AiSP

NEWSLETTER

September 2024

NEWS & UPDATE

Continued Collaboration

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

image engine

ONESECURE®

News & Updates

NTUC U SME Towkay Networking Event on 16 August

AiSP was invited to NTUC U SME Towkay Networking Event on 16 August. Thank you AiSP EXCO Member Mr Dennis Chan for dropping by and interacting with Member of Parliament for Pasir Ris-Punggol GRC / NTUC U SME & Women Unit Director: Ms Yeo Wan Ling.

National Day Rally 2024 held at ITE Central on 18 August

Our AiSP Vice-President Ms Sherin Lee represented AISP to be part of the NTUC Delegation team and attended the National Day Rally held at ITE Central on 18 August.

back to top

MOU Signing Ceremony: Design x AI x Tech (Cybersecurity) Certification Programme Launch on 29 August

AiSP, SUTD, NTUC and TTAB signed a Memorandum of Understanding (MOU) for the official launch of the new Graduate Certificate in Design, AI & Technology (Cybersecurity)!

This innovative program is designed specifically for non-IT graduates, PMEs, and practicing professionals looking to transition into the Cybersecurity industry. It also welcomes IT graduates and professionals who want to elevate their careers by gaining the latest skills and knowledge in Cybersecurity.

AiSP Vice President, Ms Sherin Lee shared on why she ventured into cyber and what motivated her to stay in the industry. She also encouraged PMEs to be part of cyber and the attendees brought back takeaways from her sharing.

The event was graced by SMS Tan Kiat How, Advisor to TTAB, Patron to AiSP, and Senior Minister of State, Ministry of Digital Development and Information. Thank you SMS Tan for joining us and supporting the importance of continuous learning for the new and old professionals to the cybersecurity landscape.

Thank you everyone who have joined us for this milestone occasion. We look forward to seeing the impact this program will have on shaping the future of Cybersecurity professionals!

Design x AI x Tech (Cybersecurity) Certification Programme Launch
MOU Signing Ceremony
29 August 2024 | 6pm – 8.30pm

back to top

Member Acknowledgment

Interview with AiSP EXCO Member Mr Cecil Su

Vision and Insights for AiSP and Cybersecurity Industry

As a Cybersecurity practitioner leading a practice in Singapore and a Fellow at the Association of Information Security Professionals (AiSP), I've had the privilege of witnessing the rapid evolution of the cybersecurity landscape. This journey has shaped my vision for contributing to AiSP and addressing the pressing issues in our industry.

Shaping the Future of Cybersecurity Through AiSP

My vision for AiSP is rooted in the belief that our collective expertise can significantly impact the cybersecurity ecosystem. I see my role as a catalyst for growth and innovation within the community. By leveraging my experience, I aim to bridge the gap between seasoned professionals and emerging talents.

One of my key focus areas is mentorship. I believe that by guiding the next generation of cybersecurity professionals, we can create a robust talent pipeline equipped to handle future challenges. This mentorship extends beyond technical skills to include soft skills and ethical considerations, which are crucial in our field.

Additionally, I'm passionate about fostering collaboration between industry and academia. These partnerships are vital for driving innovation and ensuring that our academic programs align with real-world needs. By facilitating these connections, we can accelerate research and development in critical areas of cybersecurity.

Addressing the Cybersecurity Industry's Greatest Challenge

In my view, the most significant issue facing our industry is the dynamic nature of cyber threats coupled with a persistent skills shortage. This challenge is multifaceted and requires a comprehensive approach.

Continuous upskilling is paramount. The threat landscape evolves rapidly, and our defenses must keep pace. I advocate for creating accessible, cutting-edge training programs that allow professionals to stay ahead of emerging threats. These programs should blend technical knowledge with strategic thinking, enabling practitioners to anticipate and mitigate risks proactively.

Equally important is the need to enhance cybersecurity awareness across all levels of organizations. Security is no longer just an IT issue; it's a business imperative. By promoting

back to top

a culture of security consciousness, we can create a human firewall that complements technological defenses.

Developing adaptive and resilient security frameworks is another critical area. As cyber threats become more sophisticated, our approach to security must evolve from reactive to proactive and predictive. This involves leveraging technologies like AI and machine learning while also focusing on fundamental principles of security architecture and risk management.

Representing AiSP with Integrity and Vision
As an EXCO member, I understand the responsibility of representing AiSP in various forums. My approach is grounded in professionalism, ethical conduct, and a commitment to AiSP's core values (rightfully to advance, connect, and excel the profession).

When engaging with stakeholders, I strive to articulate AiSP's mission clearly, emphasising our role in advancing the cybersecurity profession. This involves not just sharing information but also inspiring action. I believe in the power of storytelling to convey complex ideas and motivate change.

Active listening is a crucial part of my strategy. By understanding the needs and challenges of our stakeholders, we can tailor AiSP's initiatives to provide maximum value. This feedback loop ensures that our organization remains relevant and impactful in a rapidly changing landscape.

Contributing Expertise to the AiSP Community and Beyond
Indeed, AiSP has come a long way ever since the early days. My plan for sharing expertise with AiSP members and the wider community is multifaceted. I am open to participate and conduct workshops that delve into advanced cybersecurity topics, drawing from my experience at BDO Advisory. These sessions will go beyond theory to provide practical, actionable insights that professionals can apply immediately in their roles.

Writing is another powerful medium for sharing knowledge. Through articles and whitepapers, I aim to disseminate insights on emerging trends and best practices. These publications will serve as resources for professionals seeking to deepen their understanding of complex cybersecurity issues.

Participation in panel discussions and conferences is also a key part of my strategy. These forums provide opportunities to engage in meaningful dialogues about industry challenges and potential solutions. By sharing experiences and insights, we can collectively work towards advancing the field of cybersecurity.
Lastly, I'm excited about the prospect of collaborative research initiatives within the AiSP community. By combining our diverse expertise, we can tackle pressing cybersecurity issues and contribute to the body of knowledge in our field.

back to top

In conclusion, my goal is to contribute to AiSP and the wider cybersecurity community by blending practical industry experience with academic rigor. I believe that by working together, sharing knowledge, and fostering innovation, we can build a more secure digital future for Singapore and beyond.

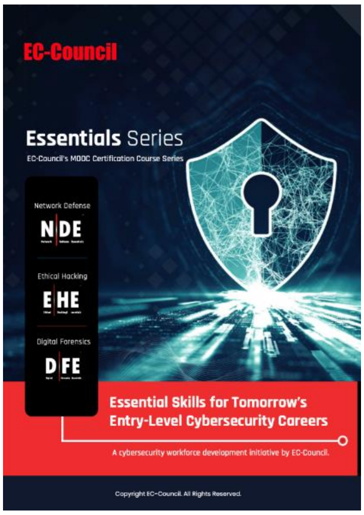
Student Volunteer Recognition Programme (SVRP)

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.

