NEWSLETTER

May 2023

NEWS & UPDATE

Qualified Information Security Professional E-Learning just launched!

Scan the QR Code above to register! Email aisp@wissen-intl.com for more information

News & Updates

AiSP x WISAP MOU Signing on 25 April

On 25 April, AiSP President, Mr Johnny Kho met up with Women in Security Alliance Philippines in Philippines for the signing of MOU for the South East Asia Cybersecurity Consortium (SEACC). As part of the MOU signing ceremony, Johnny also shared on the Building Blocks of Digital Trust For Connected Enterprises in the Elevating Transformation with Digital Trust Event organised by our CPP, Beyond Trust.

back to top

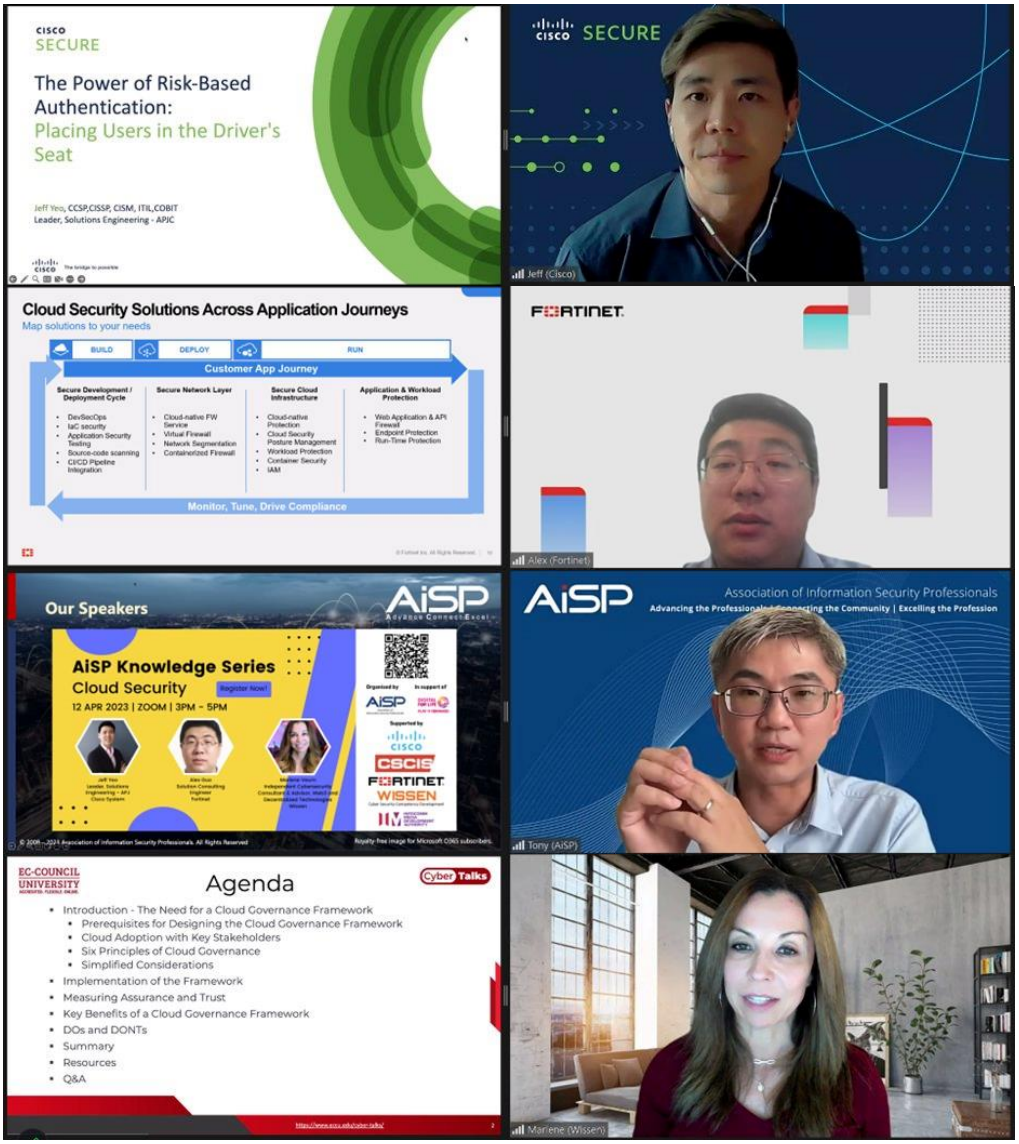
Knowledge Series Events

Upcoming Knowledge Series

Cloud Security on 12 April

As part of Digital for Life movement, we hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 12 April, we have invited our Corporate Partners, Cisco, Fortinet and Wissen International to share insights on Cloud Security with our attendees.

