

Content Page

News & Update

- SVRP
- AiSP Cyber Wellness
- Special Interest Groups
- The Cybersecurity Awards
- Regionalisation
- Digital For Life
- Corporate Partner Event
- CREST
- Upcoming Events

Contributed Contents

- CISO SIG: Introducing CISO with a deep interest in cybersecurity
- LITE SIG: Legal Investigative Technology Experts (LITE), formerly known as High Technology Crime Investigation Association (HTCIA)
- DevSecOps SIG: Putting the 'Sec' in DevSecOps: Emphasizing White Box Testing and End-to-End Security
- APP: ITE Work Study Diploma Programme
- SVRP 2023 Gold Winner, Kek Jun Kai

Professional Development

Membership

Member Acknowledgment

Interview with AiSP Vice President Mr Andre Shori



What is your vision for your contribution in AiSP? What do you think is the biggest issue in the Cybersecurity Industry?

My vision for my contribution to AiSP is to catalyse the senior cybersecurity leadership community towards building a sustainable and trusted ecosystem that elevates the overall maturity and resilience of cyber defenders in Singapore and the wider region. This ecosystem will not only facilitate networking and socializing but also provide crucial support to one another.

The biggest issue in the Cybersecurity Industry, in my opinion, lies in the current operational silos that hinder the exchange of vital strategic and operational information among cybersecurity leaders. By fostering an informal yet trusted network of leaders willing to share critical information, especially during crises, we aim to disrupt threat actors' ability to repeatedly exploit the same attacks.

As the EXCO member, there are times where you will be representing AiSP in events and engagements. How do you plan to uphold AiSP's reputation and values while effectively communicating its mission and objectives to external stakeholders?

As an EXCO member, my commitment is to uphold AiSP's reputation and values while effectively communicating its mission and objectives to external stakeholders. Our values, encapsulated in our AiSP initiatives graphic, including our Vision and Mission, provide a solid foundation. By aligning our activities with the key pillars of Advance, Connect, and Excel, we can clearly and easily communicate our objectives to all stakeholders.

Lastly, what would you like to share and contribute your expertise with our AiSP member and the wider community?

I am deeply grateful for the invaluable support and encouragement I have received from the cybersecurity community throughout my career. Many cybersecurity professionals have generously contributed to my personal and professional growth. As a

result, giving back to the community has become a lifelong commitment for me. I am dedicated to ensuring that I continue to pay it forward and contribute my expertise to support AiSP members and the wider community.

Student Volunteer Recognition Programme (SVRP)

AiSP Youth Symposium on 7 July



AiSP Youth Symposium 2024

Date: 7 July 2024
Venue: JustCo @ Marina Square
Time: 1PM - 4PM

IN SUPPORT OF:
DIGITAL FOR LIFE PLAY IT FORWARD

SUPPORTING PARTNERS:
ISACA SINGAPORE NYC
Singapore Computer Society SINDA associate
MESPAKI young nite

ACADEMIC PARTNERS:
NUS ngee ann polytechnic REPUBLIC POLYTECHNIC
SIT Singapore Polytechnic SMU
SUSS Temasek

ORGANISED BY:
AiSP
Advance Connect Excel

SUPPORTING AGENCIES:
CSA SINGAPORE
Cyber Security Agency of Singapore

SPONSORED BY:
EC-COUNCIL
Endorsing: S@f@re by WISSEN

YesWeHack




OPPORTUNITIES FOR YOUTHS TO DEVELOP YOUR PASSION AND SKILLS IN CYBERSECURITY

This presentation will give an overview of the training and education programmes to prepare our youths for a future career in cybersecurity.



Mr Wong Choon Bong | Director (SPO&W), Ecosystem Development, Cyber Security Agency of Singapore





BUILDING A CYBERSECURITY CAREER: FROM INTERNSHIPS TO LEADERSHIP


Are you ready to take the first step towards an exciting and rewarding career in cybersecurity? We are thrilled to invite you to an enlightening presentation at the upcoming Youth Symposium, titled 'Building a Cybersecurity Career: From Internships to Leadership.'

Join us as representatives from EC-Council to explore the dynamic world of cybersecurity and discover how you can build a successful career from the ground up. This presentation will provide you with valuable insights and practical tips on:

- Starting Strong
- Certifications and Training
- Networking and Mentorship
- Career Progression
- Real-World Success Stories

Whether you're a student in a ITE, Polytechnic or University, this presentation will equip you with the knowledge and tools you need to embark on a fulfilling cybersecurity career. Don't miss this opportunity to unlock your potential and take the first step towards becoming a sought-after professional in this rapidly evolving industry.

**Ms Judy Saw | Strategic Partnerships,
Director, Wissen International**





YESWEHACK DOJO: LEARNING AND EXPLOITING VULNERABILITIES TO MASTER FUNDAMENTALS IN WEB APPLICATION SECURITY

Discover DOJO, a free educational platform by YesWeHack focusing on beginner-friendly interactive challenges that simulate real-world web infrastructures, with the goal of helping students master web application security. DOJO supports aspiring hunters in learning about and exploiting real vulnerabilities, allowing them to develop fundamental skills for success in cybersecurity.

**Ms Anne-Laure Ehresmann | APAC
Lead Security Analyst, YesWeHack**



As part of Singapore Youth Day 2024 on 30 June 2024 (Sun), AiSP will be organising the 3rd Youth Symposium to reach out to the Youths for a day of sharing, internship or career opportunities with our partners on 7 Jul 2024 (Sun).

We are expecting 100 Youths and professionals (Subject to COVID restrictions) for the Symposium in this Physical Event. AiSP Patron - Senior Minister of State, Ministry of Communications and Information & Ministry of National Development Mr Tan Kiat How will be gracing the event as our Guest of Honour and have a dialogue session with the attendees on the theme "Guardians of the Digital Realm: Empowering Tomorrow's Cyber Defenders".

Event Date: 7 July 2024

Event Time: 1PM – 4PM

Event Venue: JustCo @ Marina Square

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.

*First 80 Youths that sign up and attend will receive Suntec Vouchers



Nomination Period:
1 Aug 2023 to 31 Jul 2024

CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

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



Scan the QR Code for
the Nomination Form

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

- + Skills-based: E.g. Conduct cybersecurity workshops or develop related software
- + Events-based: E.g. Provide support at technology or cyber-related events
- + Leadership: E.g. Mentoring younger students and managing teams or projects

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



Nomination Period:
1 Aug 2023 to 31 Jul 2024

CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

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

Example A

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

Example B

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

Example C

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

Example D

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



Scan the QR Code for
the Nomination Form

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

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

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

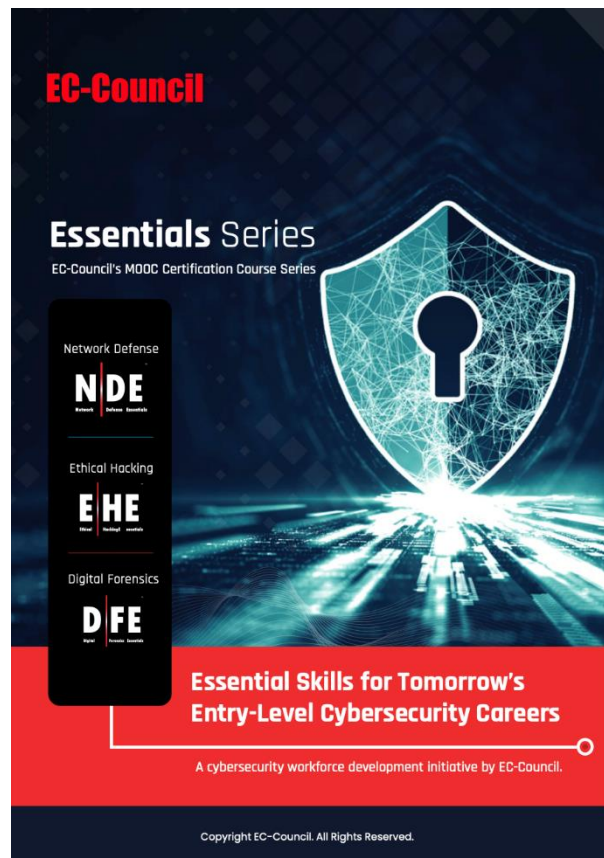
Elevating Cybersecurity Education Through Unprecedented Collaborations

