sift through growing network noise, correlate threat information, and respond in real time to any threat found anywhere along the extended attack surface.

Also, organizations today choose digital transformation frameworks as a way to reimagine themselves staying competitive in their respective businesses and industries.

There are security and governance concerns, primarily regarding data and availability, given that cloud is an outsourced model and the consumer tends to lose visibility and control.

Hence it is paramount to consider and comply with nationally and internationally established security and trust frameworks and certifications, such as from ISO, CSA and also some local ones from monetary authority, government, etc – as at least a next-best assurance and trust reference, that certain processes, policies and methodologies are in place to ensure the cyber security of the cloud services.

Author Bio



Anthony Lim MAISP

Fellow, Cybersecurity, Governance & Fintech, Singapore University of Social Sciences
Advancing the Professionals | Connecting the Community | Excelling the Profession
[back to top](#)

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, DT Asia

The Anatomy of Active Directory Attacks

Active Directory, the Tier-Zero asset is a rich attack surface. Active Directory is the vital system of 95% of Fortune 1000 companies¹ that provides the essential authentication and authorization services that keep your IT ecosystem running. If compromised, an attacker or adversaries can gain control over organisation's Active Directory to give themselves access to any system, steal sensitive data or bring your business to a standstill. Surveys reported 51% of IT professionals are "not very" or "not at all" prepared for threats². Also, reported that over 80% of breaches involve brute force or the use of lost or stolen credentials³. Are you prepared?

To fully mitigate vulnerability is to understand attack vectors and methods. This article discusses the following: How exactly does an Active Directory attack unfold? What are the most common Active Directory attacks, and what steps can organizations take to mitigate their risk?

(A)The five stages of cyberattacks

Active Directory attacks follow the same five stages of any cyberattack: reconnaissance, planning, intrusion, lateral movement & privilege escalation, and exfiltration & cleanup.

1. Reconnaissance

Adversaries start by identifying target organizations and collecting information about them; what valuable data could they steal from a ransomware attack and the strength

[back to top](#)

of organization's security. Reconnaissance can involve using public sources such as tax records, job postings and social media to discover what systems and applications organization use, names of its employees, and so on. It can also involve network and port scanning to understand organization's network architecture, firewalls, operating systems, applications and services.

2. Planning

Next, the adversary determines which attack vector for infiltration. Examples include exploiting a zero-day vulnerability, launching a phishing campaign such as a business email compromise (BEC) attack, or even bribing an employee to provide credentials or deploy malware.

3. Intrusion

The adversary then uses the chosen attack vector to attempt to breach the organization's network perimeter. For instance, the adversary might succeed in guessing an employee's credentials by password spraying, credential stuffing or brute force attack; gaining entry through an unpatched or misconfigured system and even tricking employees to open malware hidden in attachments

4. Lateral movement & privilege escalation

Once an adversary has gained an initial foothold in the network, they will seek to escalate their privileges and compromise additional systems. They maintain their access by evading detection from system audits. Adversaries make sure they can get back using persistence techniques such as creating new user accounts, setting up PowerShell scripts and installing backdoors.

5. Exfiltration & cleanup

Lastly, the adversary exfiltrates or encrypts the organization's data. In addition, they often also use their privileged access to disable backups and cover their tracks in order to thwart investigations and prevent organization from enhancing defences against future attacks. Techniques include uninstalling programs or scripts used in the attack, deleting any folders or accounts that they tampered with.

(B) Common Active Directory attacks and defence strategies

Lateral movement and privilege escalation can exploit specific features of the IT ecosystem. These are the top 4 techniques used in Active Directory attacks.

1. Attack path mapping

The main goal for an adversary is to gain permissions in a high privileged Active Directory security group. Unfortunately, becoming a Domain Admin is far easier than it ought to be. Adversaries can use an open-source tool called BloodHound to identify Active Directory attack paths - chains of abusable privileges that could enable an attacker to gain administrative privileges. BloodHound provides hackers with a clear view of Active Directory attack paths. In many organizations, a very high proportion of ordinary user accounts offer an attack path that leads to Domain Admin rights.

Defence strategies

- minimize the attack paths available for hackers by identifying and mitigating them through attack path management using Active Directory attack path management software
- monitor any Active Directory attack paths using a real-time threat monitoring and change management solution.

2. Exploiting Group Policy

Group Policy is an extremely powerful Active Directory feature. Providing centralized management to users and computers called Group Policy objects (GPOs).

