

News & Update

- Knowledge Series
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Special Interest Groups
- The Cybersecurity Awards
- Digital for Life
- CAAP
- Corporate Partner Events
- CREST
- Upcoming Events

Contributed Contents

- CTI SIG: Introduction to the Blue Team
- Blackpanda: SMEs are at risk of Cyber Attacks
- Votiro: Want to chat with Votiro about zero trust content security?
- Beyond Trust: The 2023 Microsoft Vulnerabilities Report
- DT Asia: Reduce Cyber Risk for your Organization
- TCA 2022 Winner – Hoi Wai Khin
- SVRP 2022 Winner – Edwin Chua

Professional Development

Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome Contfinity, Cybersafe Pte Ltd, DT Asia, NCS Group, Security Scorecard and Votiro as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partners



Continued Collaboration

AiSP would like to thank BeyondTrust, Govtech and Singtel for their continued support in developing the cybersecurity landscape:



Annual General Meeting

AiSP held its 15th Annual General Meeting on 30 March at Justco @ Marina Square. AiSP would like to thank Faith Chng, Freddy Tan & Tok Yee Ching for their contributions and support for the past few years as they stepped down from the main EXCO.

AiSP President, Mr Johnny Kho also shared on the few points below during the AGM:

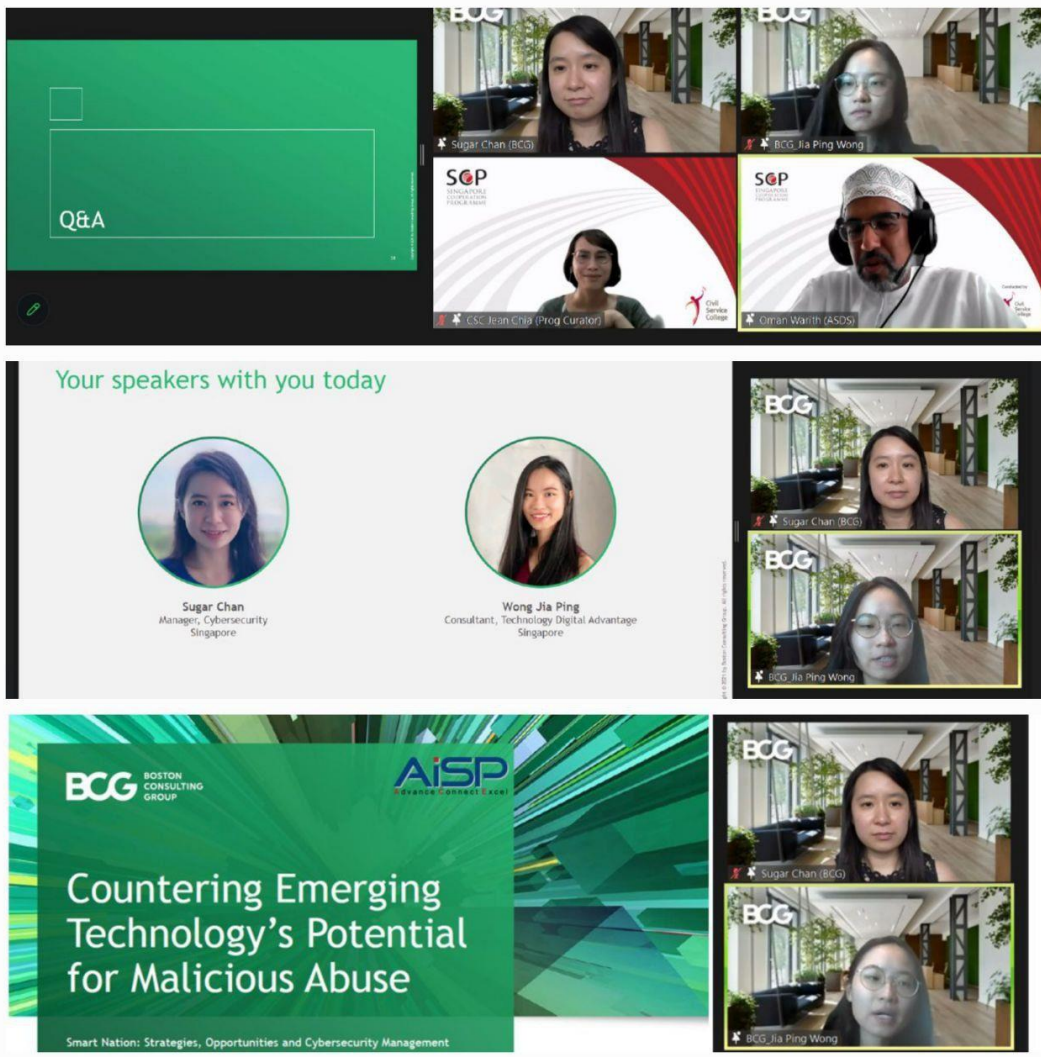
- 1) Growth in Membership and Partnership through Secretariat Outreach
 - a. 12 APPs, 66 CPPs and 2,028 members to date
- 2) Achieved the next milestone in Regionalisation with the forming of the South East Asian Cybersecurity Forum (SEACC)
 - a. SEACC Forum was held on 23 November 2022 with 8 other associations from the SEA region to pledge a commitment in developing and collaborating on more events for the region
- 3) Qualified Information Security Professional (QISP)
 - a. working with training partners to develop the courseware online for Singapore and overseas
 - b. Included 1 more tier of scoring known as Qualified Information Security Associate (QISA) for scoring above 50 and less than 65
- 4) Keeping the momentum with new committee members
 - a. Welcoming Alex Lim, Dennis Chan and Wong Onn Chee to the elected committee 2023



News & Updates

Countering Emerging Technology's Potential for Malicious Abuse on 9 March

Our AiSP EXCO Member Ms Sugar Chan and our corporate partner, BCG shared on the Countering Emerging Technology's Potential for Malicious Abuse in the MFA-SCP Smart Nation virtual programme with 20 Omani delegates on 9 March. We hope they have benefitted greatly from the event.

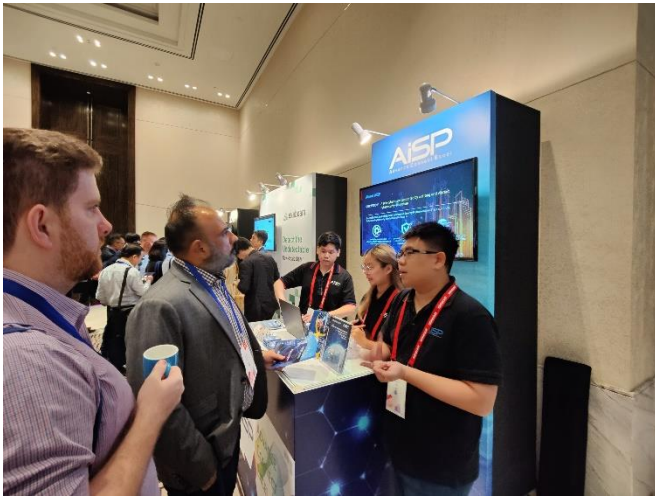


Mimecast Connect Event on 2 March

AiSP was down at the Mimecast Connect event at The Westin Singapore on 2 March to support our AiSP Corporate Partner – Mimecast in their Mimecast Connect Event 2023.

Thank you Mimecast for inviting us to share on AiSP.

We welcome all our Corporate Partners to reach out to us if you are interested for AiSP to support any of your events and have a booth showcase too.



Knowledge Series Events

Upcoming Knowledge Series

Cloud Security on 12 April



AiSP Knowledge Series – Cloud Security

AiSP Knowledge Series

Cloud Security

12 APR 2023 | ZOOM | 3PM – 5PM



Jeff Yeo
Leader, Solutions Engineering – APJ
Cisco System



Susanto Leman
Principal Solution Consultant
Fortinet



Marlene Veum
Independent Cybersecurity Consultant & Advisor, Web3 and Decentralized Technologies
Wissen



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

Supported by



In this Knowledge Series, we are excited to have Cisco, Fortinet & Wissen to share with us insights on Data & Privacy. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

The need for cloud governance model for security and compliance management
Speaker: Marlene Veum, Independent Cybersecurity Consultant & Advisor, Web3 and Decentralized Technologies

Security is also shifting accordingly with the increased adoption of the cloud for faster and more agile performance toward meeting the changing business demands. The need for compliance policies and frameworks in cloud security is motivated not only due to the increased demand and adoption but also because the approach for security in this virtual environment differs greatly from the traditional network-based counterpart. Security and compliance management in the cloud is a subset of the cloud governance framework alongside finance, operation, and data management. These frameworks majorly revolve

[back to top](#)

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

Page 5 of 59

around risk assessment, identity, and access management, data management and encryption, application security, disaster recovery, etc. The current webinar aims at explaining the need and benefits of designing and implementing a cloud governance framework, along with the approach for developing a reliable compliance framework.

Key Takeaways:

- The need for a cloud governance framework
- Security and compliance management
- Prerequisites for designing the cloud governance framework
- Design and implementation of the framework
- Key benefits of a cloud governance framework

The Power of Risk-Based Authentication: Placing Users in the Driver's Seat

Speaker: Jeff Yeo, Leader, Solutions Engineering – APJ, Cisco System

With the rise of hybrid work and the increase in cyber threats, attackers are increasingly targeting account takeovers in an attempt to gain access to corporate resources.