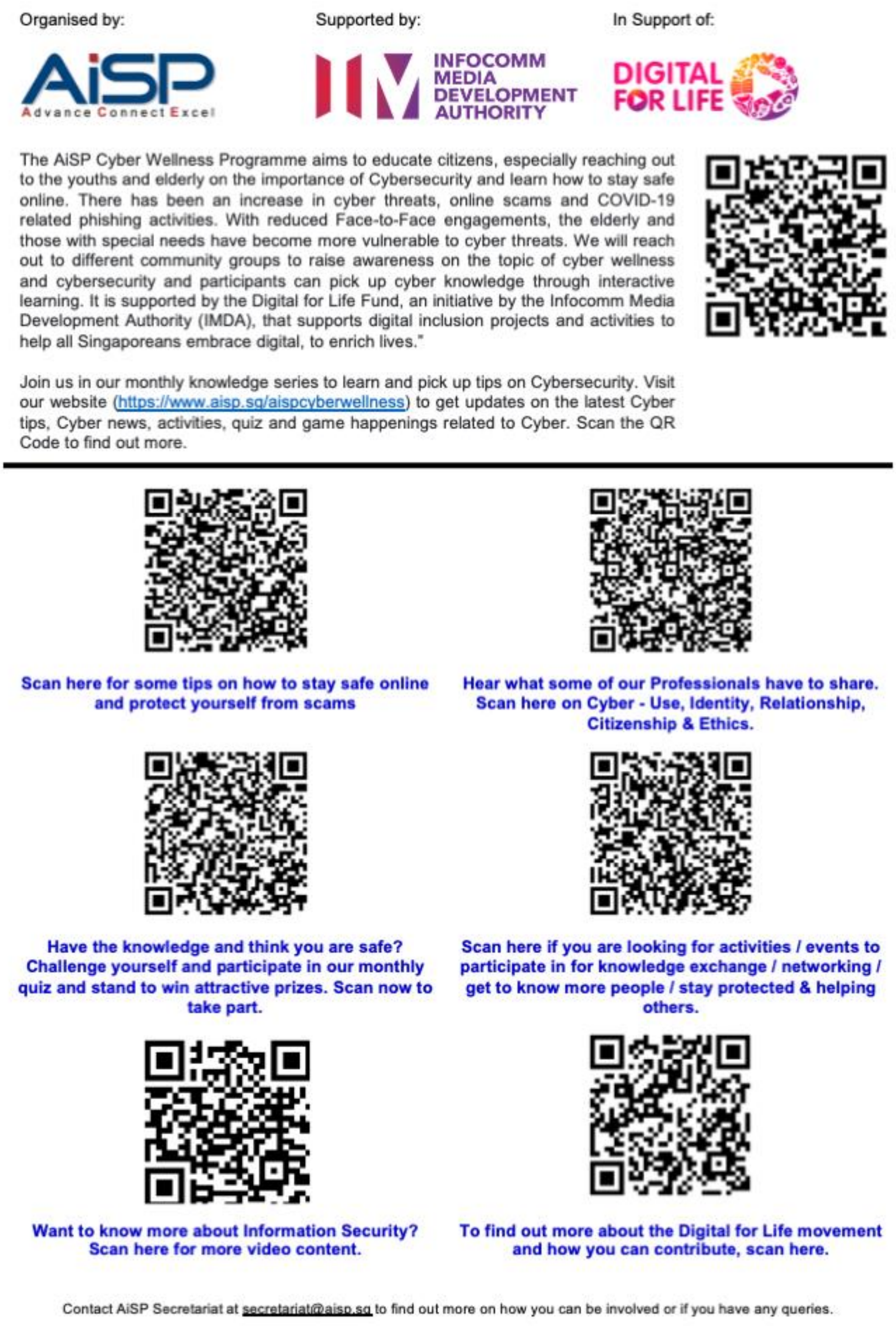
Visit (https://wissen-intl.com/essential500/) and register to start your cybersecurity credentialing journey! Terms & Conditions apply.

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.


EC-Council
Essentials Series
EC-Council's MOOC Certification Course Series
Network Defense
N|DE
Ethical Hacking
E|HE
Digital Forensics
D|FE
Essential Skills for Tomorrow's Entry-Level Cybersecurity Careers
A cybersecurity workforce development initiative by EC-Council.
Copyright EC-Council. All Rights Reserved.

back to top

AiSP Cyber Wellness Programme



Organised by: AiSP Advance Connect Excel

Supported by: Infocomm Media Development Authority

In Support of: Digital for Life

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

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

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

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

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

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

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

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

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

Click here to find out more!

back to top

Special Interest Groups

AiSP has set up 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
- Legal Investigative Technology Experts (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

back to top

AI SIG Meetup 2024 on 27 August

As part of our Artificial Intelligence Special Interest Group, AiSP was at our Corporate Partner, Trend Micro office for our AI SIG meetup on 27 August. Thank you to our speakers, Mr Jeremy Soh, Mr Tianyu Pang and Mr Paul Hidalgo for sharing insights with our attendees. Thank you Trend Micro for hosting us and AiSP Assistant Secretary cum AI SIG Lead, Mr Tam Huynh for delivering the welcome address.

back to top

DevSecOps SIG Meetup on 3 September

AiSP DevSecOps SIG Meetup

Calling all practitioners and students of DevSecOps. We are a newly minted Special Interest Group in AiSP - DevSecOps. We will be organizing a Meet Up session in Sep to build a community of professionals and students so as to share knowledge and meet others who has expertise in this area. In future, we will also provide a platform for vendors to share their solutions to help in this area to improve the practices. Come join us for some fun and food. Pizzas (Halal & Vegetarian)/Drinks/Coffee & Tea will be available but bring your Name Cards, LinkedIn QR codes to meet up and network.

Agenda:
6pm – 6.45pm Registration & dinner
6.45pm – 7.15pm Welcome address & Introduction of DevSecOps SIG by AiSP
7.15pm – 8.30pm - Audience Participation:
*Tell us about yourself! (1 min each)
* Knowledge-base (Top 3)
* What you would like to see for future Meet Ups?
- Prize Giving
- Lucky Draw
8.30pm – End of event

PS - If you would like to sponsor some prizes for the lucky draw, please let us know: stanley.eu@aisp.sg

Date: 3 September 2024, Tuesday
Time: 6PM – 8.30PM
Venue: JustCo @ Marina Square
Registration: https://www.eventbrite.sg/e/952371327277?aff=oddtdtcreator
*AiSP members who would like to bring a non member for the event can reach out to secretariat@aisp.sg for a 50% discount code.

back to top

Cloud Security Summit on 24 September

AiSP Cloud Security Summit 2024

24 Sep 2024

12.30PM - 5PM

Marina Bay Sands Convention Centre

Organised by: AiSP Advance Connect Excel

The AiSP Cloud Security Summit 2024 is an important event of the year, organised by the AiSP Cloud Security Special Interest Group. The programme schedule comprises of key notes, solutions, panel discussion and workshop. The theme for the summit is Navigating Cloud Security in the near-future Era. This event is organized for anyone with an interest or wish to find out more or understand more on the landscape of Cloud Security.

Embark on a journey into the future of cloud security at the AISP Cloud Security Summit. This meticulously organized event serves as a nexus for cybersecurity professionals, cloud experts, and industry thought leaders to converge and navigate the complexities of cloud security in the near-future era.

Throughout this immersive one-day event, attendees will immerse themselves in the latest cloud security trends, threats, and innovations, all tailored to address the unique challenges and opportunities within our region.

Join us as we explore:

- The Evolving Threat Landscape: Uncover the dynamic shifts within the cloud security threat landscape and equip yourself with strategies to stay ahead of emerging risks.
- Compliance and Regulatory Updates: Stay informed about the ever-changing landscape of compliance standards and regulatory requirements, ensuring your organization remains resilient in the face of evolving mandates.
- Best Practices for Cloud Migration and Security: Navigate the intricacies of cloud migration while safeguarding the integrity and security of your digital assets with industry-leading best practices.

back to top

- Emerging Technologies: Discover the transformative potential of cutting-edge technologies such as Artificial Intelligence (AI), Machine Learning (ML), and DevSecOps in fortifying cloud security frameworks and enhancing threat detection capabilities.
- Real-World Case Studies and Success Stories: Draw inspiration from real-world case studies and success stories, offering invaluable insights and actionable strategies derived from organizations that have successfully traversed the challenges of cloud security implementation.

Prepare to expand your network, glean wisdom from seasoned experts, and arm yourself with the insights needed to fortify your organization's cloud journey.

Date: 24 September 2024
Time: 12.30PM – 5PM
Venue: Marina Bay Sands Convention Centre
Guest of Honour: AiSP Patron - Senior Minister of State, Ministry of Digital Development and Information & Ministry of National Development Mr Tan Kiat How

For more details, you can visit https://aisp.sg/Cloud_Security_Summit_2024.html

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

By registering for this event, you hereby agreed to be contacted by AiSP and your details to be shared with our partners.

back to top

AiSP LITE SIG Meetup 2024 on 3 October

AiSP LITE SIG Meetup

LITE SIG Meetup

Chua De Hui
LITE SIG Co-Lead
AiSP
Director
Deloitte Forensic Southeast Asia
Moderator

Jacky Ang
Digital forensics analyst in a
TECH MNC
Panellist

Mohamad Ridzuan
Digital Forensic Examiner
Home Team Science and
Technology Agency
Panellist

Shirley Liew
Senior Consultant
FTI Consulting
Panellist

Organised By: Supported by:

3 Oct 2024, Thurs
6PM - 8.30PM
JustCo @ Marina Square

Register Here:

AiSP has set up a Special Interest Group - **Legal Investigative Technology Experts (LITE)**.
Our Vision is to provide a platform for AISP members who are keen in the investigations space, specialising in the realms of digital forensic / e-Discovery, to participate in and benefit from each other's expertise, so as to create a vibrant and dynamic ecosystem.
Join us for an enlightening panel discussion that delves into the daily responsibilities and challenges faced by Digital Forensic / e-Discovery specialist in the public sector, consulting, and as an in-house practitioner. This session will provide a behind-the-scenes look at the critical work conducted by these specialists in the realm of the digital, legal, and investigative landscape.