Administrators can use GPOs to Lock out accounts after certain number of incorrect passwords, block unidentified users and restrict use of command prompt. But like most powerful tools, Microsoft Windows Group Policy is a double-edged sword — by altering GPO settings, hackers can undermine a wide swath of your defences against lateral movement, privilege escalation and data theft. Once an attacker compromises a user account in your IT environment, they can use an open-source tool like BloodHound, PowerSploit or Mimikatz to review your GPOs and figure out which user accounts will provide them access to complete their Active Directory attack.

Defence strategies

To defend against Active Directory attack, you need effective Group Policy management. Pare the accounts with GPO access rights to bare minimum, and block changes to crucial GPO settings.

3. Pass the Hash attacks

Pass the Hash is an Active Directory attack that exploits the NTLM authentication protocol. This Active Directory attack enables an adversary to compromise AD accounts without cleartext passwords, all the hacker needs is the hash of the password — an encrypted version of the password that NTLM uses to authenticate users. Using a hacking tool like Mimikatz, they can use the password hash to send a logon request and respond to the domain controller's logon challenge. Attackers can easily harvest password hashes from the LSASS memory of system users.

Defence strategies

The clear-cut way to defend against Pass the Hash is getting rid of NTLM. However, many corporate applications still require NTLM, organizations often cannot simply disable it altogether. However, one could audit logon activity, limit attack path, use managed service accounts (MSAs), and restrict administrator access to their privileged accounts.

4. Kerberoasting

In a Kerberoasting attack, an adversary who compromised the credentials of a valid domain user can request a TGS(ticket granting server) for service such as SharePoint and attempt to crack the service account's password offline using a password-cracking tool such as Hashcat

Defense strategies

- Change the KRBTGT password on a regular schedule and whenever a person who had the ability to create Golden Tickets leaves your organization.
- Minimize the number of accounts that access the KRBTGT password hash.
- Don't give end users admin authority on their workstations

- Use MSAs to ensure that service account passwords are rotated on a regular basis.
- Invest in an Active Directory monitoring and protection solution that can spot activity indicative of these attacks and alert you immediately.

Conclusion

While this article details some of the top Active Directory attacks and offers strategies for defending against them, it's best not to take a piecemeal approach to Active Directory security. Remember that security is not a one-time configuration event but an ongoing process. With the threat landscape constantly evolving and IT ecosystems growing in complexity, it's wiser than ever to implement a thoughtful defence-in-depth strategy. A great way to get started is with the core best practices laid out in the blog post "[8 ways to secure your Active Directory environment](#)." A broad, defense-in-depth high-level Active Directory security goals are to:

- Minimize your attack surface area by cleaning up your Active Directory and keeping it orderly.
- Gain clear visibility into activity across your IT environment so you can promptly spot and respond to threats.
- Be prepared to recover from both accidental changes and full-on disasters to minimize their impact on the business.

Thereby helping you secure your Active Directory.

Contributor: Irving Oh
DTAsia Pte Ltd
irving@dtasiagroup.com
14August 2023

Adapted from Quest Software blog: **The anatomy of Active Directory attacks, Jason Morano**

[Active Directory attacks: Everything you need to know \(quest.com\)](#)

¹Offensive Active Directory 101 https://owasp.org/www-pdf-archive/OWASP_FFM_41_OffensiveActiveDirectory_101_MichaelRitter.pdf

²Who is responsible for Active Directory security within your organization? <https://www.helpnetsecurity.com/2019/11/06/active-directory-security>

³ Verizon 2020 Data Breach Investigations Report [2023 Data Breach Investigations Report | Verizon](#)

Article from Corporate Partner, Contfinity

Developing the Next Generation of Cybersecurity Talent : Interning at Contfinity



Nanyang Polytechnic students Hovan Cheng and Warren Gomes recently completed a three-month-long internship with Contfinity, Singapore's up-and-coming cybersecurity services provider and consultant. We spoke with them to find out what skills and knowledge they had acquired during the internship, what experiences had been most beneficial, and how they intend to follow through with what they have learnt as they embark on a future journey in this fast-growing and exciting space.

Can you share your overall impressions of interning at Contfinity?

Warren : We joined when Contfinity was celebrating our 2nd anniversary and looking ahead to an eventful and busy third year. As an SME, what Contfinity had achieved in two short years was remarkable, and this manifested itself in the wide network of partners the company had built up in the industry. This changed my view of SMEs. We also learnt about the history of the company from our seniors.