In a pioneering initiative, EC-Council and Wissen have forged a collaboration with AiSP. This collaboration includes a sponsorship of 500 EC-Council Cyber Essentials certification vouchers. These vouchers aim to empower Polytechnic and Institute of Technical Education (ITE) students pursuing cybersecurity programs, enabling them to attain their inaugural industry certificate and commence their journey with EC-Council Essential certificates (NDE, EHE, DFE), thereby initiating their cybersecurity credentialing process.

Visit (<https://wissen-intl.com/essential500/>) and register to start your cybersecurity credentialing journey! Terms & Conditions apply.

About the EC-Council Cyber Essentials Certification

EC-Council's Essentials Series is the first MOOC certification course series covering essential skills in network defense, ethical hacking, and digital forensics. The Network Defense Essentials (N|DE), Ethical Hacking Essentials (E|HE), and Digital Forensics Essentials (D|FE) are foundational programs that help students and early career professionals choose their area of competency or select a specific interest in cybersecurity. The Essentials Series was designed to give students the foundation on which to build and develop the essential skills for tomorrow's careers in cybersecurity. These programs educate learners in a range of techniques across industry verticals, such as securing networks, mitigating cyber risks, conducting forensic investigations, and more.



AiSP Cyber Wellness Programme

Organised by:



Supported by:



INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY

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!

Special Interest Groups

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

- Artificial Intelligence
- CISO
- Cloud Security
- Data and Privacy
- DevSecOps
- LITE

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



AiSP CISO SIG Meetup on 5 June

AiSP organised our CISO SIG meetup hosted by our Corporate Partner, Schneider Electric on 5 June. Our Vice President and CISO SIG EXCO Lead Mr Andre Shori facilitated a discussion on “What is the definition of a CISO in Singapore?” with more than 20 attendees.



AiSP LITE SIG Meetup on 27 June

On 27 June, AiSP organised our very first LITE SIG Meetup. Legal Investigative Technology Experts (LITE), formerly known as High Technology Crime Investigation Association (HTCIA) was formed to provide education and collaboration within AiSP for the prevention and investigation of high-tech crimes.

AiSP LITE SIG EXCO Lead, Mr Daniel Wang, did a sharing on what the LITE SIG is about, AiSP Fellow Member & Director, Mr Freddy Tan, shared insights on AiSP and AiSP Vice President Mr Breyvan Tan, did a sharing on AiSP Special Interest Groups.

Interested AiSP Members can contact secretariat@aisp.sg to join the SIG.



AI Security Summit on 3 July

ORGANISED BY:

AiSP
Advance Connect Excel

SUPPORTING AGENCY:

CSA
SINGAPORE
Cyber Security Agency of Singapore

SUPPORTING PARTNERS:














AiSP

AI SECURITY SUMMIT 2024

Date: 3 July 2024
Venue: Marina Bay Sands Convention Centre
Time: 8.30Am - 2.30PM

ORGANISED BY:

AiSP
Advance Connect Excel

PLATINUM SPONSOR:

FORTINET

GOLD SPONSOR:

CISCO

SILVER SPONSORS:

SailPoint

softScheck
— We Build Trust —



AI IN CYBERSECURITY

Artificial Intelligence (AI) is revolutionizing cybersecurity, offering advanced tools and techniques to defend against increasingly sophisticated threats. Today, cyber attackers are leveraging AI to enhance their strategies, automating attacks, and developing more complex malware. Besides the use of AI for phishing, one of the pressing concerns is machine learning poisoning, where attackers manipulate training data to corrupt AI models, leading to vulnerabilities and breaches. As we look to the future, AI holds immense potential to transform cybersecurity, enabling proactive threat detection, adaptive defenses, and robust responses to evolving cyber threats. However, it also necessitates continuous innovation to stay ahead of malicious actors who are equally eager to exploit AI for their gain.




JONAS WALKER
DIRECTOR FOR THREAT INTELLIGENCE APAC & MIDDLE EAST
FORTINET

AI SECURITY: WHAT YOU MUST URGENTLY KNOW!

AI will be deployed pervasively but unfortunately, they are also inherently fragile and are prone to robustness and data related attacks. Hence, we will need Cybersecurity for AI, i.e. how to Red-Team AI and measure their reliability, resiliency and resistance against new AI attacks. Due to AI's rapid advancement, our defensive architecture would have to be as dynamic as the attacks, and the time to worry is now, because AI legislation are being rolled out, as we speak. Starting now, AI will enter most enterprises and smart cities progressively, automating and powering business workflows and CII operations. In a short time, AI systems will become the brains of the company and will run the Smart City. If such AI systems were hacked, our safety and national security will be undermined. Thus, new government regulations will be enacted to ensure the integrity, security and accuracy of key AI systems. In addition, safeguards for disinformation and Deepfakes will have to be also implemented. Hence, this presentation will cover how AI could be defended and how to use AI to protect AI; AI for Cybersecurity using several case studies.

In gist, weaponizing artificial intelligence (AI) to attack understaffed small enterprises that lack AI expertise, is giving cyber criminals the edge in the ongoing cyberwar. APT threat actors will also have a significant advantage over most large enterprises because they can innovate at a faster speed and could overrun the defenders by agilely altering their offensives in real time. This will be the next game for the next level of cybercrime, since criminals are already exploiting AI deception scamming Deepfakes.

For national security, a key concern would be massive, directed attacks on the AI cores of banks, autonomous vehicles, and the emerging smart city systems, which will be critical information infrastructures (CII). Stronger Smart Nation leadership will be needed to overcome the known shortfalls urgently. Concluding, the presentation will highlight a guidance framework for AI security, based on Security by Design, the MITRE ATLAS framework and on secure AI applications development.

INNOVATING FOR A NEW ERA OF SECURITY

In an era where cyber threats are becoming increasingly sophisticated and multifaceted, organizations must strive to stay ahead of technology changes, protect their business ecosystem and maintain trust with their customers. In this session we will delve into the current threat landscape and how Cisco is leveraging AI to support organizations in achieving their security objectives and keep threats at bay.



PROF YU CHIEN SIANG
CHIEF INNOVATION AND
TRUST OFFICER
AMARIS AI



TIMOTHY SNOW
REGIONAL LEAD APJC,
CYBERSECURITY
ENGINEERING
CISCO SYSTEMS

A ROAD TOWARDS AN INTERACTION BETWEEN CYBER SECURITY AND AIGC

AIGC and cyber security 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, its effectiveness greatly relies on the capabilities of intelligent tools to simulate or potentially replace security experts. With the emergence of LLM, a new means to accomplish this objective is now available. In this presentation, I will discuss recent endeavors in utilizing LLM within the realm of application security, to cover the complete life cycle of the vulnerability analysis: vulnerability detection, diagnosis, POC generation and repair.