Panel Discussion
Inside the Lab: A Day in the Life of a Digital Forensic / e-Discovery Specialist
This discussion will feature a diverse panel of digital forensic / e-Discovery specialists with varied expertise from the different sectors, offering a comprehensive view of the profession. Whether you're a student aspiring to enter the field, a professional seeking to understand the digital investigative landscape better, or simply curious about the work behind the scenes, this session promises to be both informative and engaging.

Moderator:
Chua De Hui
De Hui is a Director at Deloitte Forensic Southeast Asia, bringing over a decade of expertise in Digital Forensics, eDiscovery, and investigative advisory services across Southeast Asia's diverse economies. Throughout his career, De Hui has successfully led and managed a wide array of engagements, including complex digital forensic investigations, eDiscovery reviews, and as well as execution of Search Orders across Singapore and Malaysia.

back to top

In addition to his role at Deloitte, De Hui is currently the co-lead of Legal Investigative Technology Experts, where he hopes to contribute new ideas and attract young talents to the industry.

Panelists:
Jacky Ang
With close to 4 years of DFIR experience, Jacky is currently working in-house as a digital forensics analyst in a TECH MNC and has been in both the government and private sector. He specialises mainly in Windows forensics and holds a GCFA certification. During his free time, he likes to hunt for good food, watch football matches and also read up on threat intel, DFIR blogs and general cybersecurity news to stay updated.

Mohamad Ridzuan
Ridzuan kicked off his digital forensics journey in 2016 with the Singapore Police Force and later transitioned to the newly established Home Team Science and Technology Agency (HTX). Specializing in mobile and drone forensics, and now dabbling in malware forensics, he's all about diving deep into the digital world.
Armed with certifications like GCFE, GCFA, GASF, and GREM, Ridzuan is always on the hunt for new knowledge, whether it's through training, education, or hands-on experience with the latest forensic tools.
When he's not unravelling digital mysteries, you'll find him obsessing over Capture the Flag (CTF) challenges.

Shirley Liew
Shirley is a Senior Consultant in the Technology Segment at FTI Consulting. As a digital forensic and e-Discovery consultant, she specializes in forensic collection, data analysis and assist in expert reporting of digital evidence. Shirley has been involved in matters relating to Intellectual Property (IP) theft, information leakage, bribery and corruption, and other employee-related misconduct. She has more recently attained GIAC Certified Forensic Examiner (GCFE), and is part of their advisory board.

Date: 3 October 2024, Thursday
Time: 6PM – 8.30PM
Venue: JustCo @ Marina Square
Registration: https://www.eventbrite.sg/e/aisp-lite-sig-meetup-tickets-979651402717
*AiSP members who would like to bring a non member for the event can reach out to secretariat@aisp.sg for a 50% discount code.

back to top

The Cybersecurity Awards

THE CYBERSECURITY Awards 2024

Thank you for your support! The Cybersecurity Awards 2024 nominations has ended and the awards ceremony will be on 7 November 2024.

Professionals
1. Hall of Fame
2. Leader
3. Professional

Students
4. Students

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

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.

THE CYBERSECURITY Awards 2024
ORGANISED BY
AiSP Advance Connect Excel
SUPPORTED BY
CSA SINGAPORE
Cyber Security Agency of Singapore
SUPPORTING ASSOCIATIONS
CSA cloud security alliance SINGAPORE CHAPTER
CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES
ISACA Singapore Chapter
ISC2 CHAPTER SINGAPORE
OT-ISAC
SCS Singapore Computer Society
SGTECH WHERE TECH MEETS
THE LAW SOCIETY OF SINGAPORE
PLATINUM SPONSORS
CISCO
HUAWEI
ST Engineering
GOLD SPONSORS
BeyondTrust
DBS
ENSIGN INFOSECURITY
SANS
SIT SINGAPORE INSTITUTE OF TECHNOLOGY
TREND MICRO
WISSEN Cyber Security Competency Development
wizlynx group

back to top

Regionalisation

SEA CC Webinar – Ladies in Cyber on 5 September

SEA CC Webinar – Ladies in Cyber

VIVIEN TAN
Project Manager, CyberSafe
AIMI RAMLEE
co-founder / director of digital innovation & growth
SEA CC WEBINAR
Ladies in Cyber
5 | SEPTEMBER 2024
3 - 5 PM SGT
ASSOC. PROF. TS. DR. NOOR AFIZA MAT RAZALI
Associate Professor, Defence Science and Technology Faculty at the National Defence University of Malaysia
JEIA TIRANTE
- IT Risk Management Head
- WiSAP Technical Committee Expert
- Senior Lecturer (U.P. - Technology Management Center)
ORGANISED BY:
AiSP
APTIKNAS
BRUNEI CYBERSECURITY ASSOCIATION
ISAC-CAMBODIA
MBOT
MiSA
TISA
VNISA
WiSAP

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 Ladies in Cyber as part of the International Women in Cyber Day on 1st September.

Bridging the Gap: Effective Communication in Cybersecurity for Vendor-Customer Success
Speaker: Vivien Tan, Project Manager, CyberSafe

In an era where cybersecurity is paramount, effective communication between vendors and customers is crucial. This presentation delves into the importance of clear, concise, and jargon-free communication in building trust, fostering collaboration, and ensuring successful cybersecurity outcomes.

- We will explore:
    - **The Vendor-Customer Disconnect:** Highlighting the common challenges arising from technical jargon and misaligned expectations.
    - **Value-Driven Communication:** Strategies for translating technical complexities into tangible benefits for end-users.
    - **Addressing Customer Concerns:** Proactive approaches to understanding and alleviating customer anxieties about data access and security vulnerabilities.

back to top

Securing Feminist Advocacy: Cybersecurity Priorities for International Nonprofits
Speaker: Aimi Ramlee, co-founder / director of digital innovation & growth

In a digital world where threats are increasingly sophisticated, international nonprofits—particularly feminist organizations—face unique cybersecurity challenges. This 20-30 minute session will explore the specific cybersecurity priorities for these groups, focusing on how they can protect sensitive data, secure communications, and maintain the privacy of their activists and beneficiaries. The presentation will outline the most pressing digital threats, from phishing and data breaches to state-sponsored attacks, and offer practical strategies for building resilient cybersecurity frameworks.

Women in AI for Cybersecurity: Opportunities and Challenges
Speaker: Assoc. Prof. Ts. Dr. Noor Afiza Mat Razali, Associate Professor, Defence Science and Technology Faculty at the National Defence University of Malaysia

Artificial Intelligence (AI) is transforming cybersecurity by providing advanced tools with advanced machine learning and deep learning strategies to combat increasingly sophisticated cyber threats. Despite AI's growing importance, women remain underrepresented in cybersecurity roles, which limits the diversity of perspectives necessary for innovative problem-solving. The demand for AI and cybersecurity professionals creates a pivotal moment to address this gender gap by encouraging more women to enter and excel in these fields. However, women often face barriers such as gender bias, underrepresentation, work-life balance issues, and networking gaps. Overcoming these obstacles requires targeted educational programs, mentorship and industry initiatives focused on diversity and inclusion. Let's discuss more about the opportunities and challenges!

Essential IT Risk Management Practices for Philippine Banks
Speaker: Jeia Tirante, IT Risk Management Head (a financial organization)•, WiSAP Technical Committee Expert & Senior Lecturer (University of the Philippines - Technology Management Center)

Information Technology as a competitive advantage for Philippine Banks has become a must-have. Managing the risks associated with ownership, adoption, and operation of IT is important for all industries, especially financial organization. This session will focus on the fundamentals of IT Risk Management for Philippine Banks covering the following areas:

- IT risk management system
- Information security standards and guidelines
- Project management, acquisition, and change management standards and guidelines
- IT Operations standards and guidelines
- IT Outsourcing standards and guidelines
- Reporting and notification standards

Date: 5 September 2024, Wednesday
Time: 3PM – 5PM (SGT)
Venue: Zoom
Registration:
https://us06web.zoom.us/webinar/register/7217243795901/WN_BQ9X8adGSvasmw5FY8El_g

back to top

Ladies In Cyber

Pledging of Friendship Circles on 18 August

AiSP Ladies in Cyber EXCO Lead - Ms Judy Saw represented AiSP to join 15 other female organisations in the pledging of Friendship Circles to organising at least two mentorship circle sessions over two years as part of the (SHE Singapore) SHE Supports initiative with National Trades Union Congress (NTUC). Friendship Circles, a mentorship programme designed to build networks and communities among women. The friendship circles is based on the concept of mentoring circles, the many-to-many programme leverages the expertise of women mentors to foster a supportive environment where women can share experiences, discuss strategies, address common challenges, and receive guidance from mentors across various industries. Thank you SMS Sim Ann and Sister Yeo Wan Ling for witnessing the pledging and having AiSP Ladies in Cyber charter to be part of this meaningful event to reach out to more females.

back to top

Ladies in Cyber Symposium 2024 on 30 August

AiSP Ladies In Cyber Symposium 2024 with the theme "Bridging the Gap in Cybersecurity Talent" was successfully held on 30 August with more than 150 attendees in celebration of the International Cyber Women Day. During the symposium, we launched the Ladies in Cyber Online Cyber Queens: Bug Bounty Challenge an initiative aims to empower women in cybersecurity—students, professionals, and enthusiasts alike—by providing them with opportunities to test their skills in real-world scenarios, continuously improve, and earn rewards for identifying and resolving vulnerabilities.