Hovan : The company may be young but the team of professionals helping the company come with decades of relevant experience. Working alongside them and through social conversations during lunch and non-work events enriched me in many ways, both in technical and non-technical areas.

How is learning at work different from learning in school?

Warren : The key difference is the hands-on experience we had during the internship. We got to interact with tech providers and brand principals to offer customers various cybersecurity products and solutions to meet their differing needs. Although we learned these products in school, having access to the actual dashboards to do configuration enabled us to understand them better. Furthermore, the company gave us opportunities to attend vendor courses to gain product knowledge and, in the process, we also earned certifications.

[back to top](#)

Hovan : Aside from the technical aspect, we sat in at meetings with prospective customers and observed how our superiors made persuasive sales pitches and close deals. We picked up useful tips on how to do presentations, how to speak and present oneself so as to be clear and concise in getting key points across, as well as observing customers and calibrating messages and style to suit the situation. Throughout the internship we were treated as one of the company's employees and this made us feel much at home.

Was there any major programme or initiative you were deeply involved in during your stay at Contfinity?

Hovan : Yes, definitely. Contfinity had been onboarded as a CSA-appointed consultant to provide CISO-as-a-service (CISOaaS) to SMEs under CSA's Cybersecurity Health Plan (CHP) programme, which comes with funding support. I had the opportunity to work with the team to brainstorm, develop communication plans, and implement marketing initiatives to promote the programme to our intended audience and prospective customers.

Warren : At the same time the corporate website needed to be updated with relevant information on CISOaaS. I worked closely with seniors to refresh the website with the latest content, in order to provide prospective customers with comprehensive information about CISOaaS.

Besides work what other activities did you participate in during the internship?

Hovan : CSR activities are very much part of Contfinity's DNA. During my stay here I participated in the Celebrate Digital @ East Coast Digital Festival event, where we helped spread awareness about the importance of practicing good cyber hygiene and staying cyber-secure. I also participated in various trade shows and a Cybersecurity Health Clinic, where our company promoted the CISOaaS programme to a big group of SMEs across multiple industries.

How will your time at Contfinity help you in your future?

Hovan : The internship made us more responsible and independent. Our boss and Contfinity founder Alex Chan regularly impressed on us the need to be proactive and to undertake our tasks diligently and responsibly. We also learnt to examine problems critically, ask the right questions, and think outside the box. More importantly, as we are young, we should learn and absorb as much as we can.

Warren : To add on, even though we should be as self-reliant as we can once we have received proper briefing on our tasks, if we run into difficulties or problems beyond our ability to solve, our supervisor and seniors will be there to guide and help us.

Hovan : The soft skills and words of wisdom that we acquired, aside from technical skills and experience, will certainly be beneficial in my future career.

For any enquiries, please contact Mr Raymond Lim at raymond.lim@Contfinity.com



Article from Corporate Partner, wizlynx group

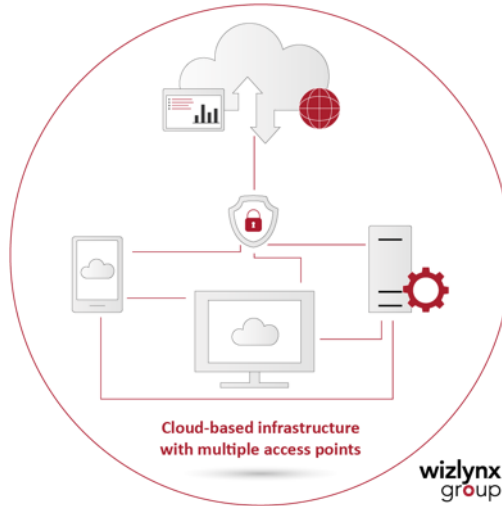
Zero Trust Framework: Bolstering Cloud Security in the Remote Work Era



In the rapidly evolving landscape of cybersecurity, where remote work and cloud computing have become integral to organizations, ensuring robust cloud security is of paramount importance. Traditional security models based on perimeter defense are no longer sufficient to protect sensitive data and critical assets. This article delves into the concept of Zero Trust Framework and its role in fortifying cloud security. As a subject matter expert, **wizlynx group** brings valuable insights to help cybersecurity professionals in the AISP community navigate the challenges of securing cloud-based infrastructure effectively.