On the other hand, LLM's security is equally important to make sure the successful deployment of the AI applications. In this direction, we will demonstrate the latest research works regarding the attack surface of LLM, blackbox/whitebox attack generation for prompt injection, attacks for multi-modality models, backdoor attacks, and possible defense mechanism. Finally, we are looking at the integration of the two aspects to develop an AI-enabled platform for application security analysis.



DR LIU YANG
EXECUTIVE DIRECTOR OF CYBER
SECURITY RESEARCH CENTRE @ NTU
NANYANG TECHNOLOGICAL
UNIVERSITY

NAVIGATING THE CYBER RISKS OF AI

As AI matures and becomes more deeply integrated into our businesses and personal lives, it introduces new attack surfaces that demand robust security measures. Meanwhile, adversaries are leveraging AI to bolster their cyber operations, presenting significant threats to our digital landscape. In this presentation, we will touch on the security of AI systems, exploring the current AI-enabled threats to the digital domain, and discuss strategies for defending against them.



DAN YOCK HAU
ASSISTANT CHIEF EXECUTIVE
(NATIONAL CYBER RESILIENCE)
CYBER SECURITY AGENCY OF SINGAPORE



NAVIGATING RISK, SECURITY AND GOVERNANCE OF AI



Wally Lee

Advisor to EXCO
& AI SIG Member
AiSP



Dan Yock Hau

Assistant Chief Executive
(National Cyber
Resilience)
Cyber Security Agency of
Singapore



Dr Liu Yang

Executive Director of
Cyber Security Research
Centre @ NTU
Nanyang Technological
University



Jonas Walker

Director for Threat
Intelligence APAC &
Middle East
Fortinet



Prof Yu Chien Siang

Chief Innovation and Trust
Officer
Amaris AI

In an era defined by rapid digital transformation and evolving cyber threats, the integration of Artificial Intelligence into the realm of cybersecurity has become not just a necessity but a strategic imperative. From machine learning algorithms that detect anomalies in network traffic to autonomous response systems that thwart sophisticated attacks in real-time, AI holds immense promise in fortifying our defenses against an ever-expanding array of cyber threats. At the same time, as organizations increasingly rely on AI to enable their business and safeguard their digital assets, the security and ethical implications of AI deployment loom large. The conference aims to help Enterprises, SMEs and individuals to be more aware of practical usages of AI in securing their digital assets as well as considerations to better governance their AI-based solutions.

Our theme for this year summit is "AI for Cybersecurity and Cybersecurity for AI".

Organized by the Association of Information Security Professionals (AiSP), the AiSP AI Security Summit is a unique event that delves into the critical intersection of artificial intelligence and cybersecurity. Our distinguished speakers from public, private and academia sectors will share audience on the innovative applications of AI in safeguarding digital asset and addressing the imperative of securing AI system themselves, tackling issues of adversarial attacks, data privacy and ethical consideration.

Event Date: 3 July 2024

Event Time: 8:30AM – 2.00PM

Event Venue: Marina Bay Sands Convention Centre

Guest of Honour: Senior Minister of State, Ministry of Communication and Information - Dr Janil Puthucheary

Click [here](#) to register.

*AiSP AVIP & Ordinary members can email to rsvp@aisp.sg for complimentary tickets. Please noted that it is based on first come first served basis.

Data & Privacy Workshop on 24 July

AiSP
Advance Connect Excel

Data & Privacy Workshop

Data Protection in an AI-powered World

24 July 2024 1.30PM - 6PM

JustCo @ Marina Square

SAVE THE DATE

Exclusive Sponsor

opentext™

opentext™

FINANCIAL RISKS FROM UNSTRUCTURED DATA & AI PRIVACY

Organisations expanding across borders has strategic business imperatives to build trust with customers and partners. Compliance with various privacy regulations is critical to facilitate a sustainable, long-term business success. With complexity compounded by urgent need to grow with the rise of AI-enabled offerings, how are organisations managing data trust to support corporate objectives downstream?

While it is critical to understand the risks of unstructured data and impact on AI Privacy amidst speed to innovations, organisations need to revisit how privacy is a catalyst for growth. We will explore how privacy-enhancing technology such as Data Discovery, Data Minimization, and Data Classification help organisations prepare to comply with global regulations, and to maintain data integrity and security of their operations for growth.

Eugene Teh, Director, Data Privacy & Protection - SEA, OpenText Cybersecurity

In the age of artificial intelligence, the integration of Generative AI (GenAI) and Large Language Models (LLMs) into various sectors has revolutionized how organizations operate. However, this technological advancement also brings with it significant data protection challenges. This event aims to explore these challenges and provide actionable insights for managing data protection in an AI-powered world.

Organized by the Association of Information Security Professionals (AiSP), the AiSP Data & Privacy Workshop is a unique event that delves into the critical intersection of Data & Privacy

Our theme for this year summit is “Data Protection in an AI-powered World”.

Event Date: 24 July 2024
Event Time: 1.30PM – 6PM
Event Venue: JustCo @ Marina Square

Click [here](#) to register.

*AiSP Members can key in "AiSPXXXXX" (where XXXXX is your membership number) for complimentary tickets

**email secretariat@aisp.sg if you have any queries

The Cybersecurity Awards



Thank you for your support! The Cybersecurity Awards 2024 nominations ended on 31 May.

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 2024! Limited sponsorship packages are available.



ORGANISED BY



SUPPORTED BY



SUPPORTING ASSOCIATIONS



PLATINUM SPONSORS



GOLD SPONSORS

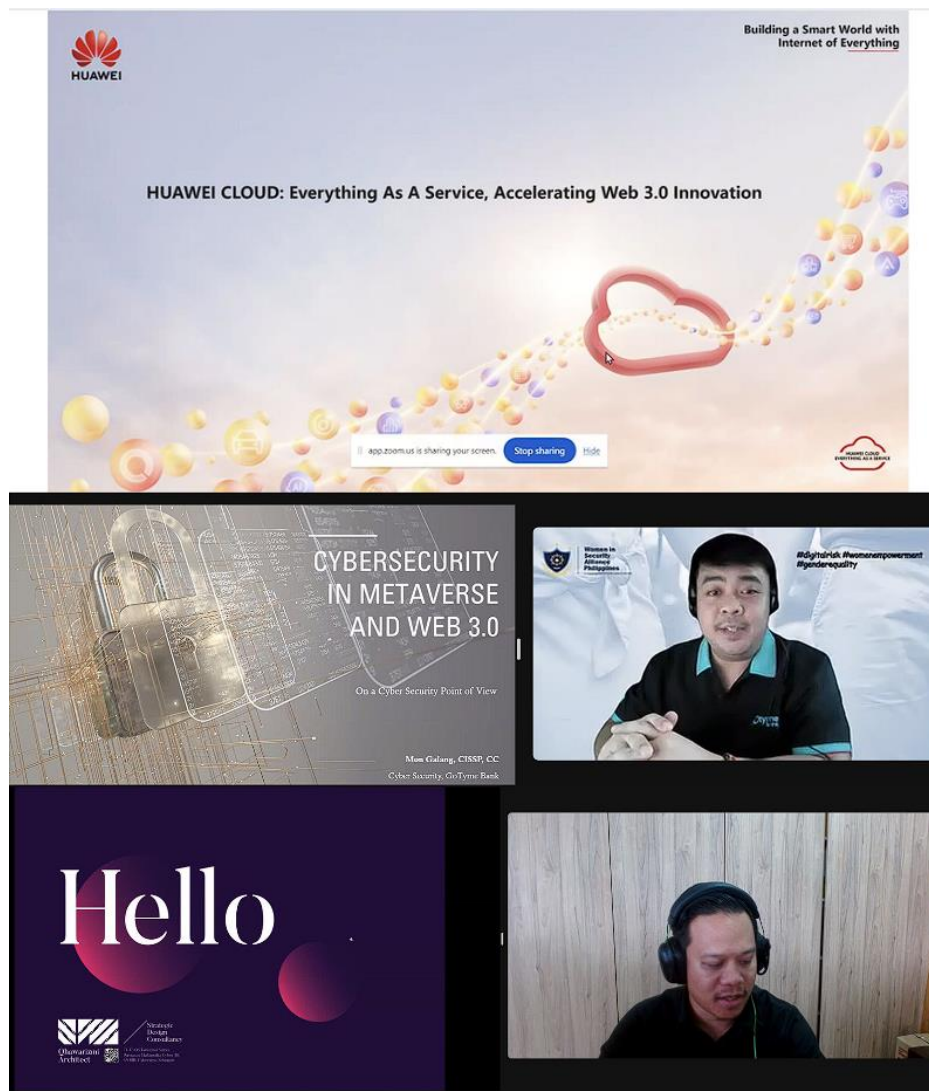


[back to top](#)