This means user authentication is more important than ever before. However, organizations need to balance the security requirements of this new world without adding unnecessary friction to users who just want to get their job done.

Striking this balance requires risk detection along with automated, and effective, responses to block the attacker before they get access.

Tune into the webinar to find out best practices and innovations to support real-time authentication requirements and meet the needs of a zero-trust environment while ensuring seamless end-user experience.

Securing Digital Transformation Journey to the Cloud

Speaker: Susanto Leman, Principal Solution Consultant, Fortinet

Organizations are rapidly shifting workloads to the cloud to improve responsiveness, reduce costs, and accelerate time to market. With the majority of organizations planning to increase their cloud workloads over the next 12-18 months, it is no surprise that cloud security remains a top concern. In this session, we will discuss the cloud security trends observed in 2022, as well as what you should consider to safeguard your cloud environment and prevent data breach.

Date: 12 Apr 2023, Wednesday

Time: 3PM – 5PM

Venue: Zoom

Registration:

https://us06web.zoom.us/webinar/register/9016758402148/WN_DUYXfAABR5uB3KratTqtgw

Cyber Defence on 25 May



AiSP Knowledge Series – Cyber Defence

AiSP Knowledge Series Cyber Defence

25 May 2023, Thursday | 3PM - 5PM

Zoom



Daniel Chu
VP of System
Engineering, APJ
ExtraHop



Wing Churn Leong
Cloud Security Specialist
Tenable



Sharat Nautiyal
Security Engineering
Leader, Asia
Vectra AI

ORGANISED BY



SUPPORTED BY



IN SUPPORT OF



In this Knowledge Series, we are excited to have ExtraHop, Tenable & Vectra AI to share with us insights on Cyber Defence. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

Owning Your Cybersecurity Midgame Strategy

Speaker: Daniel Chu, VP of System Engineering, APJ, ExtraHop

Prevention is an uphill battle for defenders: attackers only need to succeed once. And, restoring data doesn't negate downtime or the consequences of a data breach. Defenders need a much broader window to catch and stop ransomware before the damage is done and take necessary actions that can alert your team to the intrusion – command and control communications, data staging and lateral movement.

Safeguarding Your Hybrid Multi-Cloud Environments with a Unified Approach to Cloud Security

Speaker: Wing Churn Leong, Cloud Security Specialist, Tenable

From ease of deployment and maintenance, to scalability and flexibility, an increasing number of organizations around the globe are moving their business processes and applications from on-premises to the cloud. The attack surface is getting bigger and more complicated - and the security teams are constantly facing challenges trying to catch up with the changes.

This session will cover areas you should explore when looking for a holistic cloud security solution

- Evolving from Vulnerability Management to Exposure Management
- A unified platform approach - Vulnerability Management and Cloud Security Posture Management
- Key considerations for choosing a cloud security program
- Agentless scanning, automated threat detection and risk prioritisation

Harden Your M365 Tenants

Speaker: Sharat Nautiyal, Security Engineering Leader, Asia, Vectra AI

The M365 cloud provides organizations with unique opportunities to collaborate, but very few organizations have hardened their M365 environment to protect themselves from the rapidly-evolving attacks that focus on Azure AD, Exchange Online, OneDrive and Teams. Join Sharat Nautiyal for an in-depth look at how to harden M365 tenants, establish appropriate controls to detect identity abuse and unauthorized data access and build a program to sustain M365 security success.

Date: 25 May 2023, Thursday

Time: 3PM – 5PM

Venue: Zoom

Registration:

https://us06web.zoom.us/webinar/register/6016799878373/WN_kXhsliwCRqy3BJfB2XwrFw

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its [Information Security Body of Knowledge 2.0](#) topics. Our scheduled topics for webinars in 2023 are as follows (*may be subjected to changes*),

1. Cloud Security, 12 Apr
2. Cyber Defence, 25 May
3. Operations & Infrastructure Security, 19 Jul

Please let us know if your organisation is keen to provide speakers! Please refer to our scheduled 2023 webinars in our [event calendar](#).

Student Volunteer Recognition Programme (SVRP)

Learning Journey to KL Certificate Presentation on 8 March

We have concluded our Learning Journey to KL with a certificate presentation to our students who have joined us last December on 8 March. Thank you to our AiSP Student Volunteer Recognition Programme EXCO Lead & AiSP Secretary, Ms Soffenny Yap for presenting the certificates to the students.

AiSP will be bringing 21 students to Vietnam as part of Singapore & Vietnam 50years anniversary from 17 April 2023 to 21 April 2023. There will also be an upcoming learning journey to Brunei in September and registration is now open. Please fill up the form below if you wish to participate in the Brunei Learning Journey. Slots are limited!

Sign up now at: <https://tinyurl.com/aispbruneisept>



AiSP Bug Bounty Workshop on 13 April



AiSP
Advance Connect Excel

AiSP Bug Bounty Workshop

 13 April 2023, Thursday | 9:30am to 5:00pm

 SIT @ NYP



Bug Bounty Workshop

Organised by   / Supported by   

Initiation into Bug Bounty: Hands-on Workshop
followed by a **Bug Bounty Challenge**



BitK
Tech Ambassador
YesWeHack

Discover Vulnerability Across the Modern Attack Surface with Exposure Management



Dick Bussiere
Technical Head, APAC
Tenable

Build a successful pentest career with EC-Council



Judy Saw
Director of Business Development
Wissen International

In this hands-on workshop, attendees will have the opportunity to get started in the world of Bug Bounty. YesWeHack will provide a pre-configured "hacking playground" – a fake online shop with common vulnerabilities and security flaws – as well as guidance on installing the hacking tools needed to identify and exploit these vulnerabilities. Working independently, attendees will use the tools and techniques discussed in the workshop to find and exploit vulnerabilities in the hacking playground. This workshop is ideal for anyone interested in learning more about Bug Bounty and gaining hands-on experience in a controlled setting. By the end of the workshop, attendees will have a better understanding of the challenges and rewards of Bug Bounty, and be better equipped to start their own Bug Bounty journey.

Participate in our Bug Bounty Challenge and stand a chance to win up to \$300 worth of gift prizes.

AGENDA

0930: **Registration**

1000: **Initiation into Bug Bounty: Hands-on Workshop**
BitK, Tech Ambassador, YesWeHack

1230: **Lunch & Interaction**

1330: **Bug Bounty Challenge**

1500: **Build a successful pentest career with EC-Council**
Judy Saw, Director of Business Development, Wissen International

1530: **Discover Vulnerability Across the Modern Attack**

[back to top](#)

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

Page 10 of 59

1st Prize: Worth \$300 gift prizes
 2nd Prize: Worth \$150 gift prizes
 3rd Prize: Worth \$100 gift prizes

Hear from Judy Saw, Director Business Development, Wissen International on how you can build a successful pentest career with EC-Council.

Hear from Dick Bussiere, Technical Head, APAC, Tenable on going beyond risk-based vulnerability management, Exposure Management helps you discover vulnerability, prevent attacks and accurately communicate exposure risk to enable better business outcomes. In this session, we'll introduce the concept of Exposure Management, explaining how it helps you gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate exposure risk to support optimal business performance.

Date: 13th April 2023 (Thursday)

Time: 9.30AM – 5PM

Venue: SIT@NYP, located at 172 Ang Mo Kio Ave 8, Singapore 567739

Registration: <https://forms.office.com/r/GcH21RVYBd>

Surface with Exposure Management

Dick Bussiere, Technical Head, APAC, Tenable

1630: **Prize Presentation**


1700: **End of Event**



Nomination Period:
1 Aug 2022 to 31 Jul 2023

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 2022 to 31 Jul 2023

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	Example C
+ Leadership: 10 Hours	+ Leadership: 0 Hour
+ Skill: 10 Hours	+ Skill: 36 Hours
+ Outreach: 10 Hours	+ Outreach: 0 Hour
Example B	Example D
+ Leadership: 0 Hour	+ Leadership: 0 Hour
+ Skill: 18 Hours	+ Skill: 0 Hour
+ Outreach: 18 Hours	+ 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

AiSP Cyber Wellness Programme

Organised by:



Supported by:



In Support of:



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



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



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



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



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



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



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



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

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

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



Ladies in Cybersecurity

AiSP Ladies In Cyber International Women Day Celebrations & Learning Journey To SIT@NYP

AiSP celebrated the International Women Day celebrations on 8 Mar 23 at Singapore Institute of Technology with 50 over attendees as part of the AiSP Ladies in Cyber 5 year anniversary and the International Women's Day.

We would like to thank Ms Nadia (Member of Parliament for Ang Mo Kio GRC), our Guest of Honour for joining us in the celebration and dialogue session together with Ms Sandy Cheng (Assistant Director at iHIS) and Dr Purnima (Assistant Professor at SIT@NYP) with our AiSP Secretary and EXCO Lead for SVRP, Ms Soffenny Yap who moderated this event.



[back to top](#)

Ladies in Cyber Symposium on 18 March

AiSP celebrated our AiSP Ladies in Cyber Charter 5years anniversary and the International Women's Day with more than 140 attendees in our second Symposium. During the event, AiSP launched our Bear Mascot – THENA in the celebration. THENA represent the AiSP Ladies in Cyber Charter Programme.