Thank you AiSP Vice-President & Cloud Security SIG Lead, Tony Low for giving the opening address.



back to top

Cyber Defence on 25 May

AiSP Knowledge Series – Cyber Defence

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.

back to top

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_kXhsIiwCRqy3BJfB2XwrFw

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. Cyber Defence, 25 May
2. Operations & Infrastructure Security, 19 Jul
3. IoT, 24 Aug

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

back to top

Student Volunteer Recognition Programme (SVRP)

AiSP Bug Bounty Workshop on 13 April

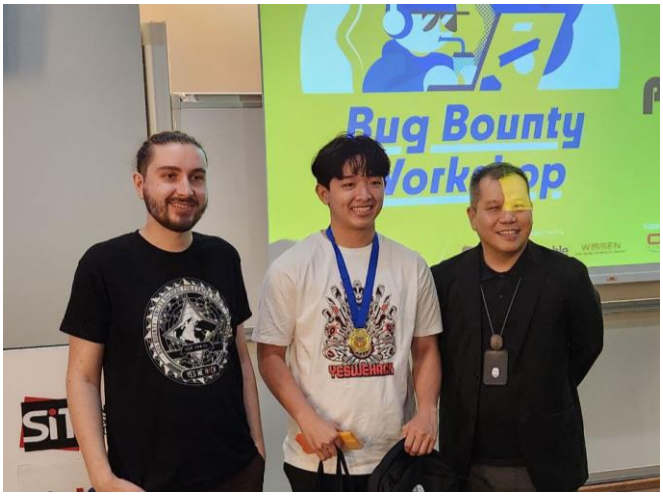
AiSP Bug Bounty Workshop has successfully concluded on 13 April and congratulations to the following winners

1st: Derrick Png from NYP
2nd: Edwin Chua from NYP
3rd: Jeryl from SIT for winning the challenge.

We would like to thank Judy Saw from Wissen International and Dick Bussiere from Tenable for sharing insights with the students. Thank you BitK from YesWeHack for facilitating the Bug Bounty challenge as well.

Big shoutout to Cyber Security Agency of Singapore (CSA), YesWeHack, Tenable, Wissen International and Singapore Institute of Technology for supporting the event!

Click here to view the workshop highlights.



back to top

Learning Journey to Hanoi from 17 April to 21 April

Day 1: Flight to Hanoi
In collaboration with Singapore Institute of Technology (SIT), AiSP brought a total of 21 students on an overseas learning journey to Hanoi, Vietnam from 17 Apr to 21 Apr with the support of the National Youth Council. The students visited universities, companies and the government authority for an insightful learning experience on cybersecurity and discover Hanoi on the cultural perspective AiSP would like to take this opportunity to thank the universities, companies and government authority for hosting us.

Interested to be part of our next trip? Register over here for our next trip to Brunei.
https://lnkd.in/dM2C7bVz

back to top

Day 2: Visit to MK Group

The students visited MK Group and their smart factory. Thank you VNISA for coordinating the visit and MK Group for hosting us.

back to top

Day 2: Visit to CPP, CISCO

The students visited our Corporate Partner, Cisco. Thank you Cisco for hosting us.

back to top

Day 3: Visit to NCS/iSpace and Posts and Telecommunications Institute of Technology (PTIT)

The students visited NCS/iSpace and Posts and Telecommunications Institute of Technology (PTIT). Thank you VNISA for coordinating and NCS/iSpace and PTIT for hosting us.

back to top

Day 4: Visit to Vietnam Cyberspace Security Technology (VNCS) and Thuyloi University

The students visited VNCS and Thuyloi University. Thank you VNISA for coordinating and VNCS for hosting us. We would also like to thank Wissen International (EC-Council ASEAN) for coordinating the visit and Thuyloi University for hosting us and AiSP EXCO Member, Breyvan Tan for presenting the Token of Appreciation to the University for hosting us.

back to top

Day 5: Visit to IPMac

The students visited IPMAC on the last day of the learning journey. We would like to thank our Corporate Partner, Wissen International(EC-Council ASEAN) for coordinating the visit and IPMAC for hosting us.

Click here for more photos of the trip.

back to top

School Talk at Kranji Secondary School on 20 April

AiSP went to Kranji Secondary School for their Education and Career Guidance Fair on 20 April. Thank you Ms Andrea Chea who had been volunteering with AiSP since 2019 when she was a student in SIT and she represented our CPP RSM Singapore and AiSP at Kranji Secondary School sharing on her volunteering journey and the career in Cybersecurity encouraging the students to join the Cybersecurity Ecosystem after they graduate.

School Talk at St Joseph Institution on 25 April

As part of Digital for Life Movement, AiSP hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 25 April, AiSP EXCO Member, Mr Freddy Tan conducted a sharing on cyber hygiene and career opportunities in Cybersecurity to close to 500 St Joseph Institution students.

back to top

Learning Journey to Singtel on 26 April

As part of Digital for Life Movement, AiSP hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 26 April, AiSP brought over 15 Secondary 4 Students from Assumption English School on a learning journey to our Corporate Partner, Singtel. Once again, thank you Singtel for hosting the students.

AiSP Youth Symposium 2023 on 2 July

As part of Singapore Youth Day 2023 on 2 July 2023 (Sun), AiSP will be organising the 2nd Youth Symposium to reach out to the Youths for a day of sharing, internship or career opportunities with our partners on 2 Jul 23 (Sun). We will also invite keynote speakers to share on the importance of Youths in Cyber and Tech.