Regionalisation

SEA CC Webinar – Web3/Metaverse on 20 June

During our SEACC Webinar on 20 June, our speakers covered insights on Web3 and Metaverse. Thank you Speakers from Malaysia Board of Technologists and Women in Security Alliance Philippines for sharing and thank you our Corporate Partner, Huawei Singapore for speaking at the webinar.



ASEAN Bug Bounty on 20 July

ASEAN BUG BOUNTY

- BETA EDITION -

SATURDAY, 20 JULY 2024, 9am - 5pm GMT+8

ASEAN Bug Bounty is an initiative to enhance cybersecurity in Southeast Asia. We invite participants to identify vulnerabilities within digital systems and applications.

With exciting target platforms such as SIT's Campus as a Living Lab (CaLL) network infrastructure, Web3.0 smart contracts and Metaverse virtual environments, join us in shaping the cybersecurity landscape of Southeast Asia!



CLOSING DATE:
13 JULY 2024

- OPEN TO LOCAL (SINGAPORE) & ASEAN PARTICIPANTS
- MULTIPLE CATEGORIES: NUMBER, COMPLEXITY, JUDGES CHOICE
- WIN GOVWARE TICKETS & UP TO \$1000 WORTH OF VOUCHERS & PRIZES



CAMPUS AS A LIVING LAB



WEB3 & METAVERSE



ORGANISED BY:



SUPPORTED BY:



IN PARTNERSHIP
WITH:



Click [here](#) to register.

[back to top](#)

SEACC Webinar – Cloud Security on 31 July



SEA CC Webinar – Cloud Security



ALVIN YEO
Cloud Specialist, Tenable, APJ



31 | JULY 2024
3 – 5 PM SGT



MON GALANG
CyberSecurity Head, GoTyme Bank and
WISAP Technical Committee Expert

ORGANISED BY:











The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2024. The upcoming webinar will be focusing on Cloud Security where speakers will be sharing insights on the best practices for cloud security.

How Tenable Cloud Security Zaps the Risk You Cannot See

Speaker: Alvin Yeo, Cloud Specialist, Tenable, APJ

Cloud infrastructure is an attacker's playground – you need to reveal the risk you cannot see.

Join Tenable's Alvin Yeo, Cloud Specialist to hear how CNAPP empowers teams with full asset discovery and risk analysis, runtime threat detection and compliance reporting for multiple clouds.

In this session you will learn how to:

- Automate cloud infrastructure security with identity-driven CNAPP.
- Close cloud security gaps through powerful visualization, prioritization and remediation.
- Reduce your attack surface with least privilege and JIT.

Cloud Security Measures in a Modern Banking Environment

Speaker: Mon Galang, Cyber Security Head, GoTyme Bank and WISAP Technical Committee Expert

In the dynamic landscape of modern banking, robust cloud security measures form the bedrock of trust and integrity. Banks fortify their cloud infrastructure against cyber threats, ensuring the confidentiality and integrity of sensitive financial data. Continuous monitoring and stringent access controls further safeguard against unauthorized access, bolstering customer confidence in the digital banking ecosystem.

Date: 31 July 2024, Wednesday

Time: 3PM – 5PM (SGT)

Venue: Zoom

Registration:

https://us06web.zoom.us/webinar/register/2017139507734/WN_coq_DDdfTD-hVwllvS7LcQ

Digital For Life

Together with our student leaders from our Academic Partners, AiSP was at the Digital Skills for Life Train the Trainer session on 25 June where IMDA trained our student leaders for future community outreach.



Corporate Partner Event

Cisco Security: Securing the AI Revolution Event on 4 July



Cisco Security: Securing the AI Revolution Event

Invitation for Cisco Security: Securing the AI Revolution Event

We are excited to extend an exclusive invitation to you for our upcoming **Cisco Security: Securing the AI Revolution Event**.

In an era where AI initiatives are rapidly advancing, establishing a security-resilient infrastructure is paramount for deterring potential cyber threats. Our upcoming event will serve as a platform for security experts to exchange insights and approaches to navigate and leverage AI.

Event Information:

1. **Venue:** JustCo, Marina Square, 6 Raffles Boulevard, Marina Square, #03-308, Singapore 039594
2. **Date:** July 4, Thursday
3. **Time:** 6:30pm - 8:30pm (Check in at 6pm. Dinner will be provided.)

This is a prime opportunity to network with fellow security professionals and leaders. Hear from Cisco and industry veterans on their approaches to AI risk management, framework development, and AI innovations for the public sector industry. This includes sharing on our new Cisco Hypershield, collaborations with Splunk, and takeaways from premier events such as the RSA Conference and Cisco Live US.

RSVP at <https://cloudsecurity.cisco.com/0704-seminar-securing-the-ai-revolution-singapore-event> to secure your spot today. We look forward to hosting you at the event.

Agenda:

[back to top](#)

Start Time	Topics
06:00pm	Registration
06:30pm	Welcome & Opening
06:45pm	Fireside Chat: Securing the AI Revolution Event
07:15pm	Securing the AI Revolution: Cisco Hypershield
07:45pm	Cisco + Splunk: Better Together
08:15pm	Summary & Networking



Cisco Systems, Inc. 170 West Tasman Dr., San Jose, CA 95134

[Privacy Policy](#)

Manage [email preferences](#) or [unsubscribe](#)



© 1992–2024 Cisco Systems, Inc. All rights reserved.

CREST

Latest Exam Updates from CREST

Following the launch of our new syllabuses for our Certified Tester – Infrastructure (CCT INF) and Certified Tester – Application (CCT APP) exams, we wanted to share our next set of exciting updates to these exams.

[CREST Certified Tester - Infrastructure](#)

[CREST Certified Tester - Application](#)

What are the upcoming changes?

The major updates for both the CCT INF and CCT APP exams are detailed on the new

[back to top](#)

web pages for both exams. In addition to the updated syllabuses and content, we have also:

- **Increased the choice of locations:** all elements of the exam are being delivered with our exams delivery partner, Pearson VUE, meaning candidates can take the exams at over 1,100 Pearson VUE centres at locations around the globe, including Singapore and across Southeast Asia
- **Changed the exam components:** the certification has been divided into two parts: a multiple choice and written scenario exam - note the scenario element will no longer be combined with the practical element - and a separate practical exam
- **Created great flexibility in the approach:** candidates are now able to pick the order in which they take the components of the exam
- **Ensured the whole exam can be concluded within a day:** candidates can now book to sit both the written and practical elements of the exam on the same day and
- **Changed the use of own machine and tooling:** candidates will in future be able to access tooling within the Pearson VUE exam environment rather than bringing their own laptops, supported by access to the toolset ahead of the exam and the ability to upload materials in advance to assist you when taking the exams.