THENA Programme includes:

- Mentorship: THENAs assist others (both internally and externally) to reach their full leadership potential
- Community Service: THENAs devote consistent and continuous time and energy to improve the quality of life for others

We would like to thank our Guest of Honour, Minister Josephine Teo, AiSP Advisory Co-Chair Ms Tammie Tham and Prof Annie Koh, PhD for joining us in the dialogue session with Sherin Y Lee, AiSP Vice-President as the moderator. Also thank you to our Guest speakers: Ms E Fang Yap from NCS group for sharing on the usage of AI in Cloud Security Operations, Ms Alona Geckler from Acronis for sharing on Responsible AI is a Data Privacy Necessity and Ms Eileen Goh from GovTech Cybersecurity Group for sharing on the IoT Security Trends.

Thank you to our supporting partners Acronis, Cyber Security Agency of Singapore (CSA), DBS Bank, GovTech, Ensign InfoSecurity, IMDA, NCS Group, National Trades Union Congress (NTUC) U Associate, SG Her Empowerment, Singtel, People's Association and Tenable for making this event possible.

JOINTLY ORGANISED BY



SUPPORTED BY



SPONSORS



SUPPORTING PARTNERS





Women possess skills to succeed in AI, cyber security: Josephine Teo

Samuel Devaraj

Women possess the skills to succeed in the overlapping fields of artificial intelligence (AI) and cyber security that are in their nascent stage, said Minister for Communications and Information Josephine Teo on Saturday.

Speaking at the Ladies in Cyber Symposium organised by the Association of Information Security Professionals (AiSP) at Capital Tower, Mrs Teo said that while nefarious actors can use AI to break apart cyber-security measures, AI can also be applied in threat containment and identifying suspicious patterns of behaviour.

AI itself is also subject to cyber risk, as it can be tampered with and produce undesirable output, she added.

She said that how the fields of AI

and cyber security come together is an exciting area that currently does not have clear answers.

"Because everything is still at the developmental stage, there is really no reason why a person applying their minds and willing to invest time and effort to acquire the skills cannot over time become very, very well established.

"But it takes effort, there is no easy way of getting it done. It takes hard work. It takes perseverance. It also takes curiosity and a sense of adventure. To my mind, these are attributes that women can be well suited to."

Mrs Teo, who is also the Minister-in-charge of Cyber Security and the Smart Nation initiative, was speaking during a panel discussion that also featured Ensign InfoSecurity group chief executive Tammie Tham and Singapore Management University professor emeritus of finance (practice) An-



From left: Minister for Communications and Information Josephine Teo with Acronis' senior vice-president Aliona Geckler and corporate communication assistant Chia Seok Cheng during the Ladies in Cyber Symposium at Capital Tower on Saturday. Mrs Teo was taking a multitasking abilities test while on an exercise bike during her tour of the booth. ST PHOTO: GIN TAY

nie Koh.

Ms Sherin Lee, who is vice-president of the AiSP, moderated the session.

The theme for this year's Ladies in Cyber Symposium – which is in its second year – was "Pioneering AI And Cyber Security: Women Charting The Course".

Ms Tham highlighted how AI is used by the "bad guys", citing the example of how AI chatbot ChatGPT has been used to make phishing e-mails look more authentic.

But she also noted how AI, which has the ability to make sense of a vast amount of data, has the capability to tackle cyber attacks.

"Even though it is a mouse and cat race, it is very challenging and very interesting," she said.

Ms Tham also encouraged girls and women in the audience to join the cyber-security field.

"Imagine you are the virtual

cop... we are the good people in the cyberspace. We earn our keep, we keep the cyberspace safe not just for ourselves. It's for our family, it's for everybody.

"So it's kind of noble in that sense, it's a higher calling."

In her opening speech, Ms Lee said that in early 2022, the Ladies in Cyber Charter set a goal to empower and mentor 3,000 aspiring women cyber talents by end-2023.

She said: "Today, I am happy to announce that we have surpassed it, with more than 4,000 talented women now part of this initiative. Among them, many are pioneering the course of cyber AI, and in cyber security, charting the course for future generations.

"However, we will continue to strive towards our goal of encouraging more women to join this field."

samuelsd@sph.com.sg

[back to top](#)

Join us in our next AiSP Ladies in Cyber Event on 30 May 23

JOINTLY ORGANISED BY:

AiSP | **LADIES IN CYBER**

SUPPORTED BY:

ENSIGN
INFOSECURITY

SMS Sim Ann
Senior Minister of State in the
Ministry of Foreign Affairs and
Ministry of National Development

Ms Sherin Y Lee
AiSP Vice-President &
Founder for AiSP Ladies in
Cyber Charter

Dr Tan Mei Hui
Vice-President of Cyber
Security Chapter at
Singapore Computer Society

Ms Jackie Low
Deputy Director, Info Sec,
CIO Office of Ensign
InfoSecurity

AiSP will be organising a learning journey to Ensign InfoSecurity on **30 May 2023 from 9am to 12noon** where we will invite about 50 to 70 female Youths from our Student Chapters to come together physically for a day of celebration, learning journey and visiting the Ops Centre at Ensign InfoSecurity and interacting with the working personnel at Ensign. Join us for an afternoon of enriching activities ranging from Dialogue Session with our Guest of Honour, Ms Sim Ann, Senior Minister of State in the Ministry of Foreign Affairs & Ministry of National Development, Recruitment Talk, Internship Opportunities and visit to the Ops Centre. The event is open to all female students in tertiary level.

The details for the event are as follow:

Date: 30 May 2023, (Tues)

Time: 9am to 12noon

Venue: Ensign InfoSecurity (Singapore) Pte Ltd located at 30A Kallang Pl, #08-01, Singapore 339213

Dress code: Smart Casual

Guest of Honour: Ms Sim Ann, Senior Minister of State, Ministry of Foreign Affairs & Ministry of National Development

*Light Refreshments will be provided at the event

Sign up now by **30 Apr 23** at <https://forms.office.com/r/QC9VJ9QK12>

Special Interest Groups

CTI Networking Session on 10 March

On 10 March, AiSP CTI SIG members gathered at Justco Marina for a networking session.



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

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

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



The Cybersecurity Awards



The Cybersecurity Awards 2023 nominations have started on 06 February 2023.

Professionals

1. Hall of Fame
2. Leader
3. Professional

Enterprises

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

Students

4. Students

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

TCA 2023 CALL FOR NOMINATION IS NOW OPEN TILL 14 APRIL 2023

THE CYBERSECURITY Awards 2023

PROFESSIONALS
LEADER
PROFESSIONAL

ENTERPRISES
MNC (VENDOR)
MNC (END-USER)
SME (VENDOR)
SME (END-USER)

STUDENTS

WWW.THECYBERSECURITYAWARDS.SG

**NOMINATION
NOW OPEN**

PLEASE SEND YOUR NOMINATIONS TO
THECYBERSECURITYAWARDS@AISP.SG

In its sixth year, The Cybersecurity Awards 2023 seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems. The Awards are organised by the Association of Information Security Professionals (AiSP), and supported by Cyber Security Agency of Singapore and the following professional and industry associations that are part of the Singapore Cyber Security Inter Association – Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Chapter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)2 Singapore Chapter, Operational Technology Information Sharing and Analysis Center (OT-ISAC), The Law Society of Singapore, Singapore Computer Society and SGTech.

If you know any individuals and companies who have contributed significantly to the cybersecurity industry, it is time to be recognized now! Nomination forms are attached for the submission according to the categories.

Nomination will end on **14 April 2023**. All submissions must reach the secretariat by 14 April 2023.

For more details on the awards, visit our website [here!](#)

TCA2023 Sponsors & Partners



Organised by



Supported by



Supporting Associations



Platinum Sponsors



Gold Sponsors



Silver Sponsors



Digital for Life

Celebrate Digital @ Bukit Panjang on 11 March

As part of the Digital for Life Movement, AiSP together with our corporate partner, RSM had a booth at Celebrate Digital @ Bukit Panjang on 11 March. AiSP would like to thank Grassroots Advisor, Member of Parliament Mr Liang Eng Hwa for visiting our booth. During the event, our Corporate Partner, Acronis did a sharing on how to stay cyber safe at Celebrate Digital @ Bukit Panjang.



Celebrate Digital @ Keat Hong on 26 March

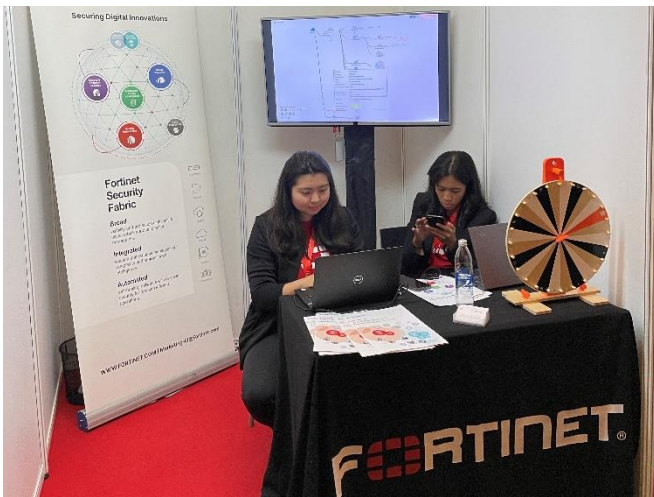
As part of the Digital for Life Movement, AiSP together with our corporate partner, Grab had a booth at Celebrate Digital @ Keat Hong on 26 March. Our speaker from Grab did a sharing on "Don't Be a Victim, be Cyber Smart".