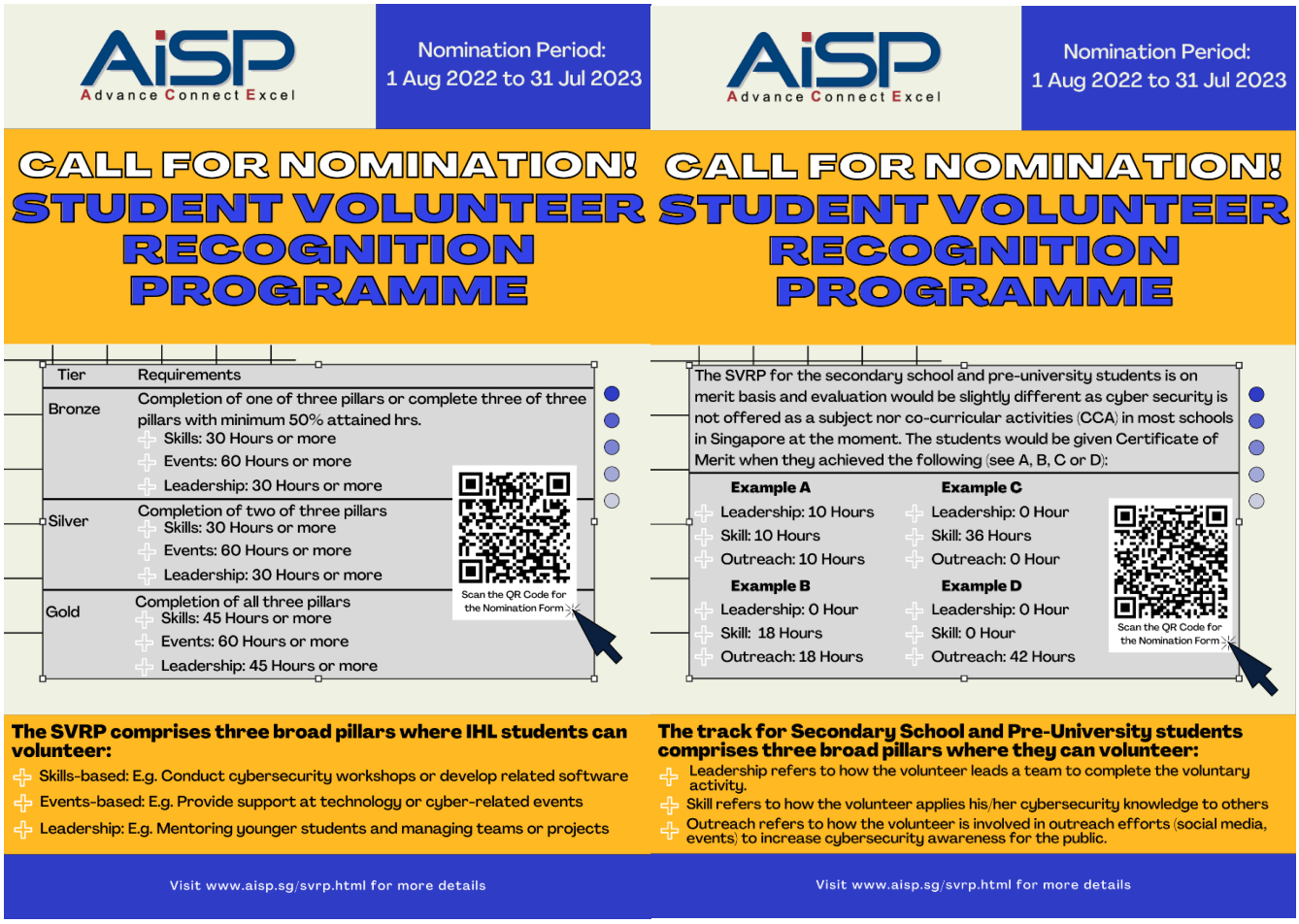
back to top

We are expecting 100 Youths and professionals (Subject to COVID restrictions) for the Symposium in this Physical Event. We have invited our Patron, Senior Minister of State, Ministry of Communications and Information and Ministry of National Development, Mr Tan Kiat How as our Guest of Honour and to have a dialogue session with the attendees on how Youth play an important role in Cyber & Tech in the future. The event is open to all students in secondary and tertiary level.

The details for the event are as follow:

Date: 2 Jul 2023 (Sun)
Time: 12.30 pm to 4.00 pm
Venue: JustCo @ Marina Square
Dress code: Smart Casual

Register here now



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

Ladies in Cybersecurity

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

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, (Tue)
Time: 9am to 12noon
Venue: Ensign InfoSecurity (Singapore) Pte Ltd located at 30A Kallang Pl, #08-01, Singapore 339213
Dress code: Smart Casual

back to top

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 here https://forms.office.com/r/QC9VJ9QK12

Special Interest Groups

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

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

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

back to top

The Cybersecurity Awards

THE CYBERSECURITY Awards 2023

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

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 2023! Only Silver sponsorship packages are available.

TCA 2023 CALL FOR NOMINATION WILL END ON 14 MAY 2023

back to top

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 May 2023**. All submissions must reach the secretariat by 14 May 2023.
For more details on the awards, visit our website here!

TCA2023 Sponsors & Partners

back to top

Digital for Life

Anti Scam Makeathon at Toa Payoh Hub on 14 April
AiSP had a great time at the Anti-Scam & Cybersecurity Makeathon 2023 engaging more than 600 members of the public on the importance of stay safe online and cyber wellness at Toa Payoh HDB Hub. Thank you to Singapore Police Force for having AiSP and our AiSP President Mr Johnny Kho & AiSP Vice-President Ms Sherin Lee for joining the event.

Congratulations to all the winners at the inaugural Makeathon. Let us all play our part and Act Against Scam.

back to top

E-Payment Learning Journey @ Yishun Park Hawker Centre on 21 April

AiSP was down at Yishun Park Hawker Centre on 21 April for the e-payment learning journey with 100 seniors to share with them on enjoying cashback up to $3 when they pay for a hawker centre meal using the DBS PayLah app on fridays.