Thank you panellists, MOS Rahayu, Ms Judy Saw, Dr Jeannie Lee & Ms Jasie Fon for the insightful panel discussion and not forgetting Ms Jasie Fon for her wonderful personal sharing after the panel discussion too!

Thank you Mdm Rahayu Mahzam, Minister of State, Ministry of Digital Development and Information for gracing the event and encouraging more women to take on leadership roles in cybersecurity. A huge thank you to everyone who have joined us and our sponsors Itel Learning, Ping Identity, MINDEF SID, SIT, Wissen International and supporting partners, NYC, SHE,SINDA,TTAB,U Associate, U Women and Family and Yayasan Mendaki who have contributed to making this symposium a memorable and impactful event!

Just make it happen!
Ladies in Cyber Symposium 2024
30 Aug 2024
6PM - 8:30PM
Guest of Honour
Minister of State, Ministry of Digital Development and Information
Mdm Rahayu Mahzam
AiSP

back to top

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
2 Sep	Grab Digital Adoption and Anti Scam Awareness	Partner
3 Sep	DevSecOps SIG Meetup	AiSP
4-5 Sep	OT-ISAC Summit 2024	Partner
5 Sep	LIC Webinar with SEA CC	AiSP
14 Sep	Anti Mooncake Scam cum Learning Journey with Huawei	AiSP & Partner
17-20 Sep	Learning Journey to Brunei	AiSP
18 Sep	SEACC Forum	AiSP
23 Sep	CISO SIG Meetup at Schneider Electric	AiSP & Partner
24 Sep	Cloud Security Summit	AiSP
26 Sep	NTUC Labour Research Conference 2024	Partner
28 Sep	DFL at Jurong Spring CC	Partner
1 Oct	QiSP Workshop	AiSP
3 Oct	LITE SIG Meetup	AiSP
7 Oct	Learning Journey to Grab by RP Students	AiSP & Partner
9-10 Oct	SMEICC 2024	Partner
9-10 Oct	Cyber Security World Asia / Cloud Expo	Partner
10 Oct	SEA CC Webinar - AI	AiSP & Partner
15-17 Oct	Govware	Partner
17 Oct	Asean-Japan Cybersecurity Community Alliance Conference	AiSP & Partner
24 Oct	URA Growth Nodes Exhibition	Partner

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

back to top

CONTRIBUTED CONTENTS

Article from CISO SIG

Dennis Chan is currently the Chief Security & Privacy Officer (CSPO) of Huawei International Pte Ltd, where he oversees and manage the governance, risk and compliance of Huawei businesses in both Singapore and Brunei. He is also responsible for policy communication and strategic partnership on cyber security and data privacy with the government stakeholders and certification bodies.

Dennis had over 15 years of ICT sales experience covering both public and private sectors with proven track records and experience in leading team of sales and pre-sales in Huawei. Prior to his current role, he has served as the Vice President (Government Affairs). Dennis is certified with CCSKv4 and other industry certifications, also trained in cyber risk management, audit and compliance. Dennis is also a member of IT Standards Committee (IOT Security) Workgroup and volunteering in SGTech Digital Trust Chapter.

1. **Introducing CISO with a deep interest in cybersecurity**

As our organization and society are embracing digitization for business transformation, naturally will expand our exposure to risks. But we should not be shy away from digitization, but CISO to take up the responsibilities to understand these possible risks and introduce controls or measures over such risks so that the organization or society can continue to reap the benefits of digitization

2. **What brought you to the Cybersecurity industry?**

I have chanced upon cybersecurity while I was doing sales for public sector years back, where I need to bring my knowledge on cybersecurity governance and risk management up to speed and that was the time I found the importance of cybersecurity

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

Not only i have helped my organization to build the trust and confidence of regulators and customers, but also to localise best practices for my internal organization

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

Driving cybersecurity awareness within my internal organisation, as knowledge and awareness is one of the best line of defence in cybersecurity. And as a member of AiSP I can also extend my knowledge and engage with local communities thru grassroot programs like Digital For Life

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

back to top

1) Ransomware and Phishing will continue to be top threats, hence internal training for management and staff is important
2) Vulnerability and Human Factor will be crucial as more organization or companies are operating more complex IT environment
3) While AI may introduce new risks or threats, but AI can also be a good assistant for cybersecurity, eg. threat hunting or analysis
4) Foreseeing future threats may be of situational-aware and/or behavioural which make detection and analysis more challenging

6. **What do you think is the role of CISO?**

Main part of the role is risk and compliance management including audit, establish policies and protocols on incident response and recovery, budget planning for cybersecurity and data protection, upkeeping security awareness and knowledge within the organization (including board and management)

7. **What can we do to encourage more people to join the cybersecurity sector?**

Getting CISOs or cybersecurity professionals to share on career success stories and accomplishments at campus talk, identify potentials via challenges or competitions (eg CTF, hackathon) . In fact mid-career conversion is a good opportunity to capture talents too.

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

Cybersecurity is about ecosystem and collaborative effort, hence doing my part in making Singapore a cyber-safe nation in any way that I may contribute, eg. lead an interest group in association and as simple as sharing cybersecurity tips at community roadshows

9. **Any advice for the Cybersecurity Professionals?**

Advanced technologies evolve much faster than the way we learn about the technology, hence lifelong learning will allow us to remain relevant in the market and also to track closely on trends

back to top

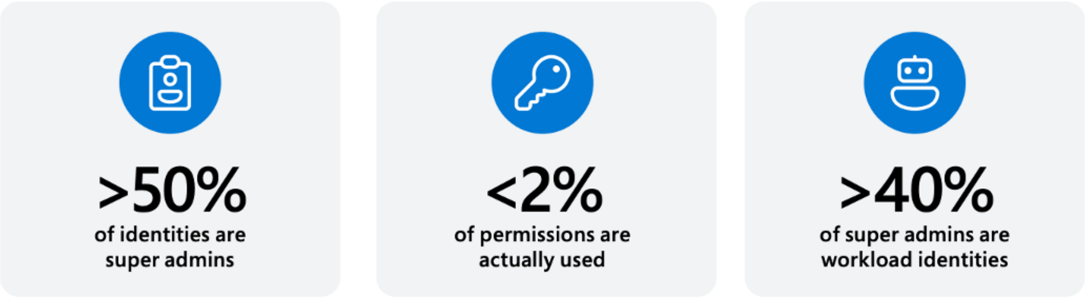
Article from Cloud Security SIG

Striking the right balance:- Zero Standing Access Approach for AWS Access from CSCIS

Rajnish Garg, CISSP CSCIS Cloud Security Member

As we all are aware of the fact that Cloud consoles should be considered as Privileged Access. Insufficient access control and unauthorised access due to credential theft and cookie stealing are the leading causes of many cloud security incidents. Strong access control policies and practices, such as multi-factor authentication, least privilege and providing just enough access, can help mitigate these risks.

The State of Cloud Permission Risks Report by Microsoft highlights a common issue in cloud service provider (CSP) environments, where a significant number of identities are granted super admin permissions, even though they only require a small subset of those permissions to perform their job functions.