Regionalisation

XCION 2023 from 1 – 3 March

AiSP is happy to support XCION 2023 held from 1 Mar 23 to 3 Mar 23 at Bali. Thank you to our Corporate Partner - BeyondTrust, Fortinet & ONESECURE Asia Pte Ltd for joining us at the event. Interested in regional activities, contact AiSP Secretariat at secretariat@aisp.sg to find out more.



Cybersecurity Awareness & Advisory Programme (CAAP)

MAP Cybersecurity and Digital Trust on 18 April



MAP

CYBER SECURITY & DIGITAL TRUST

LAUNCH EVENT

18 APR

2PM- 5PM

LIFELONG LEARNING INSTITUTE
EVENT HALL 1
11 EUNOS ROAD 8
SINGAPORE 408601



SCAN TO REGISTER FOR EVENT

EVENT HIGHLIGHTS

- Cyber Security Landscape & Schemes to Help Improve Businesses' Cyber Defence
- Panel Insights on Cyber Resilience & Data Protection
- Get Connected with Industry Experts & Solutions to Protect Your Assets

PANELLISTS



TAN KIAT HOW
SENIOR MINISTER OF STATE
MINISTRY OF COMMUNICATIONS AND INFORMATION & MINISTRY OF NATIONAL DEVELOPMENT



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



YEONG ZEE KIN
ASSISTANT CHIEF EXECUTIVE
DATA INNOVATION & PROTECTION GROUP
INFOCOMM MEDIA
DEVELOPMENT AUTHORITY



RAJESH SREENIVASAN
HEAD
TECHNOLOGY, MEDIA & TELECOMMUNICATIONS
RAJAH & TAN SINGAPORE LLP



DR MAGDA CHELLY
MANAGING DIRECTOR & CHIEF INFORMATION SECURITY OFFICER
RESPONSIBLE CYBER PTE LTD

Official Venue Partner:

Lifelong Learning Institute
SKILLSfuture SG

MAP Cyber Security & Digital Trust is Supported By:



To register, please click here - <https://forms.office.com/r/Fa7PETNEiN>

Corporate Partner Events

Navigating the Bug Bounty Landscape: Best Practices and Lessons Learned on 7 March

On 7 March, AiSP and our Corporate Partner, YesWeHack organized an event on Navigating the Bug Bounty Landscape: Best Practices and Lessons Learned. We would like to thank Eileen Neo and Edwin Feng for sharing insights on Bug Bounty Programs with our attendees.



Threats have evolved. So must your Privileged Access Management on 9 March

On 9 March, AiSP and our Corporate Partner, BeyondTrust organized a sharing session on Threats have evolved, So must your Privileged Access Management. It was an insightful time with our speakers, AiSP President, Johnny Kho, Benjamin Wong from BeyondTrust and Eric Lee from Deloitte followed by a panel discussion with the speakers and AiSP EXCO Member, Mathew Soon.

Thank you, all attendees who have joined us, physically for the event.





CREST

CREST President's Update

2022 was a pivotal year for CREST, and we built on our past achievements to deliver a new value proposition for our members, culminating in a three-year strategy and goals launched at the beginning of 2023.

We reformed our governance processes in late 2021, and early 2022 paved the way for more robust, informed and transparent decision-making processes within CREST.

One of the first decisions of the new International Council, informed by our five Regional Councils, was a revised Vision and Mission. This commits CREST to raise standards through building capability, capacity, consistency, and collaboration in the global cybersecurity industry.

We achieve this by delivering services that nurture, measure and enhance the performance of individuals and organisations.

Several new services were introduced in 2022 that support our Vision and Mission. These include the CREST OVS Program, the Skilled Persons Register and the CREST Defensible Penetration Test. Read below for further information on these key services:

The CREST OVS Programme

The new CREST OWASP Verification Standard (OVS) programme offers higher levels of assurance to organisations that build and use mobile and web-based applications. This gives OVS-accredited member companies better traction in the vast and growing app development industry.

We have already accredited the first group of member companies to the programme – Across Verticals, LE Global Services, Nettitude, Pen Test Partners, Pentest People, Trustwave SpiderLabs, URM Consulting and VerSprite – with more in the pipeline for accreditation.

Find out more here:

<https://www.crest-approved.org/membership/crest-ovs-programme/>

The Skilled Persons Register

The Skilled Persons Register allows member companies to register all the people responsible for delivering a CREST-accredited service, such as an OVS.

Registration provides your analysts with a personalised CREST ID which our members can use to give their clients added assurance about the quality of the CREST-accredited services they provide.

It also allows our members to supply enhanced information about individuals' skills, training, examinations and experience. We are working to process and anonymise this data before aggregating it in a Competency Measurement consultation document to be shared with members.

The CREST Defensible Penetration Test

The CREST Defensible Penetration Test (CDPT) addresses the inconsistencies in the definitions, practices and expectations associated with penetration tests. By communicating a minimum set of expectations for how a CREST pentest should be scoped, delivered and signed off, the CDPT supports members and their clients to work more effectively together.

Find out more about CDPT here:

<https://www.crest-approved.org/crest-defensible-penetration-test/>

The CREST Website – a tool for buyers and members

Our evolving identity was reflected in the brand refresh and new website in 2022. The CREST site is now better at connecting members with buyers of cybersecurity services, allowing members to search, shortlist and contact members directly, thereby creating measurable sales leads for members.

Cybersecurity buyers discover how easy it is to connect with our members:

<https://www.crest-approved.org/#buyer-journey>

CREST's Regional Councils – representing our members globally

As Covid restrictions began to lift globally in 2022, I have travelled with our Executive Team to the Americas, Asia, Australasia, the Middle East, and the UK, where we met with regional council members, member companies, regulators, buyers, and other stakeholders.

Thanks to the Regional Councils' hard work, our engagement work has been significant and has positively contributed to growing our profile and membership.

See who is representing the CREST community in Singapore and Asia:

<https://www.crest-approved.org/regions/region-asia/>

Read our latest news here:

- CREST celebrates 300th Member Company
<https://www.crest-approved.org/crest-welcomes-its-300th-member/>
- CREST launches practice labs with Hack the Box and Immersive Labs
- <https://www.crest-approved.org/education/practice-labs/>
- Read about CREST's work in Dubai

- <https://www.crest-approved.org/dubai/>
- Submit CRESTCon Europe Call for Papers (CFP)
- <https://www.crest-approved.org/crestcon-europe-2023-call-for-papers-now-open/>

Thank you

None of this would be possible without the fantastic support we receive from the CREST global community in the shape of the member representatives on our Regional and International Councils, our assessors, the individuals who participate in our discipline aligned Focus Groups, the thousands who attend our events, and the thousands of professional taking our exams.

I am proud and privileged to work with this CREST community. And I look forward to working with you in 2023.

Yours Sincerely,
Rowland Johnson, President of CREST



To find out more about CREST, please visit our website:
<https://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
4- 5 Apr	CISO Perth	Partner
11 Apr	Exploring The Bug Bounty Cycle: From Detection To Fixing	Partner
12 Apr	Knowledge Series – Cloud Security	AiSP & Partner
13 Apr	M365 Back Up Webinar	Partner
13 Apr	Smart Cybersecurity Summit	Partner
13 Apr	AiSP Bug Bounty Workshop	AiSP & Partner
14 Apr	Anti-Scam and Cybersecurity Tabletop Game Creation Competition at Toa Payoh HDB Hub	AiSP & Partner
14-16 Apr	Inter-Poly CTF	Partner
17 – 21 Apr	Learning journey to Hanoi, Vietnam	AiSP & Partner
18 Apr	PDD Connecting Smartness	Partner
18 Apr	Launch of SBF MAP: Cyber Security & Digital Trust	Partner
18-20 Apr	Cloud Security APAC	Partner
20 Apr	Webinar with Tenable	AiSP & Partner
20 Apr	School Talk at Kranji	AiSP & Partner
21 Apr	DFL E-Payment Learning Journey to Yishun Hawker	
25 Apr	AiSP x WiSAP MOU Signing	AiSP & Partner
25 Apr	School talk at SJI	AiSP
26 Apr	Learning Journey to Singtel for AES	AiSP & Partner
27 Apr	AiSP x Grab x Security Scorecard GRC Sharing	AiSP & Partner
5 May	AVIP Event with CE	AiSP
9-12 May	Black Hat Asia 2023	Partner
10 May	IoT Day 2023	AiSP
11- 12 May	ITE West Learning Journey to Grab	AiSP & Partner
12 May	School Talk at Presbyterian High School	AiSP
15- 17 May	FinTech Festival India 2023	Partner
17 May	ITE West Learning Journey to Grab	AiSP & Partner
18 May	Event with CISCO	AiSP & Partner
24 May	Sharing on Cyber as a Career at PSB	AiSP & Partner
24 May	Learning Journey to Singtel	AiSP & Partner
25 May	Knowledge Series – Cyber Defence	AiSP & Partner

30 May	AiSP Ladies in Cyber Learning Journey to Ensign & Dialogue Session with SMS Sim Ann	AiSP & Partner
30 - 31 May	CISO ASEAN Online	Partner
31 May	AiSP x SBF Webinar on Social Engineering (E-Commerce Fraud, Tech Support Fraud)	AiSP & Partner

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

CONTRIBUTED CONTENTS

Article from CTI SIG

Introduction to the Blue Team

As cyberattacks ramp up across world, it is an absolute necessity for every organization to have a defence capability. However, the journey of setting up such expertise and attaining the right level of maturity requires the right combination of technology, processes, and people. This roadmap may appear daunting and overwhelming to many who are just getting started.