Information on these latest updates can be found on our dedicated web pages at:

[CREST Certified Tester - Infrastructure](#)
[CREST Certified Tester - Application](#)

Subsequent updates to watch out for

- Updated syllabuses for the Certified Simulated Attack Specialist (CCSAS) and Certified Simulated Attack Manager (CCSAM) exams
- Don't forget to check out our recently relaunched exams in Singapore for [CRTI](#) and [CPSA](#)

Let's stay in contact!

To get the latest CREST communications via email, message marketing@crest-approved.org and ask to 'Subscribe to CREST News'.

You can also see us on social media here: <https://www.linkedin.com/company/crest-approved/> and here: [CREST \(@CRESTadvocate\) / X \(twitter.com\)](#), and on our website www.crest-approved.org.

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
3 Jul	AiSP AI Security Summit	AiSP
4 Jul	Cisco Security: Securing the AI Revolution Event	AiSP & Partner
5 Jul	Cybersafe 7th Anniversary & Product Launch	Partner
7 Jul	AiSP Youth Symposium	AiSP
12 Jul	Cyberwellness sharing with Lion Befrienders	Partner
16 Jul	Learning Journey to TrendMicro for ITE West	AiSP & Partner
20 Jul	ASEAN Bug Bounty	AiSP & Partner
24 Jul	Data & Privacy Workshop	AiSP
26-27 Jul	Skills for Good Festival	Partner
27 Jul	Cyber Security Awareness Event at Teck Ghee	Partner
27 Jul	Career Sharing for PME at Skills for Good Festival at Plaza Singapura	Partner
30 Jul – 1 Aug	NACSA Cyber Security Summit 2024	Partner
31 Jul	SEA CC Webinar - Cloud Security	AiSP & Partner
6-8 Aug	CyberDSA in KL	Partner
14 Aug	SEA CC Webinar - Digital ID	AiSP & Partner
20-21 Aug	Operational Technology Cybersecurity Expert Panel Forum 2024	Partner
29 Aug	AiSP x SUTD x NTUC TTAB MOU Signing & PME Sharing	AiSP & Partner
30 Aug	Ladies in Cyber Symposium	AiSP

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

CONTRIBUTED CONTENTS

Article from CISO SIG

Introducing CISO with a deep interest in cybersecurity

Andre Shori is the APAC Cybersecurity Vice President and Chief Information Security Officer at Schneider Electric. Andre brings with him over 30 years of cyber experience, a SANS Technology Institute Master of Science in Information Security Management, and 18 major cybersecurity certifications. He serves as an Executive Board Member of the (ISC)2 Singapore Chapter and Vice President of the Association of Information Security Professionals (AiSP), contributing to the development of the cybersecurity profession across the globe and creating a vibrant global cybersecurity ecosystem that enables a safe and secure cyberspace for everyone.

1. What brought you to the Cybersecurity industry?

I have always been deeply fascinated by the tools, techniques, and processes that threat actors use to breach environments and, more importantly, what defenders should do to counteract these tactics. My first entry into Cybersecurity was over 30 years ago when I served as a network operator and help desk agent for BC (British Columbia) Rail in Canada. That is where I was exposed to security topics like access controls, prevention, and detection tools, BCP/DRP, and from there, I was hooked. It has been a lifelong learning journey since then; cybersecurity evolves so fast, and there has never been a dull moment.

2. What were your defining moments in this industry, and factors or guidance that helped you achieve them?

Being accepted into the Master of Science in Information Security Management (MSISM) program at SANS was pivotal in my career. The program filled in almost all the gaps in my Cybersecurity knowledge and taught me to think strategically at the organizational level. Quitting my job at the time to complete the MSISM was incredibly challenging, but completing it helped propel me into a role that I had long dreamed about.

3. What is it that you love most about your role?

I am gratified to know that I am helping to make a real difference in the Cybersecurity of my organization and my community. It is really rewarding to help shape the industry into a mature, professional, and well-recognized discipline. I also love all my fellow practitioners who share a passion for Cybersecurity. One of my favourite pastimes is meeting with other cybersecurity folks to share our knowledge and experiences. Cybersecurity is too vast a field for anyone to truly master, so it is great to meet people who help expand my views.

[back to top](#)

4. What are some of the trends you have seen in the market lately, and what do you think will emerge in the future?

I see a lot of attention being paid to automation and process re-engineering, which bodes well for streamlining current processes in a more efficient manner. SOARs (Security Orchestration, Automation and Response) are becoming the norm, and AI (Artificial Intelligence) has helped fuel that push. I also see signs that the IT/OT convergence is starting to really gain momentum now, with more OT (Operations Technology) Cybersecurity oriented solutions appearing on the market to address the growing OT/IoT install base as people start to imagine increased use cases on how to automate the world we live in.

5. What do you think is the role of CISO?

A Chief Information Security Officer (CISO) or equivalent (Head of Information Security, Chief Security Officer, TISO, BISO, ACISO, IT Manager, CISO as a Service etc.) is the person (or any immediate direct report) accountable (or in the case of a direct report, responsible) for defining and implementing their organization's overall cybersecurity strategy to enable and advance business outcomes. This person is ideally a senior-level executive, reporting to the most senior levels of the organization, who is actively leading the defence of their organisation, its businesses and all assets, including its people, data, infrastructure, products or technologies, against internal and external cybersecurity risk.

6. How can we encourage more people to join the cybersecurity sector?

Show them what a cybersecurity career looks like. Showcase more examples of different aspects of cyber such as an OT Cybersecurity engineer working at an oil and gas plant, or a DFIR (Digital Forensics and Incident Response) investigator, or a threat intel person doing red teaming etc. Get people to understand that there are gratifying careers in cyber, that it is not just about the \$\$, and that they can enjoy a rewarding vocation while making a difference in society.

7. What do you want to achieve or contribute to the Cybersecurity Ecosystem?

I will continue to add my energy, experience, and, where applicable, my expertise to continue to help drive and uplift our Cybersecurity discipline into a well-developed, attractive, and rewarding professional vocation. I plan to help accomplish this undertaking by engaging with all relevant stakeholders at all levels to ensure that our profession has the support and visibility necessary to ensure we can value and add our tradecraft towards our respective organization's objectives.

8. Any advice for the Cybersecurity Professionals?

You must have a passion for cybersecurity to best ensure you will thrive. A career in Cybersecurity is demanding, deeply technical, always challenging and without passion

your odds of burning out are high. It is a thankless role, and you are usually first to be blamed, so you must be able to embrace the knowledge that you are performing a role in ensuring the betterment of society through your actions.

Article from LITE SIG

Legal Investigative Technology Experts (LITE), formerly known as High Technology Crime Investigation Association (HTCIA)

About us

LITE was formed to provide education and collaboration within AiSP for the prevention and investigation of high tech crimes.

As such, we are a special interest group that aspires to help all those in the high technology field by providing extensive information, education, collective partnerships, mutual member benefits, astute board leadership and professional management.

Our Mission:

LITE is a special interest group within AiSP providing individuals utilizing investigative techniques and technology with innovative networking and training.

Our Vision:

To provide a platform for AiSP members who are keen in the high technology space, to participate in and benefit from each other's expertise, so as to create a vibrant and dynamic ecosystem.

To support innovation and collaboration in the field across the government, law enforcement, academic, private industry, and legal communities.