What is the Zero Trust Framework?

Zero Trust is a security approach that emphasizes continuous verification and access controls for every user, device, and application trying to access resources organization's network, including cloud environments. Unlike the traditional castle-moat model, where trust was assumed inside the perimeter, Zero Trust assumes no trust and verifies all attempts to access resources, regardless of the user's location.



strict
within an
and-
once
implicit

Safeguarding Cloud Resources

In today's remote work era, cloud resources are accessible from various entry points, increasing the attack surface. Implementing Zero Trust principles is crucial to ensure that only authorized users and devices gain access to sensitive data and applications within the cloud infrastructure. By utilizing multi-factor authentication, identity and access management tools, and encryption protocols, organizations can strengthen their cloud security posture and mitigate potential risks.

Adopting a Risk-Based Approach

To effectively apply Zero Trust principles to cloud security, organizations must adopt a risk-based approach. This involves continuously assessing the risk associated with every user, device, and application attempting to access cloud resources. Machine learning and behavioral analytics can help in identifying anomalies and potential threats, enabling security teams to respond proactively and prevent data breaches.

Zero Trust in IoT: A Synergistic Approach

As the Internet of Things (IoT) becomes ubiquitous, integrating Zero Trust with IoT security is imperative. IoT devices are often vulnerable entry points for cyberattacks, and applying Zero Trust principles can enhance their protection. By continuously verifying the identity and security posture of IoT devices, organizations can maintain a secure environment for IoT data transmission and prevent unauthorized access.

Building Resilience against Evolving Threats

In the dynamic landscape of cloud and IoT cybersecurity, threat actors are continually evolving their tactics [link: <https://www.wizlynxgroup.com/news/cyber-security-threats-and-solutions/>]. To stay ahead, cybersecurity professionals must have access to timely and relevant threat intelligence.

As the AiSP community focuses on empowering Special Interest Groups (SIGs) in Cloud Security (CS) and Internet of Things (IoT) domains, understanding and implementing the Zero Trust Framework is instrumental in bolstering cloud security.

wizlynx group [link: <https://www.wizlynxgroup.com/news/what-does-wizlynx-group-do-a-beginners-guide-to-our-cyber-security-solutions/>], a recognized Cyber Security Partner, offers invaluable expertise and solutions to help organizations safeguard their cloud resources and protect against ever-evolving cyber threats. By embracing Zero Trust principles and integrating them with cloud security and IoT domains, AiSP members can build a resilient cybersecurity foundation for the future. For more information, visit **wizlynx group**'s website and explore our domain expertise in securing cloud-based environments and beyond. Together, let's fortify our defenses and ensure a safer digital ecosystem for all.

For any enquiries, please contact info@wizlynxgroup.com

Article from Cloud Security Summit Sponsor, Parasoft

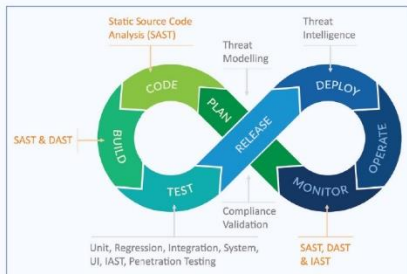
Compliance is a Pain! I need a painkiller



Compliance is a pain! I need a painkiller.

Software development is no longer just about writing code and making applications work. In many industries and systems, the expectation is that the application must also be safe, secure, stable, and scalable. In fact, there are countless pages of compliance standards that define what should and shouldn't be done when we develop applications. And now, they want us to do it faster and have less errors! It's no longer fun.

But such compliance standards can sometimes become painful for the application teams! Imagine having to spend hours to remediate a coding error by tracing the origin of an error. Or trying to find ways to scale up the tests to ensure that a higher number of users will be able to use the system without it crashing or experiencing slow response times. All this adds to the delay in deploying the software. And ultimately to the failure to recoup the costs for building the software. This might lead misguided developers or project managers to find ways to circumvent such compliances and worse still, ignore them. This may lead to detrimental outcomes.



But that is the challenge in the modern world where most of our devices, systems, and government is run on software. Whether it's a mobile device or a vehicle or the distribution of electricity, it's all driven by the humble application that is built from the ground up with code. And for instances of safety and security critical software, certain levels of compliance and certification are required. Hence, the headache increases with complexity.