In this article, we aim to help lead and aid organizations and professionals on a journey to build defence capability. This article is intended to ensure that all aspects of a blue team defence program are understood and that there are no blind spots.

Blue team cybersecurity experts identify various security loopholes also known as vulnerabilities, in the organization's infrastructure and applications. These efforts contribute to the patching and implementation of various security procedures and controls. Blue teamers typically have a talent for thinking outside the box and responding quickly to various types of security events and incidents. They oversee protecting businesses from cyber risks and threats.

How does implementing the blue teaming approach benefit organisations?

It is critical to understand that an organisation can expect to gain from establishing a blue team, as well as how to take step-by-step action to ensure success.

- Risk assessment
- Monitoring and surveillance
- Security controls
- Reporting and recommendation to management

There are many other advantages of setting up a blue team; here are only a few which are listed above.

So, who are the members of a blue team?

A blue team is made up of many people with diverse skill sets. The composition of a team varies according to the needs of an organisation. Here, are some of the typical roles that exist within this team.

Analysts

[back to top](#)

In the company's Security Operations Center, an entry-level cybersecurity position known as SOC analyst exists (SOC). A triaging analyst is another term for a cybersecurity analyst. The SOC analyst investigates evidence and responds to specific severity incident alerts. This is a reactive role. In SOC, organisations typically have Level 1 (L1), Level 2 (L2), and Level 3 (L3) roles. L1 is the most junior analyst role in a SOC, while L3 is the most senior analyst role. In most cases, increasing levels of responsibility and experience are denoted by rising numbered levels. SOC examines IT network traffic for anomalous or suspicious behaviour. Certain suspicious activities may indicate the presence of malicious entities or malicious programmes in the network, such as Trojans and ransomware.

Incident responder

An incident response analyst is another term for an IR. This position determines whether a reported alarm is the result of an organisational attack or a persistent threat to a company's network. They ensure that it is contained as soon as possible and that the organisation can respond and recover as planned. IRs typically investigate the scope of a cyberattack. IRs develop a remediation strategy based on the scope of the cybersecurity problem. This entails looking into the specifics of the incident. This includes the types of malicious activities performed by the malware as well as the business assets targeted by the malware. The IRs then recommend the best course of action. They carry out remediation with the appropriate teams, such as opening IT tickets to re-image compromised systems.

Threat Hunter

This job title is also known as threat analyst or threat researcher. The threat hunter's job is to be proactive. They conduct regular threat and risk research to stay current on the latest threats. They are also interested in the evolution and anatomy of threats. Threat hunters frequently create coding rules that alert the company's SIEM solution to specific cyber threats. Threat hunters are skilled at configuring and monitoring multiple threat intelligence platforms (such as IBM X-Force, AlienVault OTX, VirusTotal, and others) to conduct proactive research into the life cycle of threats. Based on various parameters such as the industries targeted, vulnerabilities exploited, and attack TTPs, they determine whether new and emerging threats pose the greatest risk to their company. Threat hunters frequently use system configuration.

Security Consultant

Security consultants are frequently hired on a contract basis and perform tasks as needed throughout the project's life cycle. They may also be hired from outside the organisation to provide a dependable source of knowledge or expertise in a specific tool or security area. They are frequently regarded as experts in their field. Subject Matter Experts is another term that is frequently used to describe security consultants (SMEs). A few examples of specialised roles include security strategy consultant and security operations consultant.

Security Administrator

A security administrator is not the same as a SOC analyst. However, it has been observed that organisations frequently regard security administrators as Level 4 (L4) SOC analysts, whose job it is to download, install, configure, deploy, and launch various security tools in

the SOC. They are also in charge of updating those tools when vendor updates arrive. This job is like that of a systems administrator, but it deals with all the security tools in the SOC, such as SIEM, SOAR, AV-NGAV, EDR-XDR, DLP, honeypots, cloud governance, WAF, firewall, load balancers, IAM and AD, brand abuse and defamation monitoring solutions, and more. The job also entails applying patches or fixes released by the respective tool vendors and configuring security tools to ensure peak performance.

They frequently collaborate with threat hunters and incident response teams to develop security scripts and programmes that automate some of the redundant security tasks. They are not, however, tasked with investigating security events and incidents flagged by security tools.

Identity and Access Management (IAM) administrator

This position supports several departments within a company with Identity and Access Management (IAM). An IAM administrator's key responsibilities include managing application/system authority and privileges, Single Sign-On (SSO), application reporting, and collaborating with developers to integrate identity and access management policies for new applications and software. These experts specialise in the use of various IAM tools as well as networking administration.

Compliance analyst

This position supports several departments within a company with Identity and Access Management (IAM). An IAM administrator's key responsibilities include managing application/system authority and privileges, Single Sign-On (SSO), application reporting, and collaborating with developers to integrate identity and access management policies for new applications and software. These experts specialise in the use of various IAM tools as well as networking administration.

There will be more roles to consider, depending on the type or complexity of an organization. However, in this section, we covered some of the skills that are typical in any organization. Next, we will briefly touch upon the red team and the purple team. These two teams may not be part of a blue team, but it is important to understand what these teams do as well. Moreover, we will also understand the role of a cyber threat intelligence team. This skill set typically sits within the blue team, but it is also common to have this team segregated from the blue team.

Blue team members must possess the following abilities. Members work to secure the business network infrastructure and strengthen its cybersecurity posture. The methodologies and strategies they employ to defend the network and systems from cyberattacks are inextricably linked. Management must gain a better understanding of the blue teamers' goals and functions.

1. Eager to learn and detail-oriented
2. In-depth knowledge of networks and systems
3. Outside-the-box and innovative thinking
4. Ability to cross conventional barriers to perform tasks
5. Academics, qualifications, and certifications

Learn more about the defensive cybersecurity measures while thinking from an attacker's perspective. With this [book](#), you'll be able to test and assess the effectiveness of your

organization's cybersecurity posture. No matter the medium your organization has chosen- cloud, on-premises, or hybrid, this book will provide an in-depth understanding of how cyber attackers can penetrate your systems and gain access to sensitive information.

Beginning with a brief overview of the importance of a blue team, you'll learn important techniques and best practices a cybersecurity operator or a blue team practitioner should be aware of. By understanding tools, processes, and operations, you'll be equipped with evolving solutions and strategies to overcome cybersecurity challenges and successfully manage cyber threats to avoid adversaries.

Cybersecurity Blue Team Strategies gives you enough exposure to blue team operations which will enable you to successfully set up a blue team in your organization.

This book is recommended for cybersecurity professionals involved in defending an organization's systems and assets against attacks. Penetration testers, cybersecurity analysts, security leaders, security strategists, and blue team members will find this book helpful. Chief Information Security Officers (CISOs) looking at securing their organizations from adversaries will also benefit from this book.

To get the most out of this book, click [here](#).

Biography

Kunal Sehgal (Author)

Kunal Sehgal has been a cyber-evangelist for over 15 years and is an untiring advocate of Cyber Threat Intelligence sharing. He encourages cyber-defenders to work together by maintaining a strong level of camaraderie across public and private sector organizations. He has worked on setting up two Information Sharing & Analysis Centres to combat cybercrime, and regularly shares credible intelligence with law enforcement agencies around the world. Kunal has also worked for various organizations, in leadership roles, to drive security improvement initiatives and to build cybersecurity services, especially within the APAC region. He specializes in helping businesses improve their security posture and resilience while leveraging the power of the cloud. Kunal resides in Singapore, and invests his non-working hours in researching, blogging, and presenting at cyber-events across Asia. He has 17 certifications/degrees in various IT- and information security related topics.

Nikolaos Thymianis (Author)

Nikolas has studied cultural informatics at the University of the Aegean in Greece, during which he received a scholarship to go to the UK and continue his education to gain an MSc in information security, at the University of Brighton. Nick's work experience led him to associate with people in the healthcare industry, while doing cybersecurity assurance and maturity assessments for organizations in the NHS, helping to set the standards and guidelines for hospitals in the UK. Nikolaos was the CISO of care socius from 2018 until 2022. Nick is now active in big pharma, working in risk management/exception management. He always encourages everyone he meets to be security aware, because information security is a problem everyone faces. He is an advisor at the University of Piraeus and has also become a recognized cybersecurity speaker.

Article from our Corporate Partner, Blackpanda

SMEs are at risk of Cyber Attacks

Small and medium-sized businesses (SMBs) are facing increased risks of cyber attacks. Hackers are increasingly targeting these businesses, seeing them as low-hanging fruit with limited resources and knowledge to defend themselves against sophisticated cyber threats. According to a recent report, 43% of all cyber attacks are aimed at SMBs, making them vulnerable to significant financial and reputational damages.