AMK BLK Party at Blk 624 on 29 April

As part of the Digital for Life Movement, AiSP together with IMDA, had a booth at Ang Mo Kio Blk party for Blk 624 on 29 April. Thank you Mr Yip Hon Weng for visiting our booth.

back to top

DFL IT Workshop for Bukit Batok Residents on 30 April

As part of Digital for Life Programme to reach out to all walks of life. On 30 April, AiSP went to Bukit Batok to present laptops to lower income families sponsored by Tian Kong Temple. Our CPP Contfinity Pte Ltd also conducted a IT workshop for the 40 attendees and provided each lower income family an End Point Protection and Wireless Access Point. Thank you to Alex Chan for conducting the workshop and sharing with them the importance of stay safe online. Thank you to SPS Mdm Rahayu Mahzam who joined us to present the laptops and End Point Protection.

back to top

Regionalisation

SEA CC Webinar – Data & Privacy on 8 Jun

SEA CC Webinar – Data & Privacy

The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2023. The first webinar will be focusing on Data & Privacy where speakers will be sharing insights on the best practices for data protection.

Data Protection ABC
Speaker: Hoi Wai Khin, Partner, RSM [Association of Information Security Professionals]

The phrase "Not IF but WHEN" perfectly captures the reality of the current cyber threat landscape. Locally, security incidents, data breaches, and cases of non-compliance with the Personal Data Protection Act (PDPA) are becoming increasingly common. Your organization may have already been affected or will likely face these challenges in the future. With cyber attacks occurring daily and in multiple locations, it can be challenging to keep track of them all.

back to top

It is crucial for organizations of all sizes to stay Aware of the latest data breaches and threats, Be prepared for potential breaches or threats, and ensure Continuity of operations in the event of a breach. Using experiences gained on the ground, the session will be sharing the ABC of good internal controls that will help manage incidents, limit reputational damage, and reduce recovery time and costs.

Brunei Darussalam's Personal Data Protection Journey
Speaker: Farah Zainal, Personal Data Protection Manager [AiTi (Brunei)]

The webinar aims to provide the audience with a brief overview of the upcoming Personal Data Protection law in Brunei Darussalam.

Cambodia Data Protection Initiative
Speaker: Ou Phannarith, Founder of ISAC-Cambodia [Innovations for Social Accountability in Cambodia]

This presentation will discuss about the current landscape of data protection in Cambodia and the effort to establish the data protection regulations.

Data Protection and CyberSecurity
Speaker: Ts Alan Yau [Malaysia Board of Technologists]

Companies frequently create two discrete teams and purchase different tools to address cybersecurity and data protection separately. Two teams, two software sets, and considerable IT costs and administrative expenditures are required to maintain and manage them.
But is it the best course of action to separate data protection from cybersecurity? If you read the definitions of data protection and cybersecurity, it makes sense.
Data protection deals with a number of concerns connected to data storage, administration, and access, whereas cybersecurity deals with protection against cyberattacks. These two fields do differ from one another. To successfully handle data breaches, organisations should integrate cybersecurity and data protection into their routine operations.

Navigating Key Legal Issues on Data Privacy Compliance
Speaker: Maria Keala Mae M. Bleza, Data Privacy Lawyer [WiSAP (Women in Security Alliance Philippines)]

The presentation will delve on the discussion of the legal milieu of data privacy with focus on the following topics:

1. Key legal issues of data privacy concepts, compliance and implementation
2. Survey of data privacy cases in SEA

Date: 8 June 2023, Thursday
Time: 3PM – 5PM (SGT)
Venue: Zoom

back to top

Registration:
https://us06web.zoom.us/webinar/register/4216810994785/WN_llsql6lzSRy0VdqtSyKouQ

Cybersecurity Awareness & Advisory Programme (CAAP)

MAP Cybersecurity and Digital Trust on 18 April

AiSP had a booth at the MAP Cybersecurity Digital Trust Launch Event at Lifelong Learning Institute on 18 April. Thank you Singapore Business Federation for inviting us!

back to top

AiSP x SBF Workshop on 31 May 2023

back to top

Corporate Partner Events

Panel Discussion: Explore "2022 Threat Landscape Report" For A More Secure 2023 With Exposure Management on 20 April

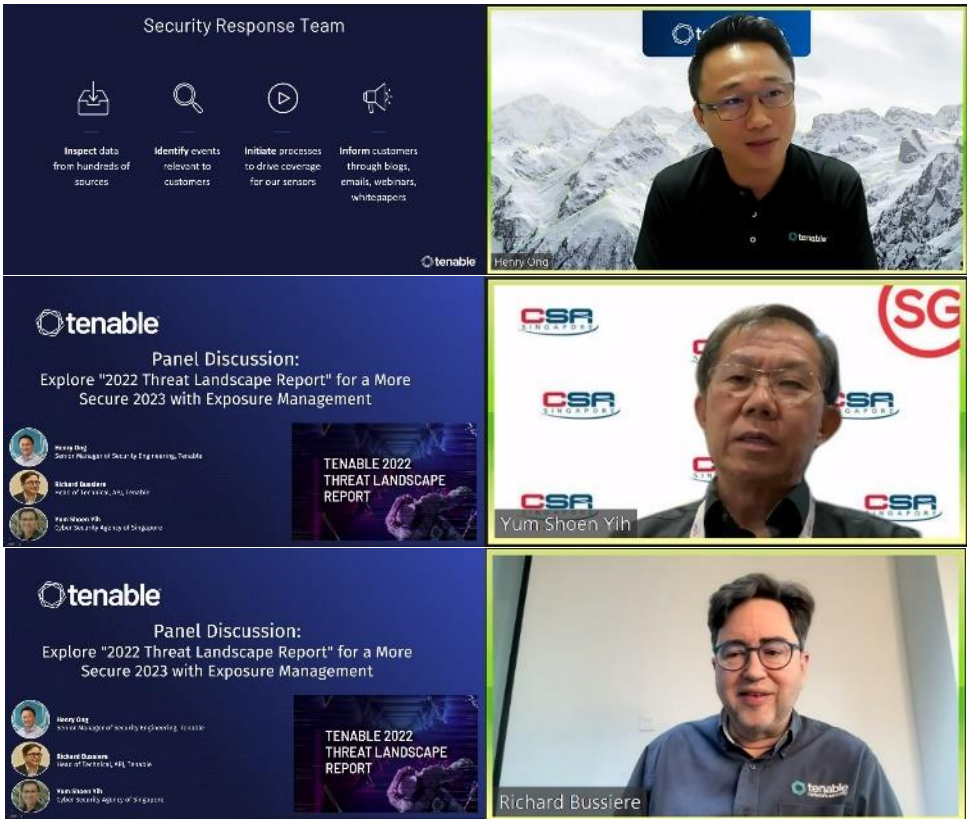
On 20 April, it was an insightful session with Mr Henry Ong and Mr Richard Bussiere from Tenable and Mr Yum Shoen Yih from Cyber Security Agency of Singapore (CSA) as they shared on