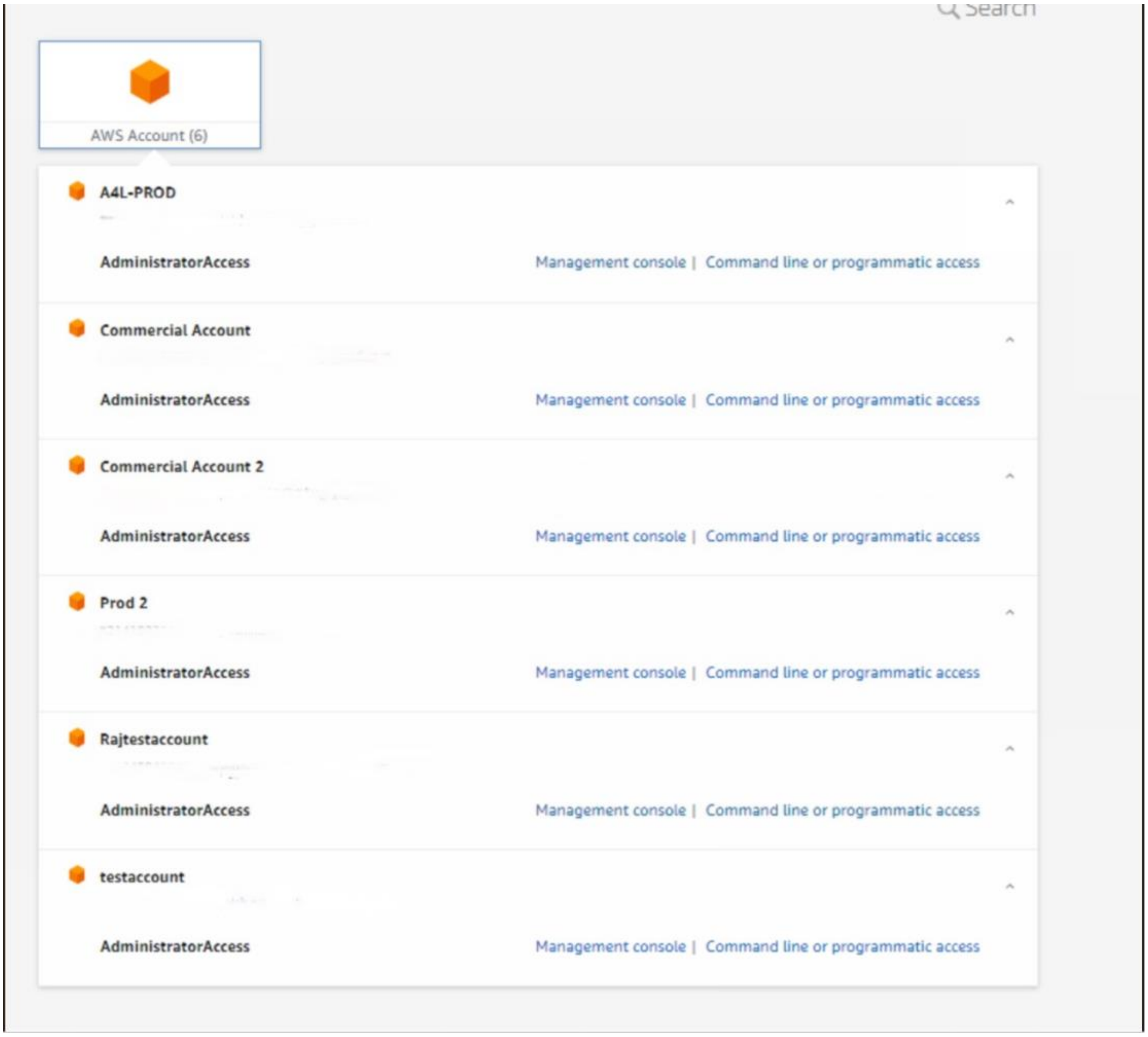


State of Cloud Permission Risk Report

Super admin permissions provide a user with access to all areas of a cloud environment and the ability to perform any action, which can make them a high-value target for attackers.

Current State:-According to a Microsoft Cloud Permission report, it is quite common for half of the identities in cloud environments to be granted administrator access, and cloud team members often receive administrator access for the entire AWS organization.

Below mentioned is the typical example what many of the organization may have adopted where any cloud or security admin when logs into the AWS IAM identity centre, and simply gets Administrator Access across all the AWS Accounts within an organization.



A4L-PROD
AdministratorAccess — Management console | Command line or programmatic access

Commercial Account
AdministratorAccess — Management console | Command line or programmatic access

Commercial Account 2
AdministratorAccess — Management console | Command line or programmatic access

Prod 2
AdministratorAccess — Management console | Command line or programmatic access

Rajtestaccount
AdministratorAccess — Management console | Command line or programmatic access

testaccount
AdministratorAccess — Management console | Command line or programmatic access

Typical Access for the Organization Cloud Team

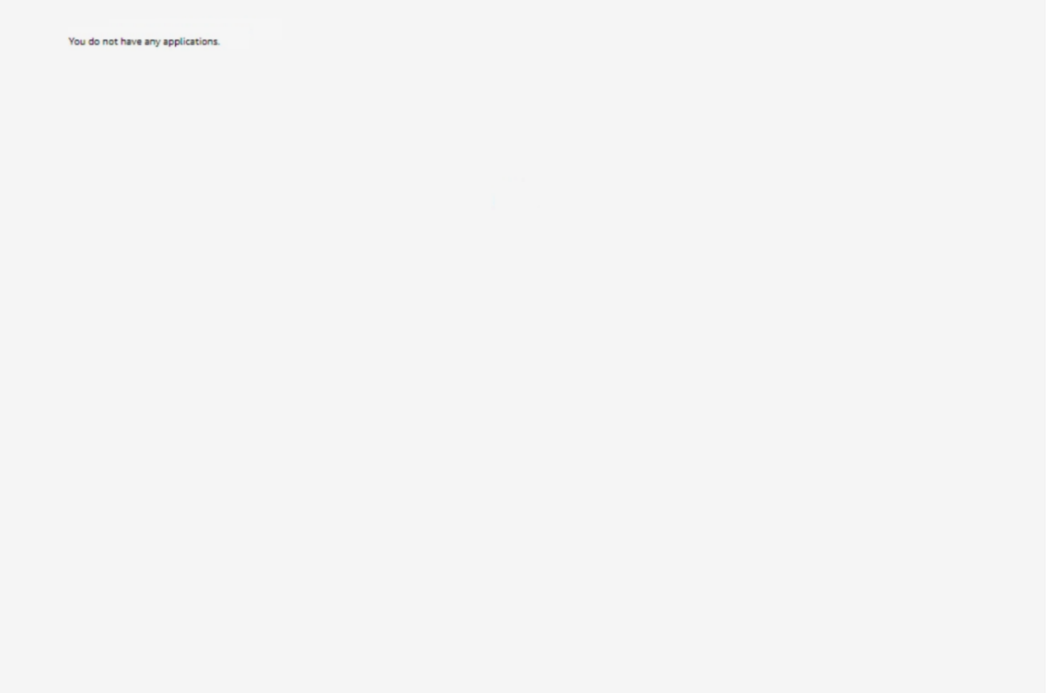
Just imagine- If a rogue employee or someone with authorized access misuses their privileges or can be unauthorized access via credential theft/cookie theft, it can cause significant damage to an organization. They could steal sensitive data, modify or delete critical resources, or launch attacks on other systems or accounts. This could lead to financial losses, legal liabilities, regulatory fines, damage to reputation, and other serious consequences.

back to top

To-Be State

Here are few thoughts organization can adopt to reduce the entire risk.

1. First of all-No standing access at all. By default, employees should have no access at all whenever they access to the AWS IAM Identity Centre.

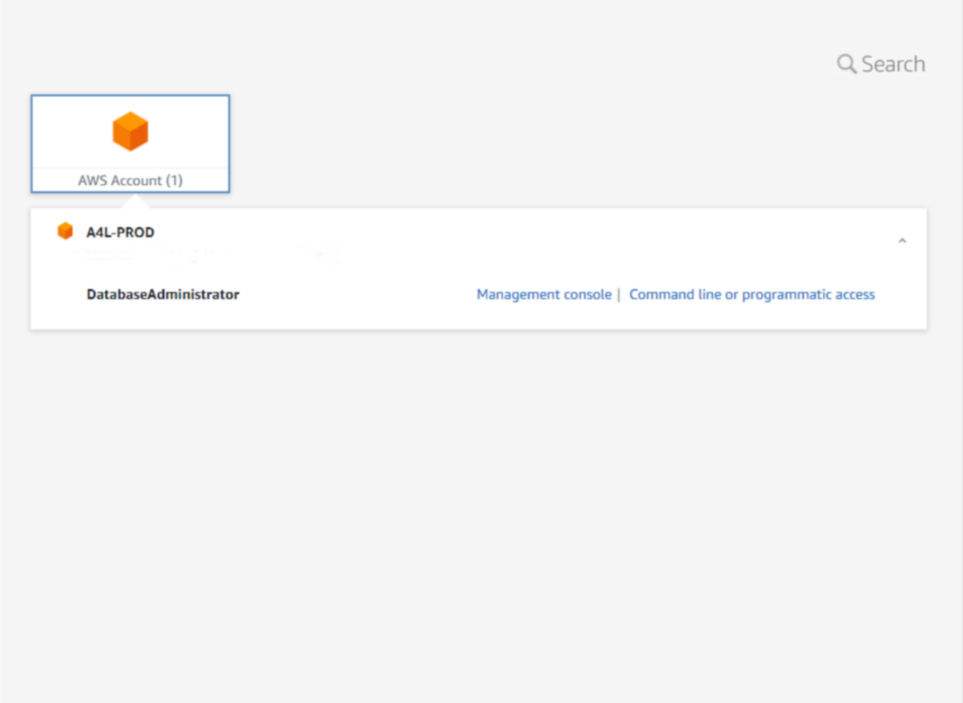


You do not have any applications.