One of the primary reasons SMBs are at risk is due to their lack of preparedness. Unfortunately, 86% of SMBs are not prepared to defend themselves against these attacks. This leaves them exposed to the risk of business interruption, which accounts for 67% of the cost of a cyber attack, followed by incident response and forensics (18%), increased manpower (9%), ransom payment (4%), and others (2%). The average cost of incident response for an SMB is between USD 20,000 and USD 100,000.

In this article, we will present three case studies: a school hit by ransomware and a small clinic affected by a data breach that were crippled by the respective cyber breaches, and a retailer hit by Business Email Compromise who had a Blackpanda IR-1 subscription and managed to spring back into business. We will discuss the increasing risk of cyber attacks on small and medium-sized enterprises (SMEs) and why they are vulnerable to these threats. We will also discuss the importance of preparation and proactivity in ensuring that a business can quickly bounce back from a cyber attack.

Singaporean School Hit by Ransomware

In January of this year, a school in Singapore fell victim to a ransomware attack. The school was unable to access its critical data, including student records and financial information, resulting in the disruption of lessons.

The attack was attributed to the Maze ransomware group and was initiated through the Remote Desktop Protocol (RDP). The school's database was encrypted, and the hackers demanded a ransom payment of SGD 70,000 to restore access to the school's systems. The attack caused disruptions to the school's internal communication and compromised the normal teaching schedule for several days. The school also incurred significant financial and reputational damage as a result of the attack. The costs incurred by the school included SGD 45,000 for incident response team costs, SGD 40,000 for new computers and servers, and an estimated 2500 hours to reproduce the lost data, valued at SGD 70/hour. The total cost of the attack was significant and included the loss of trust and credibility in the school's reputation, legal implications for failing to protect students' personal information and data, and the loss of donors, funding, and future partnerships.

Clinic Hit by a Data Breach

In November 2022, a small private clinic in Singapore experienced a data breach that resulted in the exposure of patients' sensitive information, including their personal and medical information. The breach was a result of weak password practices and unsecured servers, leaving the clinic's systems vulnerable to cyber attacks.

The attackers exploited a reused password from one of the clinic's employees that had been previously involved in a data leak. They found the credentials on the Dark Web, and used social engineering to guess the email address, and then proceeded to log into the employee's admin account. This allowed them to gain access to the clinic's database, which contained patients' personal and medical information. The attackers had access to the data for several days before being detected. They stole a vast amount of information, including patients' full names, contact details, medical histories, and diagnoses.

Upon discovering the breach, the clinic management immediately shut down their systems and conducted an internal investigation to assess the damage. Unfortunately, the attackers had already accessed and exfiltrated a significant amount of patient data, including their full names, contact details, medical histories, and diagnoses. The clinic management was unable to access any of the stolen data and feared that the attackers may still have ongoing access to their systems.

The breach not only put affected patients at risk of identity theft and other privacy violations, but also had legal implications for the clinic. The clinic's failure to protect sensitive medical data could result in legal action, lawsuits, and significant financial penalties under Singapore's data protection laws.

Retailer with a Blackpanda IR-1 subscription hit by Business Email Compromise

In February 2023, a retail company in Singapore experienced a devastating Business Email Compromise (BEC) attack that left them reeling from financial losses and a damaged reputation. However, the retailer had an IR-1 subscription, which enabled them to quickly respond and mitigate the impact of the attack. IR-1 is a subscription-based solution designed to help SMBs manage cyber breaches and mitigate their impacts. The solution offers a 12-month subscription plan that includes 24/7 incident response availability, one incident response activation credit, discounted rates for all Blackpanda services, and unlimited access to a digital library.

The attackers behind the BEC attack on the retailer had conducted extensive reconnaissance to identify vulnerable employees with access to sensitive financial information and payment systems. They then sent phishing emails to these employees, tricking them into clicking on a malicious link or downloading a file containing malware. One unsuspecting employee fell for a fake software update email prompt, which gave the attackers access to their email account. Using this access, the attackers were able to gather sensitive client information and send fraudulent emails to clients requesting funds for ongoing transactions to bank accounts owned by the threat actor.

Thanks to Blackpanda's quick response, the retailer was able to limit the financial losses and prevent any further damage to their reputation. The IR-1 solution was able to identify and stop the attack within two hours of being notified. This incident serves as a reminder of the importance of having a reliable and responsive incident response partner like Blackpanda to protect your business from cyber threats.

IR-1 helps businesses in Asia build cyber resilience

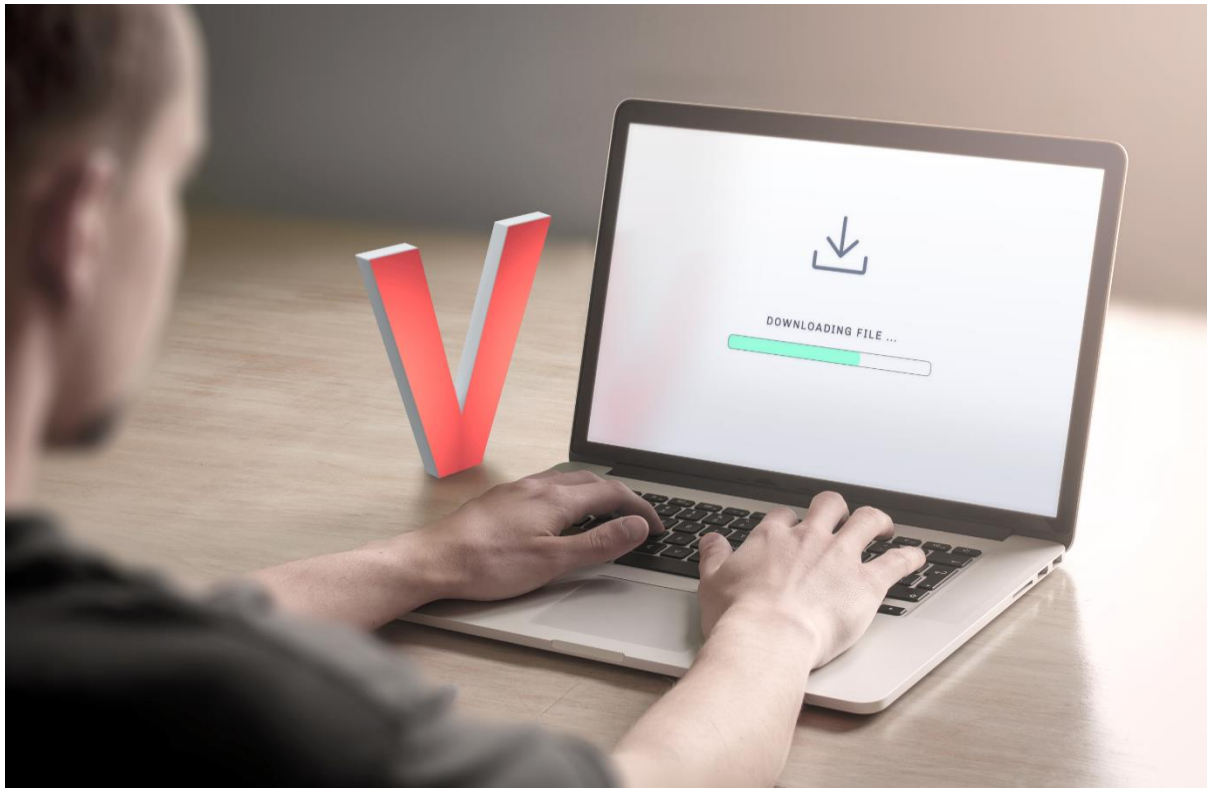
The increasing frequency and severity of cyber attacks on SMBs are a cause for concern. Small and medium-sized businesses are particularly vulnerable to cyber threats due to their limited resources and lack of preparedness. However, with proper preparation and proactivity, SMBs can effectively manage cyber breaches and mitigate their impacts. The case studies presented in this article illustrate the potential financial and reputational damage that SMBs can face as a result of cyber attacks. These businesses can suffer significant losses due to business interruptions, incident response costs, legal fees, and reputational damage.

The Blackpanda IR-1 subscription is an excellent solution for SMBs looking to protect themselves from cyber threats. The subscription offers a range of features designed to help businesses manage cyber breaches and mitigate their impacts. This includes incident response credits, 24/7 incident response availability, ongoing support and guidance, legal and PR support, and more.

In today's digital landscape, it is essential for SMBs to take cyber security seriously and invest in robust cyber security measures. By doing so, these businesses can protect themselves from cyber threats and ensure their long-term success.

[Contact Blackpanda to learn more about IR-1.](#)

Article from our Corporate Partner, Votiro



Want to chat with Votiro about zero trust content security?