1) A review of the top threats, vulnerabilities and trends from 2022, including those impacting Cloud, Active Directory and OT environments

2) Takeaways and lessons learnt to enable defenders to enhance risk-based vulnerability and exposure management practices and improve overall security posture in 2023

3) How embracing the concepts of Exposure Management can help you and your team get grounded for a secure 2023.

Please click on the links if you're interested in the reports
https://www.tenable.com/.../2022-gartner-exposure...
https://www.tenable.com/.../tenable-2022-threat-landscape...
We hope the participants have benefitted greatly with the two perspectives presented and be able to apply what they learned today.



back to top

AiSP X SecurityScorecard – Navigating The Governance, Risk, And Compliance Landscape: Strategies For Success on 27 April

In collaboration with our Corporate Partner, SecurityScorecard and Grab, we organised a session on Navigating the Governance, Risk, and Compliance on 27 April. Thank you David Ng, Abhishek Gupta, Lau Han Yang and Catherine Lee for speaking. We hoped the attendees have gained insights from the session.

back to top

Cyber Intelligence Briefings - The Threat Of ARES Leaks on 24 May

Cyber intelligence Briefings - The Threat of ARES Leaks

Cyber threats are constantly evolving, so staying informed is crucial to maintaining strong security practices. This webinar will be an excellent opportunity to stay up-to-date and learn about the latest threats as they develop.

In this upcoming webinar, we will share our finding on **ARES**, a new threat actor group identified by CYFIRMA Research, that sells corporate and government authority databases. They exhibit cartel-like behavior, associate with other threat actors including RANSOMHOUSE, KelvinSecurity, and Adrastea hacker groups. ARES Leaks aims to rival BreachedForum by adding more threat actors and leaks to their platform. **The ARES group consists of penetration testers, malware developers, and offers Botnet and DDoS services**. The admin of ARES is involved in selling Zero-day vulnerabilities, indicating their exploitation of such vulnerabilities to compromise systems.

Join us to learn how ARES Leaks may pose a serious cybersecurity threat to your organization.

Date: 24 May 2023, Wednesday
Time: 11AM
Venue: Zoom
Registration Link:
https://us06web.zoom.us/webinar/register/2916826469767/WN_KAdj_9B9TYWurxa6a3UCRg

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 May	CISO Public Sector ANZ	Partner
5 May	AVIP Event with CE	AiSP
6 & 13 May	Cyber: 100	Partner
9-12 May	Black Hat Asia 2023	Partner
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
17 May	QUEST-AiSP Cybersecurity Talk Series	Partner
18 May	Cisco Fireside Chat	AiSP & Partner
24 May	School Talk at PSB	AiSP & Partner
24 May	Cyfirma Webinar	AiSP & Partner
25 May	Knowledge Series – Cyber Defence	AiSP & Partner
26 May	DFL E-Payment Learning Journey @ Admiralty	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
7 Jun	Cyfirma Webinar	AiSP & Partner
8 Jun	SEA CC Webinar – Data & Privacy	AiSP
9 Jun	AVIP Event with SMS Tan Kiat How	AiSP
10 Jun	Celebrate Digital @ East Coast	AiSP & Partner
10 Jun	Zhenghua Community Day	AiSP & Partner
21 Jun	Cyfirma Webinar	AiSP & Partner
22 – 24 Jun	CYSummit	AiSP & Partner
25 Jun	DFL @ Bukit Panjang	AiSP & Partner
27 – 28 Jun	Seamless Asia	Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

The ABC of Zero Trust and Interview with Cloud Leader "Swapnil Shah"

Introduction:

Many cybersecurity products, solutions and services are touting Zero Trust, Zero Trust security model, Zero Trust Architecture, etc. The purpose of this article is to help readers understand in simple form what is Zero Trust, how is it related to Zero Trust Architecture.

Finally this article wraps up with an Interview with Cloud Leader "Swapnil Shah" who will share insights into the new Norm for clients adopting Cloud and adopting Zero Trust in securing their assets in Cloud.