Take, for examples, the automotive, aeronautics, and medical device industries where software failure could cause loss of life. Organizations cannot leave it to chance that the software for brakes or flight instrumentation might fail while in use. Or the possibility that a medical device suddenly stops working because of a software bug. All of these scenarios have played out in real life. And in the financial industry, a life may not be at risk, but arguably as important is ensuring that no glitches exist that cause money to be transferred incorrectly.

As such, compliance standards are provided to ensure safety, security, reduce risk, and manage the consistency so that we can go about our lives without too much stress or worry. ISO 26262, MISRA, AUTOSAR, and UL 4600 are standards

that provide development teams a compliance framework to work on for the automotive industry. OWASP, SEI CERT, CVE are standards used for security and vulnerability analysis across industries. Many of these standards are there to help identify the problems early in the developmental phase before it becomes a bug that would cause more pain after the application has been deployed.

With Agile and DevOps methodologies as well as CI/CD pipelines, we need to update and shift left in the development and quality life cycle. Leveraging on the prevalence of containers and using the various quality processes and standards, you can automate and integrate the processes of static code analysis, unit testing, coverage analysis, functional testing, load testing, penetration testing and regression testing into the compliance requirements. In this way, the safety, security, and stability of the application is built into the processes rather than done as an afterthought.

Finally, to manage the pain, an overview of the performance of the development can help teams understand their roles better and provide training for the new developers to integrate them into the team. We find that giving the tools to the various teams is not sufficient. Understanding the rationale and the buy-in from the teams on why compliance is needed and how to make it easier for them to do their job would make life a lot easier for all concerned.



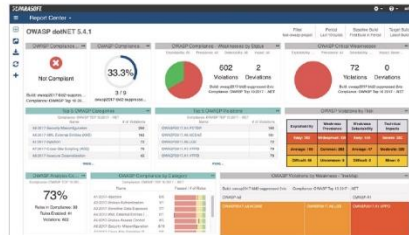
At Parasoft, we believe the success depends on more than the products and tools in use. Just as important is aligning the people, processes, and policies to support the push to make software compliant, high quality, and satisfy certification needs. In this way, the desire to do well permeates from the management team all the way to the project managers, developers, testers, and end users.

Parasoft has assisted organizations developing software in many industries to establish auditable quality processes that include complete visibility into compliance efforts. For more information about how to deploy Parasoft's complete software development management platform as well as the tools for compliance and quality testing, visit www.parasoft.com.

Contact us to find out how our painkillers can work for you and your team.

ABOUT PARASOFT

Parasoft helps organizations continuously deliver quality software with its market-proven, integrated suite of automated software testing tools. Supporting the embedded, enterprise, and IoT markets, Parasoft's technologies reduce the time, effort, and cost of delivering secure, reliable, and compliant software by integrating everything from deep code analysis and unit testing to web UI and API testing, plus service virtualization and complete code coverage, into the delivery pipeline. Bringing all this together, Parasoft's award-winning reporting and analytics dashboard delivers a centralized view of quality enabling organizations to deliver with confidence and succeed in today's most strategic ecosystems and development initiatives—security, safety-critical, Agile, DevOps, and continuous testing.



For Parasoft South East Asia:
60 Albert Street
#09-08 OG Albert Complex
Singapore 189969
Tel: +65 6338 9628
Fax: +65 6297 7597
For **ASEAN** inquiries: info-sg@parasoft.com
For Parasoft Corporation, USA:
101 E. Huntington Drive
Second Floor
Monrovia, CA 91016 USA
Within the US: +1 626 305 0041
International: +1 626 305 9048
Fax: +1 626 305 9048
For all inquiries: info@parasoft.com

For any enquiries, please contact Ms Ismaliah at admin-sg@parasoft.com

Article from SVRP 2022 Winner, Claudia Chan



Although I couldn't attend the award ceremony, the news of receiving the SVRP Gold Winner award in 2022 filled me with gratitude. This award holds deep meaning for me, reminding me that the time and dedication I invested in supporting the community were recognized. This recognition highlights the value of my efforts and motivates me to continue making a positive impact.

My journey into the realm of cybersecurity began during my time at Singapore Polytechnic, where I studied in the Infocomm Security Management course. In my first year, a pivotal moment arose when I participated in an internal Capture-The-Flag (CTF) competition organized by the Special Interest Group in our course.