No Standing Access

2. To perform any task within the AWS env. With the help of external automation tool, user should get added automatically to the specific permission set for a given account for a specific timeframe only.

back to top

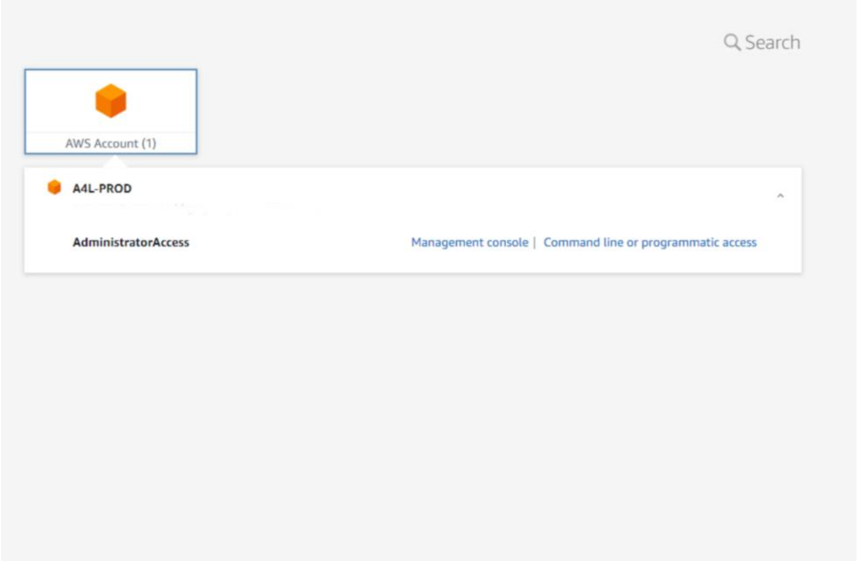


Users get added to the Specific Permission Set Only

Once timeframe expires, user should get removed automatically from the specific permission set.

3. In case of any Super Admin access such as AWS Administrator IAM Administrator access required for the Production accounts, users should go through the proper workflow approval.

Once approval are sought with a proper justification, user get added to the specific permission set for a specified timeframe. There are lot of tools out there for workflow approval such as ServiceNow, Slack, MSFT teams etc.



Super-Admin Access only after Proper Workflow Approval

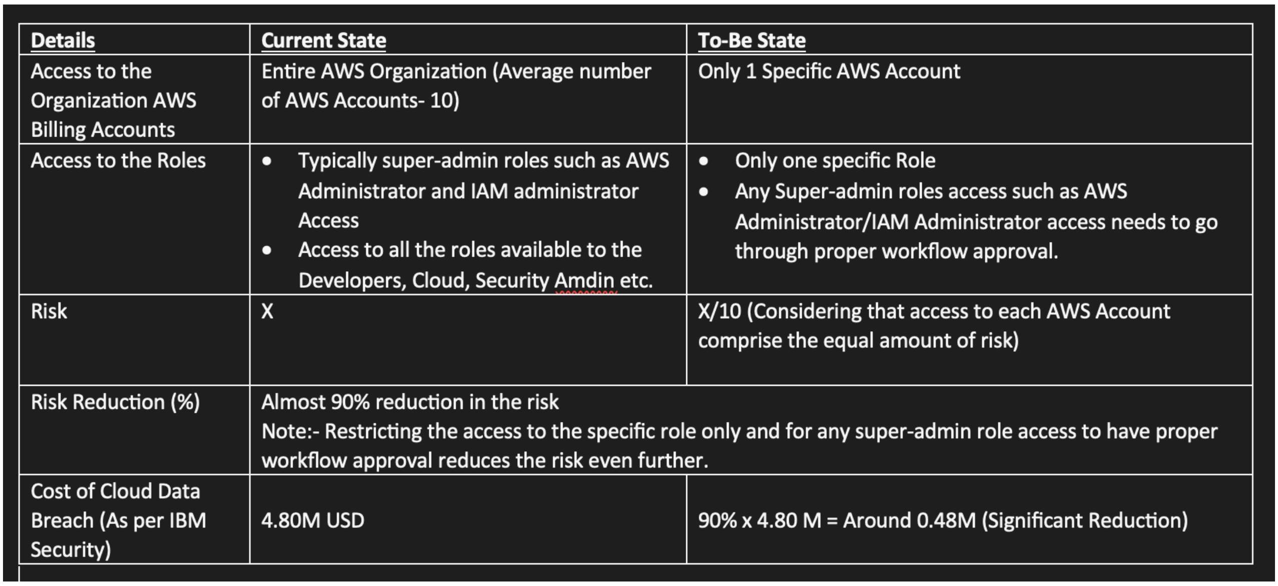
back to top

What's the business value?

- Reduce the risk

1. Theft of intellectual property, trade secrets, and other confidential information, which can be highly damaging to a company's competitive position and brand reputation.
2. Regulatory and compliance considerations that must be taken into account when using cloud services. For example, companies may need to comply with data protection regulations such as GDPR or HIPAA, which can impose significant fines and legal liabilities in the event of a breach.
3. To manage the Cyber Insurance Premium

- Here is potential risk reductions what businesses can consider for the proposed approach.



Details	Current State	To-Be State
Access to the Organization AWS Billing Accounts	Entire AWS Organization (Average number of AWS Accounts- 10)	Only 1 Specific AWS Account
Access to the Roles	• Typically super-admin roles such as AWS Administrator and IAM administrator Access • Access to all the roles available to the Developers, Cloud, Security Amdin etc.	• Only one specific Role • Any Super-admin roles access such as AWS Administrator/IAM Administrator access needs to go through proper workflow approval.
Risk	X	X/10 (Considering that access to each AWS Account comprise the equal amount of risk)
Risk Reduction (%)	Almost 90% reduction in the risk Note:- Restricting the access to the specific role only and for any super-admin role access to have proper workflow approval reduces the risk even further.	
Cost of Cloud Data Breach (As per IBM Security)	4.80M USD	90% x 4.80 M = Around 0.48M (Significant Reduction)

Potential Risk Reduction

How to achieve it ?

- AWS provides the extensive API's to manage access with the AWS IAM Identity centre. With the help of the automation tools, organization can provide the access on the fly.
- Here are few AWS CLI commands organization can leverage upon to add, delete or list users access for the specific permissions sets.
- https://awscli.amazonaws.com/v2/documentation/api/2.1.29/reference/sso-admin/index.html#cli-aws-sso-admin
- List Assignments

back to top

  - https://awscli.amazonaws.com/v2/documentation/api/2.1.29/reference/sso-admin/list-account-assignments.html
  - Example from my AWS environment:-
  - aws sso-admin list-account-assignments --instance-arn arn:aws:sso:::instance/ssoins-8210b98ad604XXX --account-id 19XXXXXXXX --permission-set-arn arn:aws:sso:::permissionSet/ssoins-8210b98ad604XXXX/ps-1eb8baed86XXXXX
- Add Assignments
  - https://awscli.amazonaws.com/v2/documentation/api/2.1.29/reference/sso-admin/create-account-assignment.html
  - Example from my AWS environment:-
  - aws sso-admin create-account-assignment --instance-arn arn:aws:sso:::instance/ssoins-8210b98ad60XXXX --target-id 19533533XXXX --target-type AWS_ACCOUNT --permission-set-arn arn:aws:sso:::permissionSet/ssoins-8210b98ad60421e1/ps-1eb8baed86f84cc8 --principal-type USER --principal-id b9fab5fc-3061-70ae-f902-438bXXXXX
- Delete Assignments
  - https://awscli.amazonaws.com/v2/documentation/api/2.1.29/reference/sso-admin/delete-account-assignment.html
  - Example from my AWS environment:-
  - aws sso-admin delete-account-assignment --instance-arn arn:aws:sso:::instance/ssoins-8210b98ad60XXXX --target-id 19533533XXXX --target-type AWS_ACCOUNT --permission-set-arn arn:aws:sso:::permissionSet/ssoins-8210b98ad60421e1/ps-1eb8baed86fXXXX --principal-type USER --principal-id b9fab5fc-3061-70ae-f902-438bea4eXXXX

back to top

Article from AI SIG

With GenAI-powered phishing threats, it's time to rethink cybersecurity training

By Shannon Murphy, Global Risk and Security, Strategist, Trend Micro

Driven by a growing digital economy and rapid digital penetration, cybercriminals are going on phishing trips in Southeast Asia with increasing frequency. A recent report found that the region experienced a 48% increase in phishing URLs in 2023 alone. In Singapore, phishing attempts more than doubled between 2021 and 2022, making it the fourth most common scam in the city-state.