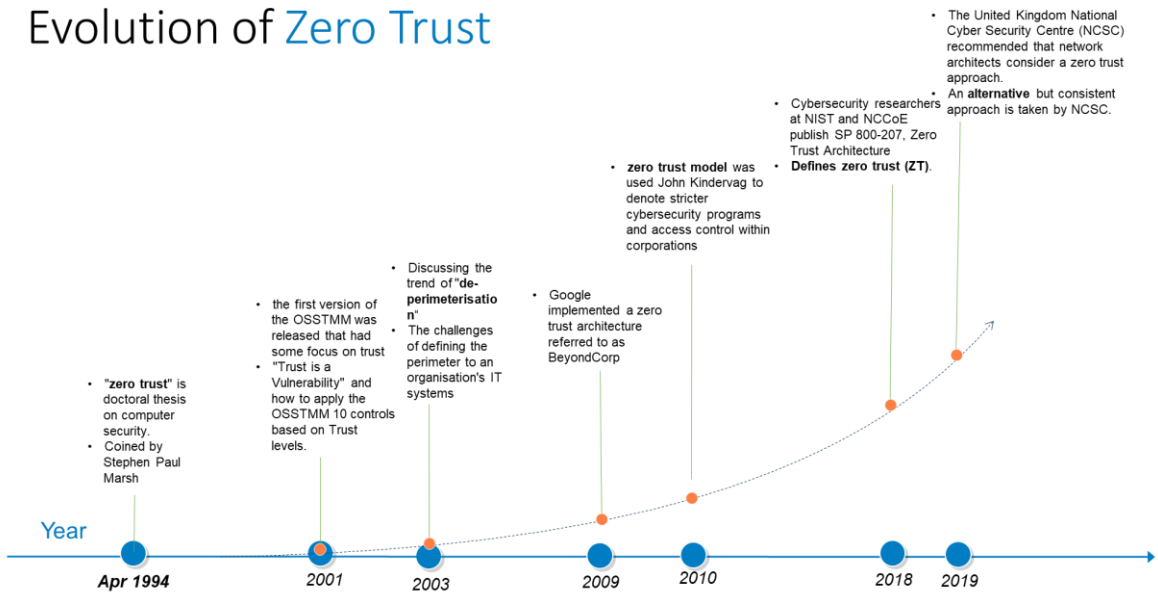
(A) Evolution of Zero Trust

To understand Zero Trust, we first look at the history of Zero Trust. The term "zero trust" started as a doctoral thesis by Stephen Paul Marsh in 1994. He believes that the concept of trust transcends human factors such as morality, ethics, lawfulness, justice, and judgement. Thereafter the concept of "zero trust" has been discussed. In 2009 Google implemented a zero-trust architecture referred to as BeyondCorp which consider both internal networks and external networks to be completely untrusted.

In 2018, US cybersecurity researchers at NIST and NCCoE publish Zero Trust Architecture (SP 800-207). They define Zero Trust (ZT) as a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. In 2019 the United Kingdom National Cyber Security Centre (NCSC) stressed the important of considering a zero trust approach for new IT deployment especially for cloud services.

The following diagram shows the timeline of Zero Trust:

back to top



(B) What is Zero Trust (ZT) security model and Zero Trust architecture (ZTA)

NIST defines that Zero Trust is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level.

Zero trust architecture (ZTA) is a plan where enterprise uses zero trust concepts and implementing it in its environment that includes network infrastructure (physical and virtual) and operational policies. Oftentimes the term ZTA is also known as follows:

1. Zero Trust architecture (ZTA)
2. Zero Trust security model
3. Zero Trust network architecture
4. Zero Trust network access (ZTNA)
5. Perimeterless security

The aim of ZTA is to prevent unauthorized access to data and services and to make the access control enforcement as granular as possible. This focus of ZTA is:

1. Enforce authentication, authorization, and
2. Reduce implicit trust zones without impacting service availability and delays in authentication mechanisms.
3. Access rules are made as granular and enforcing least privileges principle.

In today's market ZTA concept is commonly known as ""never trust, always verify," which means that devices should not be trusted by default whether they are in trust or untrusted network.

back to top

(C) Basic Rules of Zero Trust

A Zero Trust Architecture is designed and deployed with adherence to the following basic rules. These rules are ideal goals and it must be acknowledged that not rules can be fully implemented in the ZTA.

1. All data sources and computing services are considered resources.
2. All communication to be secured regardless of network location (trusted or untrusted location)
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. Enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Interview with Cloud Leader "Swapnil Shah"

In this section I had the privileged to interview Cloud Leader "Swapnil Shah" who share insights into client adopting cloud, viewpoints on cloud security and Zero Trust.

1. What is the new Norm for clients adopting Cloud?

   Cloud adoption is mainstream for some time now and Cloud First or Cloud Only strategies are commonplace across most enterprises across all leading markets. The adoption of the Cloud is key, and sometimes even synonymous, with Digital Transformation initiatives. It is common knowledge that Cloud adoption is the underlying key enabler for innumerable business use cases like telemedicine and connected health devices, smart grids for utilities, financial risk analysis, edge computing on 5G, IoT-enabled shop floors, contactless retail, drone-powered delivery, networks on the Cloud, autonomous and driverless cars, etc. Nevertheless, Cloud computing continued to languish as a mere technology upgrade project within most enterprises. The focus of enterprises is now shifting to how to innovate and differentiate by leveraging a wide range of cloud-native offerings and industry cloud solutions available from hyperscalers and various eco-system partners.
   The current pandemic has inserted an additional dimension of unpredictability and has accelerated the pace of digital transformation across industries. Multi-year project timelines are being compressed, and project requirements are being dramatically altered on-the-fly. Enterprises are now at a tipping point, for having to super-scale their Cloud-powered Digital transformation efforts.
2. Accelerated adoption of cloud combined with complex integration of eco-system, hybrid working environments is the new norm which poses interesting challenges to IT

back to top

executives not only from architecture & technology side but also from culture and security perspective as well. What are your viewpoints on Cloud security?