Key activities:

- Knowledge sharing of Digital Forensic / e-Discovery in Q4 2024

Support required:

- Sponsorship for workshop or conference
- Active participation from the SIG
- Interest from greater AiSP members to join this SIG

Article from DevSecOps SIG

Putting the 'Sec' in DevSecOps: Emphasizing White Box Testing and End-to-End Security

In the fast-paced world of software development, the traditional silos of development, operations, and security are rapidly breaking down. The advent of DevSecOps reflects this evolution, integrating security practices into the entire lifecycle of application development and deployment. However, to truly embed security within the DevOps framework, organizations must prioritize rigorous testing methodologies, with White Box testing and comprehensive end-to-end testing at the forefront. This is also why organizations are delving into Security-by-Design rather than Security after Design!

The Essence of DevSecOps

DevSecOps is more than just a buzzword—it's a transformative approach that embeds security considerations into every phase of the software development lifecycle (SDLC). The objective is to address security issues as early as possible, fostering a culture where security is everyone's responsibility. This proactive stance contrasts sharply with the traditional reactive approach, where security checks are performed late in the development process, often resulting in costly and time-consuming fixes.

White Box Testing: The Cornerstone of Secure Code

White Box testing, also known as clear box, open box, or glass box testing, is a method where the internal workings of the application are known and utilized to design test cases. This testing strategy is invaluable in a DevSecOps environment for several reasons:

1. Early Vulnerability Detection

White Box testing allows testers to examine the internal code structure, logic, and flow. By doing so, vulnerabilities can be identified early in the development process, mitigating risks before they escalate into more significant security threats. This proactive identification of security flaws aligns perfectly with the DevSecOps philosophy of early and continuous security integration.

2. Comprehensive Coverage

By understanding the internal workings of the application, developers can create more thorough and targeted test cases. This comprehensive coverage ensures that even the most obscure and deeply embedded vulnerabilities are identified and addressed. It contrasts with Black Box testing, where testers only evaluate the software from an external perspective, potentially missing critical internal flaws. With test case coverage, the depth of coverage becomes more important – especially for safety critical and mission critical applications where lives are at stake or important data is imperatively guarded.

[back to top](#)

Automotive, Aviation, Government, Financial and Healthcare industries are prime examples of high coverage needs. Unfortunately, not many are willing to incorporate high coverage into their requirements as it might cause delays or incur higher costs.

3. Enhanced Code Quality

White Box testing not only focuses on security vulnerabilities but also on code quality. By scrutinizing the code, developers can identify areas of inefficiency, redundancy, and potential bugs, leading to overall better code quality. High-quality code is inherently more secure and reliable, contributing to a more robust application. Thus, code quality will provide a more stable application that is less prone to crashing or failing and in so doing contributes to the overall security of the application.

The Imperative of End-to-End Testing

While White Box testing is essential, it must be complemented by end-to-end testing to ensure comprehensive security coverage. End-to-end testing evaluates the entire application flow, from start to finish, simulating real-world scenarios and user interactions. Here's why it's crucial in a DevSecOps framework:

1. Holistic Security Validation

End-to-end testing ensures that all components of the application work together seamlessly and securely. It validates the security of integrations, data flows, and user interactions, identifying potential vulnerabilities that might arise from complex interdependencies within the system.

2. User Perspective Security

By simulating real-world usage scenarios, end-to-end testing provides a user's perspective on the application. This approach helps uncover security issues that may not be apparent through internal code analysis alone, such as vulnerabilities in authentication, authorization, and data handling processes.

3. Regression Prevention

As applications evolve, new features and updates can inadvertently introduce security vulnerabilities. End-to-end testing is crucial for regression testing, ensuring that new changes do not compromise the existing security posture. This continuous validation is essential for maintaining a secure and resilient application over time.

Integrating Testing into DevSecOps Workflows

For organizations aiming to put the 'Sec' in DevSecOps, integrating White Box testing and end-to-end testing into the CI/CD pipeline is essential. Here are some best practices:

1. Automate Testing

Automate White Box and end-to-end testing to ensure consistent and continuous security checks. Automation tools can integrate seamlessly with CI/CD pipelines, providing immediate feedback and allowing developers to address issues in real-time. This is especially pertinent to current practices in agile development and devops. A continuous testing and feedback loop would help drive the efficiency and productivity for software development teams.

2. Shift Left

Embrace the "shift left" approach by incorporating security testing early in the development process. This strategy not only identifies vulnerabilities sooner but also instills a security-first mindset among developers, fostering a culture of proactive security. The promotion of shift left culture is not straightforward. It requires a lot of training to the development teams and requires buy-in from management to project managers as well as any stakeholders in the organization. But once implemented, there will be a lot of benefits inculcated into the teams and by extension, to the applications that are built.

3. Continuous Monitoring

Implement continuous monitoring to track the effectiveness of security measures and adapt to new threats. Monitoring tools can provide insights into security performance, helping teams make informed decisions and quickly respond to emerging vulnerabilities.

4. Collaborative Culture

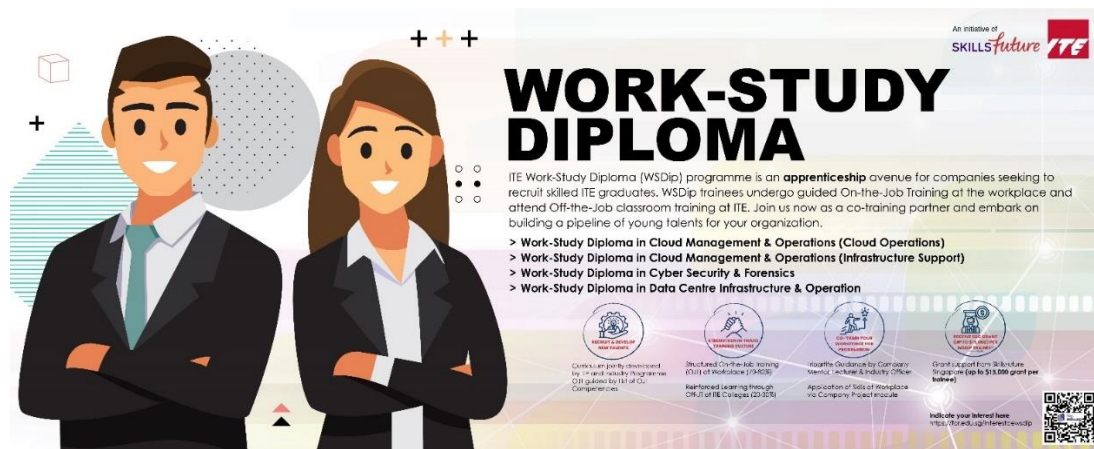
Foster collaboration between development, operations, and security teams. Encourage regular communication and knowledge sharing to ensure that security is a shared responsibility and that all team members are equipped to identify and address security issues.

Conclusion

Putting the 'Sec' in DevSecOps requires a comprehensive and proactive approach to security. By emphasizing White Box testing and end-to-end testing, organizations can ensure that security is deeply integrated into the software development lifecycle. These testing methodologies provide the thorough coverage needed to identify and address vulnerabilities early, ensuring the delivery of secure and resilient applications.

As the landscape of cybersecurity threats continues to evolve, the commitment to rigorous testing and continuous improvement will be the cornerstone of effective DevSecOps practices.

Article from APP, ITE



We offer the following Work Study Diploma Programmes at ITE College East:

- Work Study Diploma Programme in Cyber Security & Forensics
- Work Study Diploma Programme in Cloud Management & Operations (Infrastructure Support)
- Work Study Diploma Programme in Cloud Management & Operations (Cloud Operations)
- Work Study Diploma Programme in Data Centre Infrastructure & Operation

The highlights of the Work Study Diploma are:

- Companies can claim up to \$15,000 for every Work Study Diploma Trainee they engage.
- Companies will be able to interview and select graduates of Nitec / Higher Nitec in IT / Cyber Security for this programme.
- Companies will be assured of manpower for the next 2.5 years.
- Companies may send representatives to sit on the Technical Committee and provide input for the course.