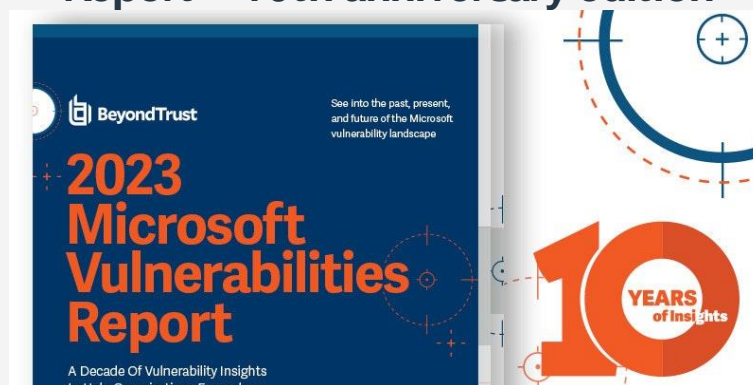
[Hop onto a discovery session](#) with Votiro Experts for a great conversation and a live demo of our content disarm & reconstruction platform.

Contact us at votiro-sg@votiro.com for any enquiry anytime!

Article from our Corporate Partner, Beyond Trust



Now Available: The 2023 Microsoft Vulnerabilities Report – 10th anniversary edition



The Microsoft Vulnerabilities Report is proudly celebrating its tenth year. Since the report debuted in 2013, it has garnered over 15,000 downloads and has benefited thousands of users with detailed data analysis and expert findings.

This 10-year anniversary edition of the report dissects the 2022 Microsoft vulnerabilities data and highlights some of the key shifts since the inaugural report.

Key Highlights from the 2023 Edition:

- **Elevation of Privilege** is the #1 vulnerability category for the third year running, accounting for **55%** of the total Microsoft vulnerabilities in 2022.
- In 2022, total Microsoft vulnerabilities **rose to 1,292**, hitting an all-time high, since the report began 10 years ago.
- Azure & Dynamics 365 vulnerabilities skyrocketed **by 159%**, from 44 in 2021 to 114 in 2022.
- Critical vulnerabilities dropped for the 2nd year in a row, hitting a **five-year low of 89 in 2022**.

[Download the full report](#) to take a closer look at these findings and more, including a panel of some of the world's leading cybersecurity experts who weigh in on the report findings.

Finally, we will also have a special AI guest weigh in as we look ahead to how the next decade in threats, vulnerabilities, and cyber defenses may unfold.

[Download Report](#)

Article from our Corporate Partner, DT Asia

Active Directory Cyber Resiliency

Reduce Cyber Risk for your organization



Active Directory is the cornerstone of almost all Enterprise IT infrastructure. By leveraging on the 5 principles of the NIST Cyber Security Framework, we discuss how we help businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their critical Active Directory as well as Azure AD.

Speaker: **Ronino Tabana**, Solutions Consultant

IT Solutions Consultant with Pre and Post-Sales experience in Architecture Design, Planning, Migration, Build and Deployment of IT Infrastructure, focusing on Private/Public Cloud offerings built on Microsoft, Citrix and VMWare technologies.

Experienced Software and Solution Seller enabling customers in their transition to the cloud. Enabling clients to achieve IT Business Resilience with Hybrid Solutions on Identity Security, Platform Management and Data Operations with Quest Software's Microsoft Platform Management team.



Venue : NUSS Suntec
Date : 17-May-2023
Time : 3 PM -5 PM



Please sign up by 1 May. Please note that registration is based on first come first serve.

[Register here!](#) or contact Irving@dtasiagroup.com

Article from our TCA 2022 Winner, Hoi Wai Khin



A Technology/Cyber Security Professional Journey

As I was climbing the stairs of a nearby HDB block after my usual 3 KM run, my mind was suddenly drawn to my journey in the security profession. The climb created a moment of solitude, providing on opportunity for reflection on my security career. On the third floor, I can see everything clearly: the cars parked in the lot, the different models and makes, and their conditions.



But as I climb higher, my perspective becomes more and more limited. By the tenth floor, the once clear view is now fuzzy, and the car models are unrecognizable.



On the eighteenth floor, the car park is lost entirely from my view, and all I see are the other blocks around me.



And by the time I reach the top floor, I am disconnected from the ground, with my view are obstructed.



It reminds me of the journey of a cybersecurity professional. Starting from the ground up, we learn everything we can about the issues and challenges of the field. But as we move up the ranks, we face new challenges, such as budget constraints, organizational issues, and cultural barriers. To be a successful cybersecurity leader, we must keep one foot grounded in the issues of the lower levels, while also being able to influence and manage the top.

So how do I continue my passion after 20 years?

One valuable step for personal and professional development in the cybersecurity or GRC field is to join industry associations like AISP, ISACA, ISC2, DRII or CMI. These associations provide a forum for like-minded professionals to gather and learn from one another.

ISACA, for example, is focused on technology governance, risk, and compliance, while ISC2 is a highly regarded organization that trains cybersecurity professionals. DRII, on the other hand, focuses on business continuity and disaster recovery and CMI helps to supplement cybersecurity professionals with good manager skillset.

By joining an association, individuals can expand their network of contacts, exchange ideas, and tap into the collective knowledge of hundreds of security professionals. Ultimately, these associations offer a valuable resource for problem-solving and personal growth in the cybersecurity and GRC industries. Other notable associations exist as well, and it is worth exploring them as part of one's own development.

Volunteering is an integral part of personal and professional development in the field of cyber security. It extends beyond assisting in the operation of the association you joined, as it presents an opportunity to make a significant impact by imparting good cyber security practices to individuals with limited or no IT knowledge. For instance, the IMDA Digital for Life programme is a government initiative aimed at promoting technology literacy among people of all ages. Volunteering with AISP to support such events is a great way to contribute to the cause. Furthermore, sharing your experiences with institutes of higher learning or even secondary school students can inspire them to become part of the cyber security community. By doing so, you can educate them about both the challenges and rewards of defending against technology risks, and potentially inspire future generations to pursue careers in cyber security. Assisting non-profit organizations (NPOs) in strengthening their cybersecurity posture is a valuable contribution to the community. NPOs often face resource constraints that limit their ability to invest in robust cybersecurity measures. As a result, they may be vulnerable to cyber attacks and data breaches that could potentially harm their operations and reputation.

By volunteering our time and expertise, we can help NPOs identify and address their cybersecurity weaknesses. We can assist them in implementing best practices and industry standards in cybersecurity, such as data encryption, access controls, and employee training. Furthermore, we can provide guidance on developing incident response plans to ensure they are prepared to respond to a cyber attack.

Helping NPOs in enhancing their internal controls on cyber-related protection not only improves their cybersecurity posture but also strengthens the overall cybersecurity of the community. It is a fulfilling way to use our skills and knowledge to make a positive impact to the Singapore cyber landscape.

Finally, it is essential for cyber security professionals to improve their management skillsets. Effective cyber security professionals not only need to have technical knowledge but also need to be able to connect different components and lead the team. They should possess the following characteristics:

- Strong problem-solving skills. Cyber security professionals must be able to identify and resolve problems efficiently and effectively.
- Influential. Cyber security professionals should leverage their experiences to influence and gain support from top management to achieve the organization's goal of defending against technology risk.

- Excellent salesmanship. The person needs to be able to communicate and promote the importance of security to the ground, mobilizing the organization towards a common goal of defending against technology risk.
- Project management skills. Cyber security professionals should be adept at managing stakeholders' expectations, project requirements, risk management, and continual security awareness within the organization.
- Innovative. Cyber security professionals should keep themselves updated with the latest developments and bring value to the organization, ensuring compliance with regulations, meeting stakeholder expectations, and most importantly, fostering a good security culture.
- Leadership qualities. Cyber security professionals need to lead by example, inspiring others to do the right thing instead of just doing things right. By being a value to the organization, they can influence, sell, problem-solve and lead the team towards a common goal

Receiving the 2022 TCA cybersecurity leader award is not just about starting or finishing a journey, but about remembering our passion and why we do what we do. The path of a cybersecurity professional is not easy; we must be resilient because we are dealing with problems everyday. We need to persevere through the ever-increasing demands of data protection and the fast-evolving technology landscape.

In conclusion, it's crucial to approach this not as a job, but as a passion. If we're truly passionate about security, we'll find joy in the journey despite encountering many obstacles along the way. There will be tough times, but during those moments, it's important to remind ourselves why we're here. We're not just doing a job, but rather, we're helping our organization, peers, and juniors become better equipped to manage and defend against cyber risks.

Reflection from our SVRP 2022 Winner, Edwin Chua

I am incredibly honoured and humbled to have been selected as one of the seven recipients of the Student Volunteer Recognition Programme (SVRP) Gold 2022 award. This initiative, which is run by the Association of Information Security Professionals (AiSP) with support from the Cyber Security Agency of Singapore (CSA) and private sectors, was established to encourage volunteerism among students and to foster their interest in the field of cybersecurity.

As the Vice President of the Nanyang Polytechnic Cybersecurity Interest Group, I have had the opportunity to engage with tertiary students and to help them develop their interests in the technical aspects of cybersecurity. Through organizing competitions and workshops, I have been able to provide students with hands-on experience and to help them understand the complexities and challenges of this field.

I was given the opportunity to coordinate the annual Youth Cyber Exploration Programme (YCEP) Cybersecurity bootcamp in 2021 and 2022. This outreach

programme reached over 100 secondary school students and provided them with an introduction to the field of cybersecurity. YCEP is a key component of Singapore's Cybersecurity Strategy and is designed to build a strong future cybersecurity talent pipeline and to engage with youth at the pre-tertiary level.