In traditional IT world, IT security was completely owned and controlled by various teams within IT or ISG groups. Cloud Security is a Shared Responsibility now shared between enterprises IT teams, Cloud provider and any eco-system partners involved in the solution. Modern cloud adoption presents very challenging security realities due to below key elements:

- automated CI/CD methods
- distributed serverless architectures
- and ephemeral assets like Functions as a Service and containers
- no clear perimeter boundaries
- api adoption explosion

This creates unique challenges like below which enterprise security team needs to assess on continuous basis

- complex environments with complex integration points outside enterprise perimeter
- increased attack surface
- lack of visibility & tracking
- complex data flow patterns between on prem, hybrid cloud (IaaS/PaaS) & SaaS based applications and users spread everywhere
- everchanging workloads

3. How should customers adopt Zero Trust in securing their assets in Cloud?

Basic guiding principles for Zero Trust in cloud security is not to automatically trust anyone or anything within or outside of the network and to authorize, inspect and secure everything. A Zero Trust approach extends throughout the entire digital estate and serves as an integrated security philosophy and end-to-end strategy. Enterprises as part of their cloud adoption journey should look at below Zero Trust based elements at a high level:

- Leverage cloud-delivered security measures where possible to implement Zero trust on cloud
- Granular, policy-based IAM and authentication controls across complex infrastructures: Reduce the attack surface area by limiting user access based on context.
- Zero-trust cloud network security: Controls across logically isolated networks and micro-segments
- Enforcement of virtual server protection policies and processes such as change management and software updates:
- Safeguarding all applications (and especially cloud-native distributed apps): E.g. leverage a next-generation web application firewall
- Enhanced data protection

back to top

- Threat intelligence that detects and remediates known and unknown threats in real-time
- Develop apps using Zero Trust principles

Biography: Alvin Tan

Alvin is a security practitioner certified in CISSP, CCSP and Azure. He has worked in the ICT industry for over 20+yrs. Alvin is experienced in several key technologies such as Data centres, Hybrid Cloud, International connectivity, Networks, Cloud Security, Information Security, Apps and Big Data solutions. He focused in helping enterprises creating competitive advantage through business transformation. He is a SIG member of AISP and a (ISC)² member.

Biography: Swapnil Shah

Swapnil Shah is Cloud executive with a passion for transitions and transformations in business and people. He is driven to empower clients to accelerate their digital transformation initiatives supported by technology and service transformation enabled by Cloud technologies. Swapnil holds a Bachelors Degree in Electronics Engineering. His career spans 23 years where he has played wide range of roles across Asia, UK, US and Australia across enterprise and telecom sector. He is also a very passionate and driven career & life coach who empowers IT, professionals & executives to successfully transition & transform their careers.

back to top

Article from our Corporate Partner, Wissen International

What is Privilege Escalation? Attacks, Understanding its Types & Mitigating Them

What is Privilege Escalation?

Privilege escalation is a cyberattack technique where an attacker gains unauthorized access to higher privileges by leveraging security flaws, weaknesses, and vulnerabilities in an organization's system. It is the attempt to elevate access permissions by exploiting bugs, system flaws, human behaviors, configuration oversights, or weak access controls. In most cases, the first penetration attack attempt is not enough to gain the required level of access to data. Attackers then resort to **privilege escalations** to gain deeper access to networks, assets, and sensitive information.

Privilege escalation attacks are performed to jeopardize business operations by exfiltrating data and creating backdoors. The goal of **privilege escalations** is to gain complete control over the system or network, with a malicious intent of security breaches, data theft, etc. Threat actors performing these attacks can be external hackers or insiders who start by carrying out a social engineering attack like phishing to gain access to computer networks and systems through credential theft.

As **privilege escalation attacks** can impact business reputation and continuity, strategic measures should be implemented for prevention, early detection, and mitigation.

Main Types of Privilege Escalations

Privilege escalation can be broadly classified into **vertical privilege escalation** and **Horizontal Privilege Escalation**.

Horizontal privilege escalation or account takeover is gaining access to the rights of lower-level accounts with similar privileges, mainly performed to increase the attacker's sphere of access.

Vertical privilege escalation, or privilege elevation attack, is hacking into a system to gain elevated privilege access beyond what the attacker already has.

Vertical vs. Horizontal Privilege Escalation

Often confused, vertical and horizontal **privilege escalations** refer to different methods of obtaining higher privileges within a system or a network. Horizontal privilege escalation

back to top

means obtaining access to the same level of privileges as a user. In contrast, vertical privilege escalation refers to obtaining a higher level of privileges than the user.
In case of a **horizontal privilege escalation**, a low-level employee with access to sensitive data may use that access to gain the same privileges as a higher-level employee, such as a manager. This enables the attacker to perform actions with the same level of authority as the compromised employee.

On the other hand, **vertical privilege escalation** refers to the process of gaining higher privileges than the user currently has. For example, a low-level employee may exploit a vulnerability in the system to gain administrative privileges, thus obtaining the ability to perform actions with a much higher level of authority.

Common Types of Privilege Escalation Techniques or Methods

There are various types of privilege escalation techniques that attackers can use to compromise a system. Some of them are discussed below.