Companies can email at lee_choon_giap@ite.edu.sg or call/WhatsApp at 91276308.

Companies can also indicate interest thru' this link.

<https://for.edu.sg/interestcewsdip>



Article from SVRP 2023 Gold Winner, Kek Jun Kai [NP]



How do you think SVRP has directly impacted your cybersecurity journey?

The SVRP wasn't just another program for me; it was an awakening. Receiving the Silver Award was honestly more than just a certificate on the wall. It was a pat on the back, a validation that I was on the right path. Every workshop, interaction, and mentorship session during the program was like adding a piece to the puzzle of my cybersecurity journey. It's where I truly felt the weight of our responsibilities in cybersecurity, realizing it's not just about codes and algorithms, but real lives and stories. I vividly remember the conversations with my lecturers, seniors, and mentors. They didn't just teach; they shared, guiding me with their experiences, wisdom, and sometimes, their mistakes. And it was through these genuine interactions that I found direction and purpose. Reconnecting with peers during SVRP, especially after such long breaks, was like catching up with old friends. We were all there with a shared goal - to make a difference. So, every time I think of SVRP, I'm reminded of that spark, that drive it reignited in me. And that's why it holds such a special place in my heart. It's more than a program; it's where I found a deeper sense of belonging and purpose in the world of cybersecurity.

How has SVRP inspired you to contribute to the cybersecurity field?

SVRP was a turning point for me. Before joining, I knew I had a passion for cybersecurity, but it was during my time with the program that this passion transformed into a deep-rooted purpose. Interacting with like-minded individuals, sharing experiences, and learning from some of the best in the field showed me the real-world impact of our roles. It's not just about protecting systems; it's about safeguarding memories, preserving livelihoods, and sometimes, saving lives. The recognition through the Silver Award wasn't just an accolade for me. It was a tangible reminder of the difference I could make and the responsibilities I shouldered. The people I met, the stories I heard, and the challenges we discussed instilled

a drive in me to give back, to be more than just a participant in the cybersecurity field. Today, inspired by SVRP, I'm committed to not only enhancing my skills but also mentoring, educating, and collaborating. The program highlighted the importance of community, of working together to combat threats, and of ensuring the next generation is equipped, inspired, and ready to take on the challenges of tomorrow. SVRP didn't just shape my journey; it redefined it, pushing me to be a proactive contributor to the cybersecurity ecosystem.

What motivates you to be a student volunteer?

Being a student volunteer is driven by a combination of passion and purpose for me. Firstly, I'm motivated by the opportunity to learn and grow outside of the traditional classroom setting. Volunteering allows me to see the real-world applications of what I'm studying, and it adds layers of depth to my academic pursuits. Secondly, I believe in giving back. I've been fortunate to receive guidance and mentorship in my journey, and volunteering provides me a platform to pay that forward, to possibly be that beacon for someone else. Additionally, the camaraderie and connections I've forged while volunteering are priceless. Interacting with diverse groups of people, sharing experiences, and collaborating on projects have enriched my perspective and broadened my horizons. Lastly, there's a unique satisfaction in knowing that my efforts, however small, are making a difference. Whether it's helping organize an event, mentoring a peer, or contributing to a community project, the tangible impact of my volunteer work serves as a constant reminder of the positive change we can affect when we come together. In essence, it's this blend of personal growth, community, and purposeful impact that drives me to be a student volunteer.

How would you want to encourage your peers to be interested in cybersecurity?

I'd start by making it relatable. Instead of diving into the technical jargon, I'd share real-world stories and scenarios. I'd talk about how our entire digital lives, from our personal photos to our bank details, are safeguarded by cybersecurity. I'd mention stories where a simple cybersecurity oversight had significant consequences, like the ransomware attacks on hospitals or data breaches affecting millions. Then, I'd highlight the empowering aspect. In cybersecurity, we're not just passive consumers; we have the skills and knowledge to protect ourselves, our families, and even our communities. It's like having a digital superpower! I'd also emphasize the vast opportunities in the field. With the increasing digitization of our world, cybersecurity professionals are in high demand, offering promising career paths, lucrative salaries, and the chance to be at the forefront of technological evolution. Workshops and hands-on sessions would be a great way to ignite interest. By giving peers a taste of ethical hacking, for instance, they'd get to experience the thrill of the chase, the challenge of the puzzle, and the satisfaction of 'cracking the code'. Lastly, I'd encourage them to join me in volunteering or attending cybersecurity events. Sometimes, the best way to spark interest is to immerse someone in the community, to let them see the passion, the challenges, and the rewards firsthand. Through these combined efforts, I hope to not only share my enthusiasm for cybersecurity but also inspire them to explore and possibly find their niche in this dynamic field.

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

New versions launched!



Stay ahead of the curve with EC-Council certification programs!

The all popular Certified Network Defender (CND), Certified Threat Intelligence Analyst (CTIA) and Certified Hacking Forensic Investigator (CHFI) are now available in the latest versions!

Master advanced network security requirements with CND, excel in predictive threat intelligence CTIA and build ultimate investigative skills with CHFI. With the latest tools and technologies in these programs building job-ready skills, you can set yourself up for success!

Available as self-paced learning kits, each bundle includes EC-Council instructor-led training videos, e-book, virtual labs and remote proctored exam voucher.

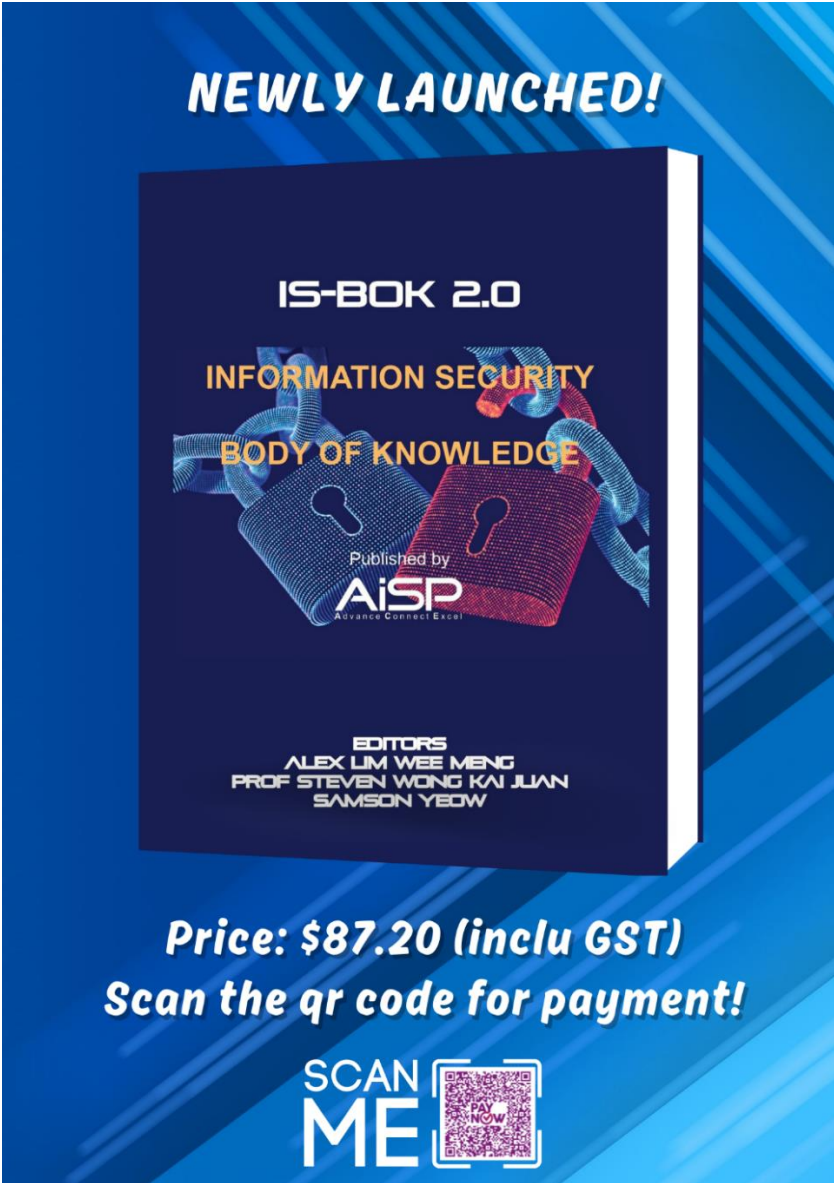
Special discounts available for AiSP members, please email enquiry@wissen-intl.com for details!