Beyond the sheer volume of attacks, the sophistication of phishing techniques is also advancing. Historically, cybercriminals employed broad-spectrum phishing, mass-sending generic emails or texts to gather sensitive information, and spear-phishing, which used detailed personal information from social media to craft highly specific messages targeting high-value individuals or organisations.

As such, traditional phishing awareness training focused on spotting suspicious emails and language quirks – and was fairly effective. However, GenAI has transformed the face of phishing by generating realistic, context-aware messages that mimic legitimate communications in language, style, and tone. AI-powered tools can even break language barriers, allowing cybercriminals to target a global audience with accurate translations that incorporate cultural nuances. Consequently, traditional training is no longer sufficient against GenAI's capabilities.

Countering AI-Assisted Phishing Begins with the Zero Trust Framework

Defending against deception-driven attacks is not solely a technological battle; it is equally a human challenge, necessitating a combination of adjustments across people, process, and technology to fortify organisations against emerging threats.

It starts with adopting a Zero Trust — or 'never trust, always verify' — philosophy and building a security culture. Organisations should always verify identities, and allow only necessary people and machines to access sensitive information or processes for defined purposes at specific times. This limits the attack surface and slows attackers down. AI-driven detection tools, such as writing style analysis, computer vision, can further help protect the enterprise and support employees in identifying malicious content and behaviour more efficiently.
Beyond technological defences, organisations should implement processes such as multi-stakeholder approval for significant transactions and establish a 'safe list' of numbers for live voice authorisation calls, rather than relying on a phone number embedded within a transfer request email. These measures can prevent attacks, even

back to top

as cybercriminals increasingly use convincing voice deepfakes. Coded language could even be used for additional authentication.

At the same time, cybersecurity awareness training also needs to evolve accordingly — rather than focusing solely on identifying suspicious or malicious emails, it should educate employees on when and how to execute the above processes to prevent successful phishing attempts. These sessions should include simulations of phishing attacks to provide practical experience in identifying potentially suspicious situations — not just emails — and executing the related verification processes.

Most importantly, cybersecurity training should not be a one-time event but an ongoing process with content that is regularly refreshed and updated with the latest phishing techniques, which are constantly evolving with advancements in AI.

Staying Ahead of Cybercriminals with a Unified Approach

However, as the digital attack surface continues to expand through digital and AI transformation, cyber threats like phishing attacks will continue to become increasingly sophisticated and well-coordinated. This growing complexity is even more concerning due to the persistent talent and resource gap that organisations face in keeping up with the rapidly evolving threat landscape.

More than ever, businesses need to adopt a proactive posture towards cybersecurity. This involves moving away from traditional approaches of security — which is to apply uniform security measures across all known systems — and adopting a risk-based approach, which includes continuous asset discovery and assessment to focus on prioritising and building the appropriate controls for the most critical vulnerabilities.

A unified cybersecurity platform helps empower businesses by providing comprehensive visibility and centralised risk management, enabling quick detection and response to anomalies. This combination allows businesses to identify the most at-risk assets and potential intrusions, preventing and mitigating threats before they cause significant harm.

Ultimately, there isn't one single way of combatting security threats — the most effective approach is one that combines all of the above. By equipping employees with better, smarter tools and a comprehensive understanding of security practices, businesses can more effectively combat cyber threats and protect their digital assets and brand.

For more information please contact, joycelynn_teh@trendmicro.com

back to top

Article from SVRP 2023 Gold Winner, Ho Zhi Hao [RP]

How do you think SVRP has directly impacted your cybersecurity journey?
SVRP has allowed me to stay on track and relevant with cybersecurity. Since my passion is in cybersecurity, it ensured me to participate actively in the cybersecurity track. SVRP allowed me to have the opportunities to organize and arrange for cybersecurity related workshops. For instance, at multiple instances, I was able to work with CSA so that I am able to garner more skills and awareness in cybersecurity. For instance, I was able to work with CSA on a weekend to spread awareness about cybersecurity and online scams.

How has SVRP inspired you to contribute to the cybersecurity field?
SVRP has inspired definietly alot of people to contribute to the cybersecurity field. For instance, SVRP has given us multiple opportunities to run events and participate in events. One of which would be The Youth Cyber Exploration Program which allowed me and my peers to work together to come up materials to teach the secondary school students that have participated in the event. At many points of times, we have to work closely with one another so that we can gel our CTF competition together for the different flags that were created. For instance, since we have came up with a problem solution, the different concepts that were taught in the first two days must be linked with one another. Another way where SVRP has inspired my peers and I to contribute to the cybersecurity would be my interest group, Hextech, since we are working closely such that my peers and I are able to run multiple events and workshops together.

back to top

What motivates you to be a student volunteer?
My motivation starts all the way before stepping into cybersecurity. I started to be a student volunteer for multiple events outside of cybersecurity. However, when I stepped into Republic Polytechnic, there were many opportunities that were given to me so that I am able to carry out events that are related to cybersecurity as a student volunteer. For me, I felt fortunate as I was able to work closely with cybersecurity with the fact that I have to run an interest club called Hextech. Hextech is where I showcase and spread awareness about Cybersecurity to my peers. My peers and I are able to organize CTF competitions for my other peers to join and win prizes and at the same time they are able to learn about the different concepts that they were taught in the cybersecurity diploma, DISM.

How would you want to encourage your peers to be interested in cybersecurity?
As I continue to learn about cybersecurity whether be it in Republic Polytechnic or University when I graduate, I would want to encourage my peers to be interested in cybersecurity in many aspects. One of which would be to organize more cybersecurity related events so that both my peers and I can learn. For myself, when I carry out such events, I am both learning better and sharpening my skills so that I can improve more on my skills. An additional way to encourage my peers to be interested in cybersecurity is to allow them to participate in more events with me be it a CTF competition or an awareness workshop. This allows them to learn more with me in cybersecurity and stay relevant and at the same time allowing them to be interested in cybersecurity. Since most of my friends are interested in cybersecurity because of the practicals and demonstrations that I have performed in school for different workshops, I think that they are more of a practical person. This is where I would want to encourage my peers to be interested in cybersecurity using demonstrations and more cybersecurity practical. I hope with the different kinds of demonstration, it will spark my peers with different interest or passions in cybersecurity.

back to top

PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®)