I have also been fortunate enough to be a part of the organizing committee for the Interpol Lag and Crash 2.0 Capture-The-Flags (CTFs) Competition, which targets Polytechnic, ITE, and JC students. This event, which is organized by different Polytechnic Cybersecurity Interest Groups, provides students with exposure to the field of cybersecurity and allows them to experience the different concepts involved in this complex field.

I am grateful for the opportunities I have had to be involved in various initiatives and events that aim to promote cybersecurity awareness and education. These experiences have not only allowed me to deepen my own understanding of the field, but also provided me with the chance to give back to the community and to help others develop their own interests and skills.



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

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

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International



EC-Council's Blockchain Certifications Overview

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

These programs have been designed to meet the industry requirements of developers, business leaders, and fintech professionals in this rapidly growing area.

Our blockchain certification courses consist of three knowledge and competency areas: development, implementation, and strategy.

During the course, students get exposure to multiple blockchain implementation concepts and a unique guideline for sustainable and scalable blockchain development using quantum-resistant ledgers.

Considering the market opportunity and skills required for different target groups, EC-Council has launched three new blockchain programs:

- 1. Blockchain Business Leader Certification (BBLC)**
- 2. Blockchain Fintech Certification (BFC)**
- 3. Blockchain Developer Certification (BDC)**

Blockchain technology is becoming more prominent in today's digital world, and getting certified is a great way to showcase your knowledge and lend credibility to your resume.

EC-Council's expert-designed courses will provide you with hands-on experience and help you gain valuable insights that are mapped to real job roles.

Special discount available for AiSP members, email aisp@wissen-intl.com for details!

Listing of Courses by ALC Council



Stand out from the crowd

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

We offer the most in-demand cyber certifications including:

- CISM®, CRISC®, CISA®, CGEIT®, CDPSE®
- SABSA®, NIST®, ISO 27001
- CISSP®, CCSP®
- CIPM, CIPT, CIPP/E

The right training makes all the difference

Lots of things go into making a great course, but the single most important is always the trainer: their knowledge of the subject; their real-world experience that they can draw upon in class; their ability to answer questions; their communication skills. This is what makes the difference.

ALC works only with the best. That has been the core of our business model for the past 28 years. You can see the calibre of our trainers on our [Faculty](#) page.

AiSP Member Pricing – 15% discount

AiSP members receive 15% discount on all ALC training courses. To claim your discount please enter the code **ALCAiSP15** in the Promotion Code field when making your booking.

Upcoming Training Dates

Click [this link](#) to see upcoming Course Dates. If published dates do not suit, suggest an alternative and we will see what we can do.

Special Offers.

We periodically have special unpublished offers. Please contact us aisp@alctraining.com.sg to let us know what courses you are interested in.

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

Thank you.

The ALC team



ALC Training Pte Ltd

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

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

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

Qualified Information Security Professional (QISP®)

Promotion for Qualified Information Security Professional (QISP) Exam until 30 April!

AiSP
Advance Connect Excel

QISP EXAM

Increase your certification profile and sign up for
**QUALIFIED INFORMATION SECURITY PROFESSIONAL
(QISP) exam!**

**Complimentary FIRST year Membership
till
31 Dec 2023**

Price

Sign up before **30 April** to get **\$50 off (U.P \$370)**
Sign up in **bulk of 10** to get **\$70 off per pax**

**For individual sign up, please register via the qr code
here**



**To sign up in bulk of 10, please send to
secretariat@aisp.sg**

If you have One (1) to five (5) years of working experience in Information Security; or Formal training in cyber security in an educational institution and would like to increase your certification profile, sign up for AiSP one and only Qualified Information Security Professional (QISP) exam!

Complimentary 1- year AiSP membership (till 31 Dec 2023) will be given to all candidates who have signed up for the exam.

Sign up before 30 April to get \$50 off the exam price (U.P \$370) which is just **\$320** before GST to achieve the certification!

AiSP QISP Exam is based on IS-Body of Knowledge 2.0:

- Validated by corporate companies, IHLs and associations.
- This includes government agency such as GovTech, IHL schools such as polytechnics and associations such as Singapore Computer Society and SGTech.
- Developed by referencing from the Skills Framework for Infocomm Technology by IMDA on cybersecurity topics.

**Terms and conditions apply*

Register [here now!](#)

For more details visit our website [here!](#)

If you have any enquiries, please contact secretariat at secretariat@aisp.sg

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP)
- 5 DAYS-

\$840*

~~\$2800~~

*70% funding for Singaporeans 40 and above.
50% funding for all Singaporeans below 40 & all PRs.

Call us: +65 8839 0071
Email us: training@opusit.com.sg

AiSP
Advance Connect Excel

OPUS
ACADEMY

Companies around the world are doubling down on their security as cyber-attacks see an increase in frequency, intensity and severity. It is thus critical for businesses and organisations to have Qualified Information Security Professionals to manage cybersecurity threats and incidents.

To support the development of personnel in this profession, the Association of Information Security Professionals (AiSP) is offering the Qualified Information Security Professional (QISP) Programme.

This special five-day training programme is based on AiSP's Information Security Body of Knowledge (IS BOK) 2.0. This course will prepare participants for the QISP examinations.

After attending this course, participants will also be able to understand and attain knowledge in these areas:

- Enterprise Governance
- Risk Analysis and Management
- Security Controls
- Security Principles and Lifecycle
- Business Continuity Planning
- Develop and Implement Security Goals, Objective and Strategy and Programs
- Maintain and Review Security Operations

COURSE DETAILS

2023 Course dates can be found on https://www.aisp.sg/qisp_training.html

Time: 9am-6pm

Fees: \$2,800 (before GST)*

**10% off for AiSP Members @ \$2,520 (before GST)*

***Utap funding is available for NTUC Member**

*** SSG Funding is available!**

TARGET AUDIENCE

- Professionals who wish to learn more or embark into Cybersecurity
- Security Professionals who will be leading or taking on a senior management/technical role in ensuring Enterprise Governance is achieved with Corporate, Security and IT Governance

COURSE CRITERIA

There are no prerequisites, but participants are strongly encouraged to have:

- At least one year of experience in Information Security
- Formal institutional training in cybersecurity
- Professional certification in cybersecurity

*For registration or any enquiries, you may contact us via email at secretariat@aisp.sg or Telegram at **@AiSP_SG**.*

Program Partner

Delivery Partners



Cybersecurity Essentials Course



This course is suitable for people who are new to information security and in need of an introduction to the fundamentals of security, people who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification. Professionals who are in need to be able to understand and communicate confidently about security terminology.

To support the development of personnel who are new to information security and wish to pursue career in this profession, the Association of Information Security Professionals (AiSP) is offering the Cybersecurity Essentials Course. With the completion of this course, participants will have an overview on cybersecurity. The course will build on the foundation to prepare participants for Qualified Information Security Professional (QISP) course.

Course Objectives

This 3-day training program is for those who have very little knowledge of computers & technology with no prior knowledge of cyber security. After attending this course, participants will also be able to understand and attain knowledge in these areas:

- Introduction to Security
- Risk Management
- Cybersecurity IT Platform
- Securing the Server

- Securing the Network
- Cloud Computing
- Cybersecurity Operations

COURSE DETAILS

Training dates for year 2023 can be found on
https://www.aisp.sg/cyberessentials_training.html

Time: 9am-6pm

Fees: \$ \$1,600 (before GST)*

*10% off for AiSP Members @ \$1,440 (before GST)

*Utap funding is available for NTUC Member

* SSG Funding is available!

TARGET AUDIENCE

- New to cybersecurity
- Looking for career change
- Professionals need to be able to understand and communicate confidently about security terminology

Please email us at secretariat@aisp.sg to register your interest.

Program Partner

Delivery Partners



MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

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

Complimentary Affiliate Membership for NTUC Members

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

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

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

CPP Membership



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

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

For any enquiries, please contact secretariat@aisp.sg

AVIP Membership

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



AVIP membership is the FIRST in Asia to bundle the Professional Indemnity for professionals involved in cybersecurity related work, to give them greater assurance undertaking projects in Singapore and worldwide.

BENEFITS

- Recognition as a Trusted Infocomm Security Professional. You can use the designation of **AVIP (AiSP Validated Information Security Professionals Member) as your credentials.**
- **Special Invite** to Exclusive Activities & Events.
- AVIP members enjoy the **Professional Indemnity Coverage in Singapore and Overseas (FIRST in Asia)!**
- AVIP members will be invited for key dialogue sessions with national & industry leaders for their opinions on cyber security.
- AVIP members will be invited to **represent AiSP for media interviews** on their opinions on cyber security.

PRICE

**Application Fee : \$486.00 (1st 100 applicants),
\$324 (AiSP CPP members)
Annual Membership: \$270.00**

*Price includes GST

EMAIL MEMBERSHIP@AISP.SG TO SIGN UP AND FOR ENQUIRIES

Membership Renewal

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

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

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

For more updates or details about the memberships, please visit www.aisp.sg/membership.html

AiSP Corporate Partners



Acronis







YES WE H/CK

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

AiSP Academic Partners



Our Story...

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

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

Our Vision

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

Our Mission

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

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

AiSP Secretariat Team



Vincent Toh
Associate Director



Elle Ng
Senior Executive



Karen Ong
Executive



Jennifer Goh
Finance & Human
Resource Officer



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.