[back to top](#)

Qualified Information Security Professional (QISP®)

Body of Knowledge Book (Limited Edition)

Get our **Limited Edition** Information Security Body of Knowledge (BOK) Physical Book at **\$87.20 (inclusive of GST)**.



NEWLY LAUNCHED!

IS-BOK 2.0

INFORMATION SECURITY


BODY OF KNOWLEDGE

Published by
AiSP
Advance Connect Excel

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

Price: \$87.20 (inclu GST)

Scan the qr code for payment!

SCAN ME 

Please scan the QR Code in the poster to make the payment of **\$87.20 (inclusive of GST)** and email secretariat@aisp.sg with your screenshot payment and we will follow up with the collection details for the BOK book. **Limited stocks available.**

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

AiSP QISP Workshop on 1 October



AiSP QISP Workshop



QISP INSIGHT MASTERCLASS
ONE-DAY APPRECIATION WORKSHOP
FOR THE QISP PROGRAMME



Workshop Details

-  **1 October 2024**
Tuesday
-  **9AM - 5PM**
Registration starts at 8.30AM
-  **NTUC Centre, Level 7**
Room 701, One Marina Boulevard, S (018989)



ORGANISED BY 

SUPPORTING AGENCY 

TRAINING PARTNER 

REGISTER NOW!

QISP Insight Masterclass

Join us for an exclusive QISP Insight Masterclass, a unique opportunity to delve into the QISP (Qualified Information Security Professional) Certification Programme. This masterclass is designed for cybersecurity professionals seeking to enhance their expertise and stay ahead of the curve in the ever-evolving field of cybersecurity.

What to Expect:

Explore the QISP Certification Programme: Gain insights into the structure and benefits of the QISP certification. Understand how this certification can propel your career and equip you with the skills needed to tackle modern cybersecurity challenges.

Insight into the 6 Domains: Experience a comprehensive overview of the six domains covered in the QISP curriculum. Engage in interactive sessions that provide a snapshot of the knowledge and skills you will acquire, from risk management to incident response.

Network with Professionals: Connect with like-minded cybersecurity experts and expand your professional network. Share experiences, exchange ideas, and build relationships that can support your career growth.

Hands-on Discussions: Participate in dynamic discussions on the latest trends and threats in cybersecurity. Learn from industry leaders and peers as you explore real-world scenarios and cutting-edge solutions.

Why Attend?

Experience the QISP Programme: Get a first-hand look at what the QISP certification entails and how it can benefit your career.

Engage with Experts: Learn from top cybersecurity professionals and gain insights into best practices and emerging trends.

Expand Your Network: Meet and collaborate with other professionals in the cybersecurity community.

Stay Informed: Stay ahead of the curve by participating in discussions on the latest cybersecurity developments.

Don't miss this opportunity to enhance your knowledge, network with peers, and gain insights into the QISP Certification Programme. Secure your spot in the QISP Insight Masterclass today!

Date: 1 October 2024, Tuesday

Date: 9AM to 5PM (registration from 8.30am)

Venue: NTUC Centre, Level 7, Room 701, One Marina Boulevard, S (018989)

Registration: <https://go.wissen-intl.com/qispmasterclass>

Online Course launched on 1 March 2024!

QISP Exam Preparatory E-Learning Course

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

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

Grab the exclusive launch offer at SGD 499 nett!

Special price of SGD 429 nett for AiSP members!

- Governance and Management
- Physical Security and Business Continuity
- Security Architecture and Engineering
- Operation and Infrastructure Security Software Security
- Software Security
- Cyber Defense

WISSEN Cyber Security Competency Development | enquiry@wissen-intl.com | www.wissen-intl.com

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

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

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: 2024) from 1 Jan 2024 to 31 Dec 2024. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. [This does not include Plus! card holder \(black-coloured card\), please clarify with NTUC on your eligibility.](#)

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

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

CPP Membership



For any enquiries, please contact secretariat@aisp.sg

AVIP Membership

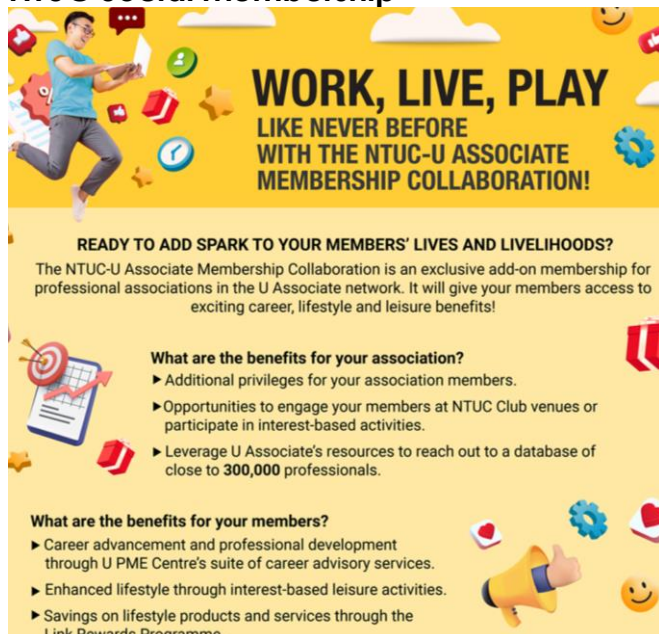
AiSP Validated Information Security Professionals (**AVIP**) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development, and career progression for our professionals.

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!

NTUC Social Membership



WORK, LIVE, PLAY
LIKE NEVER BEFORE
WITH THE NTUC-U ASSOCIATE
MEMBERSHIP COLLABORATION!

READY TO ADD SPARK TO YOUR MEMBERS' LIVES AND LIVELIHOODS?
The NTUC-U Associate Membership Collaboration is an exclusive add-on membership for professional associations in the U Associate network. It will give your members access to exciting career, lifestyle and leisure benefits!

What are the benefits for your association?

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

What are the benefits for your members?

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

Some benefits include

Benefits and privileges from RX Community

Member Programme

<https://www.readyforexperience.sg/>

Please fill in the form below and make payment if you would like to sign up for the membership.

<https://forms.office.com/r/qtjMCK376N>

Please check out our website on [Job Advertisements](#) by our partners. For more updates or details about the memberships, please visit www.aisp.sg/membership.html

AiSP Corporate Partners

Acronis

athena
dynamics



bugcrowd



CLIXER



CYBERSAFE
YOUR SECURITY, OUR PRIORITY



DETECT



FORTINET®





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



Freddy Tan
Director



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.