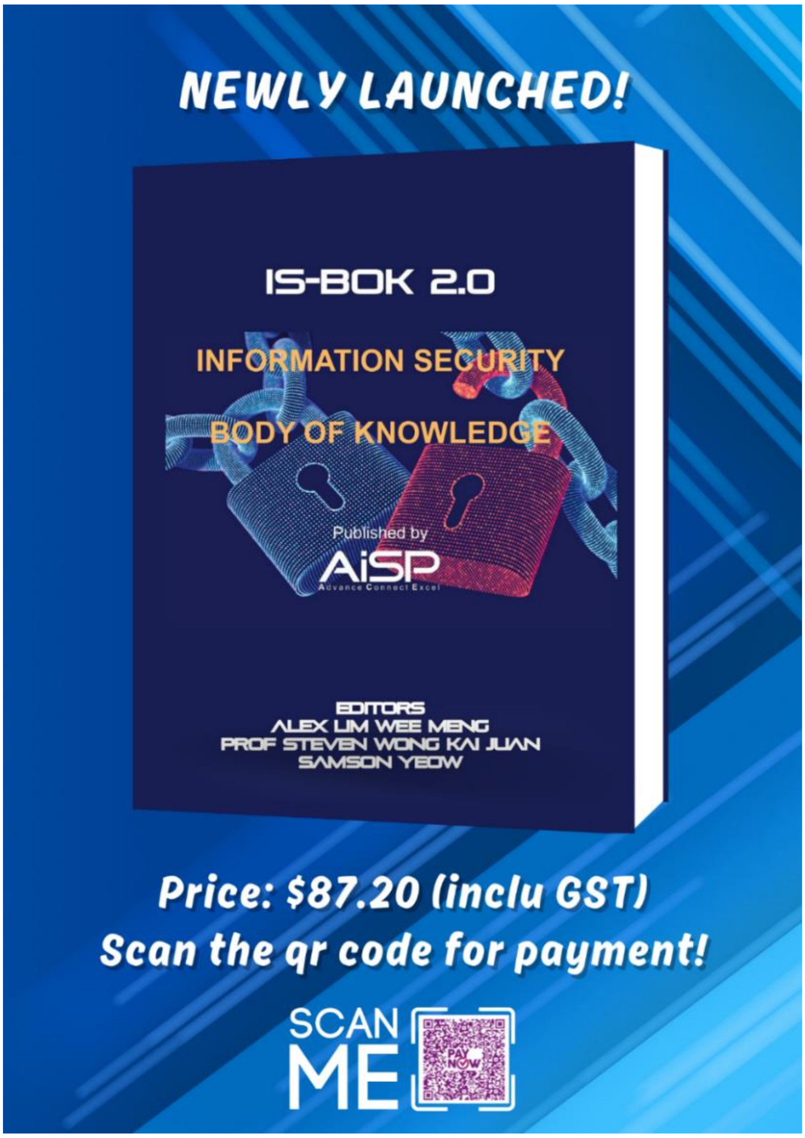
QISP Insight Masterclass on 1 and 5 August

QISP Training Partner, Wissen International conducted two 1-day introductory class on QISP for AiSP Corporate Partner, Huawei on 1 and 5 August respectively. More than 100 participants attend the session both online and physical. The sessions provided the participants with valuable insights into the QISP framework and they enjoyed the collaborative learning experience.

back to top

Body of Knowledge Book (Limited Edition)

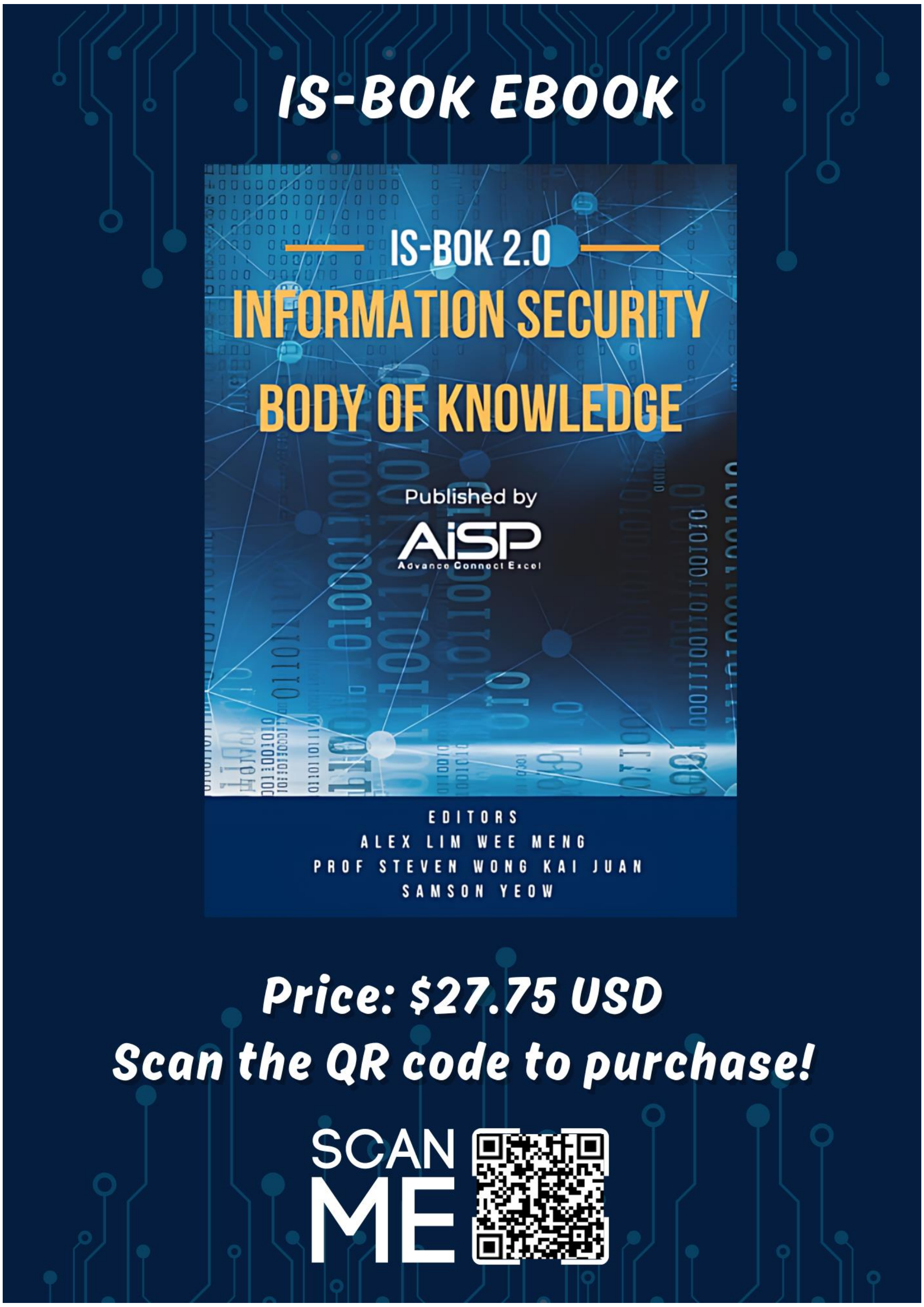
Get our **Limited Edition** Information Security Body of Knowledge (BOK) Physical Book at **$87.20 (inclusive of GST)**.



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. **Last 30 books for sale!**

back to top

Body of Knowledge E Book



back to top

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

AiSP QISP Workshop on 1 October

AiSP Advance Connect Excel

AiSP QISP Workshop

AiSP Advance Connect Excel

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 AiSP

SUPPORTING AGENCY CSA SINGAPORE

TRAINING PARTNER WISSEN Cyber Security Competency Development

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.

back to top

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 firsthand 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 (*Please note the full amount paid via above link will be FULLY REFUNDED including the Eventbrite admin.fees)*

back to top

Online Course launched on 1 March 2024!

QISP Exam Preparatory E-Learning Course

Governance and Management

Physical Security and Business Continuity

Security Architecture and Engineering

Operation and Infrastructure Security Software Security

Software Security

Cyber Defense

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!

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!

back to top

Advertisements

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 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

back to top

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 CRT 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.

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.

back to top

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

back to top

AiSP Corporate Partners

Acronis

athena dynamics

AZ ASIA-PACIFIC

BD

BeyondTrust

BLACKPANDA

bugcrowd

CISCO

CLIXER

C8N+FINITY

CSA SINGAPORE

CSIT Centre for Strategic Infocomm Technologies

CYBERSAFE YOUR SECURITY, OUR PRIORITY

DBS

DETACK

DSTA Defence Science & Technology Agency

eclypsium

ENSIGN INFOSECURITY

FORTINET

Genesis NETWORKS

GOVTECH SINGAPORE

Grab

HORANGI CYBER SECURITY

HUAWEI

illumio

image engine

INTfinity

ITSEC ASIA

KnowBe4 Human error. Conquered.

MAGNET FORENSICS

back to top

MySQL™	M.TECH Your Preferred i-Security Partner	oneSECURE®
opentext™	OPSWAT.	PARASOFT®
RAJAH & TANN CYBERSECURITY	Responsible Cyber	RSM
SailPoint	SCANTIST	Schneider Electric
Security Scorecard	Singtel	softScheck We Build Trust
ST Engineering	TEMASEK	tenable
TREND MICRO™	VECTRA®	Veracity Trust Network
VOTIRO	WISSEN Cyber Security Competency Development	wizlynx group
xcellink.pte.ltd. completing your technology chain	YesWeHack	

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

back to top

AiSP Academic Partners

ITE Institute of Technical Education

NYP NANYANG THE INNOVATIVE POLYTECHNIC

NGEE ANN POLYTECHNIC

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

NUS National University of Singapore

REPUBLIC POLYTECHNIC DISCOVER. TRANSFORM. ACHIEVE

SIT SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SMU SINGAPORE MANAGEMENT UNIVERSITY

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek POLYTECHNIC

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.

back to top

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.

back to top