As a newcomer, the challenges posed by the CTF competition felt extremely challenging. The complexity of the questions left me both curious and bewildered. However, I was fortunate to have a supportive network of senior peers who generously provided guidance and advice after the competition concluded. Their encouragement not only propelled me to engage in more CTFs but also sparked a deep interest in the cybersecurity and penetration testing domain.

As time went on, my fascination with cybersecurity grew exponentially. I wholeheartedly engaged in numerous CTFs and pursued various educational courses, driven by a thirst for knowledge and skill acquisition. This journey nurtured a genuine passion within me, motivating me to continuously learn and develop in the cybersecurity field.

However, my aspirations extended beyond personal growth. I held a strong desire to contribute significantly to the broader cybersecurity industry. My ultimate aim is to offer aspiring individuals the guidance and direction needed for their success.

In my perspective, mentorship encompasses more than just knowledge transfer – it involves building a sense of community and fostering an environment conducive to

growth. My ultimate goal is to nurture the upcoming generation of cyber professionals who play a pivotal role in safeguarding the nation's digital landscape for years to come.

Moreover, being a woman in a predominantly male-dominated tech industry brings its own set of challenges. Nonetheless, I am determined not to let these challenges define my journey. My aspiration goes beyond inspiring fellow women – I actively strive to encourage their participation in the cybersecurity community. By showcasing our capabilities and resilience, we can start a positive shift towards increased diversity in the industry.

In conclusion, my journey from a curious student to an advocate for cybersecurity illustrates how discovering your true passion can lead to transformative experiences. My commitment to continuous learning, mentoring, and overcoming gender biases emphasizes the potential within each of us to drive positive change. In the ever-changing landscape of technology, it is my sincere hope that every individual plays their part in fostering a brighter and safer cyber future for all.

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 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 to let us know what courses you are interested in.

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

Thank you.

The ALC team



ALC Training Pte Ltd

3 Phillip Street, #16-02 Royal Group Building, Singapore 048693

T: (+65) 6227 2883 | E: learn@alctraining.com.sg | www.alctraining.com.sg

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

Qualified Information Security Professional (QISP®)

BUNDLE PROMOTION VALID TILL 30 SEPTEMBER 2023

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 promotional banner features the AiSP logo at the top right. The main headline reads "Limited Time Promotion for QISP Exam and BOK Book!" in a dark purple font, with a sub-headline "While stocks last! till 30 September 2023" below it. The central focus is the cover of the "IS-BOK 2.0 INFORMATION SECURITY BODY OF KNOWLEDGE" book, which is published by AiSP and edited by Alex Lim Wee Meng, Prof Steven Wong Kai Juan, and Samson Yeow. The book cover shows two padlocks, one blue and one red, with a keyhole. To the right of the book cover is a QR code with the text "PAY NOW" overlaid. Below the QR code, it says "Scan the QR code here to make the payment". At the bottom of the banner, the price is listed as "\$216 inclusive of GST" and "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 with your screenshot receipt and we will follow up with the collection details for the BOK book. Limited stocks available.

Promotion is valid until **30 September 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



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

MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

If you are currently a full-time student in the IHLs that are onboard of our [Academic Partnership Programme \(APP\)](#), AiSP is giving you complimentary Affiliate Membership during your course of study. Please click [here](#) for the application form and indicate your student email address, expected graduation date and name of your institution in the form.

Complimentary Affiliate Membership for NTUC Members

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2023) from 1 Jan 2023 to 31 Dec 2023. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. [This does not include Plus! card holder \(black-coloured card\), please clarify with NTUC on your eligibility.](#)

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

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

CPP Membership



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

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

For any enquiries, please contact secretariat@aisp.sg

AVIP Membership

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

Membership Renewal

Individual membership expires on 31 December each year. Members can renew and pay directly with one of the options listed [here](#). We have GIRO (auto - deduction) option for annual auto-renewal. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.

Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!

Please check out our website on [Job Advertisements](#) by our partners.

For more updates or details about the memberships, please visit

www.aisp.sg/membership.html

AiSP Corporate Partners



Acronis



ASUS



bugcrowd



CLIXER



[back to top](#)





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

AiSP Academic Partners



Our Story...

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

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

Our Vision

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

Our Mission

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

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

AiSP Secretariat Team



Vincent Toh
Associate Director



Elle Ng
Senior Executive



Karen Ong
Executive



www.AiSP.sg



secretariat@aisp.sg



+65 8878 5686 (Office Hours from 9am to 5pm)



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

Please [email](#) us for any enquiries.