1. **Social engineering-**
   In this technique, an attacker tricks a user into giving away their credentials or performing actions that grant the attacker elevated privileges. This can include phishing attacks, where an attacker sends an email posing as a trusted entity to trick the recipient into giving away their credentials, thereby giving the attacker access to the system.
2. **Pass-the-Hash/Rainbow table attacks-** Another technique is the pass-the-hash (PtH) attack, which aims at impersonating a user by using a stolen password hash to create a new session on the same network. To defend against this attack, modern systems must employ robust password management solutions to keep the hash unique between two sessions.
3. **Vulnerabilities and exploits-** Exploiting vulnerabilities in software and operating systems is another popular method of privilege escalation. Here, attackers exploit unpatched software vulnerabilities, buffer overflow issues, or other backdoors to gain privilege escalation.
4. **Misconfigurations-** In this attack, the attacker takes advantage of misconfigured systems to escalate their privileges. This can include weak passwords, unsecured network services, open ports, authentic failures, and other misconfigured systems.
5. **Kernal exploits-** In this technique, the attacker exploits zero-day vulnerabilities in the operating system kernel to escalate their privileges. This poses a serious threat as the kernel gets complete control over the system and can bypass security measures.

Best Practices to Prevent Privilege Escalation Attacks

Privilege escalation attacks can have severe consequences, including theft of sensitive information, disruption of operations, and reputational damage. By implementing strong passwords, restricting access, regularly updating systems, monitoring activity, and having

back to top

a clear response plan, organizations can reduce their risk of falling victim to privilege escalation attacks. Below are some best practices that must be adopted to prevent and mitigate such attacks:

- **Principle of least privilege-** This measure is required to limit access to sensitive systems, applications, and data to only those who need it.
- **Patch and update software regularly-** Keeping all systems, software, and applications up to date with the latest security patches is essential in fixing known vulnerabilities.
- **Vulnerability scanning-** Attackers find it harder to enter the network when all the IT infrastructure's components are routinely scanned for weaknesses. Before potential attackers can take advantage of them, vulnerability scans identify misconfigurations, undocumented system changes, unpatched or unsecured OSes and programs, and other problems.
- **Implement strong passwords-** Encourage users to use strong and unique passwords that are more challenging to guess or crack.
- **Security awareness training-** Conducting security awareness training is essential to prevent people in organizations from unintentionally assisting a privilege escalation attack by opening malicious links and attachments. It is also essential to emphasize the hazards and perils of sharing accounts and passwords.
- **Incident response plan-** It is imperative to have a clear incident response plan that outlines the steps to swiftly respond to detected incidents and prevent further exploitation.

Examples of Privilege Escalation Attacks

Some common examples of privilege escalation attacks are discussed below.

1. **Windows Sticky keys**– The 'sticky key' attack is the most common and fairly easy way of performing a privilege escalation attack. It does not require high technical skill sets. Attackers must have physical access to the system and should be able to boot it from a repair disk. By pressing the Shift key five times, an attacker can gain access to the Command Prompt with administrator privileges, allowing them to execute malicious code.
2. **Windows Sysinternals**– The Windows Sysinternals tool suite is another common method to conduct a privilege escalation attack. In this case, an attacker first performs a 'sticky key' attack to gain a backdoor into the system and then executes "psexec.exe -s cmd" to gain administrator privileges.
3. **Process Injection**– This privilege escalation attack targets weak processes. This process involves injecting malicious codes into running processes to elevate the privileges of that process.
4. **Linux Password User Enumeration**– This is another prevalent privilege escalation method where the attacker can use tools to enumerate valid usernames on a target system. Attackers first identify target accounts on a Linux system to carry out this attack by gaining access to the system's shell. This is mostly performed by exploiting misconfigured FTP servers.

back to top

5. **Android Metasploit**– Android Metasploit refers to using the Metasploit framework to exploit vulnerabilities in Android devices. The Metasploit framework is a popular hacking tool used by attackers that contains a library of known exploits. Attackers can leverage these exploits to perform privilege escalation attacks against rooted android devices.

Tools to Protect Your Systems from Privilege Escalation

The use of UEBA, password security tools, and vulnerability scanners can prevent privilege escalation attacks to a large extent. By monitoring user behavior, securing passwords, and identifying vulnerabilities, organizations can reduce their risk of being compromised by a privilege escalation attack.

1. **UEBA (User and Entity Behavior Analytics)**– UEBA is a security tool that uses machine learning to analyze user behavior and detect anomalous activity. This tool can identify changes in access patterns, attempts to access sensitive information, or escalate privileges. The **Exabeam Security Management Platform** and the **Cynet 360 Platform**, powered by UEBA, analyze abnormal account and user behaviors and provide comprehensive solutions to offer organizations real-time visibility into the security landscape.
2. **Password security tools**– One of the most common privileges escalations methods is cracking or guessing passwords. **Password Auditor** and **Password Manager Pro** are popular password security tools that offer a comprehensive password management solution and help individuals and businesses save and store their passwords securely. They also make the task of remembering complex passwords easy and encourage the use of unique and strong passwords for different accounts.
3. **Vulnerability scanners**– Vulnerability scanners are automated tools that scan a system, network, or application for vulnerabilities and misconfigurations that could be exploited for **privilege escalations**. Using vulnerability scanners will help organizations identify weaknesses, find coding bugs and get remediation guidance to mitigate security flaws before they are exploited. **Invicti** and **Acunetix** are two of the popular vulnerability scanners that can be used to detect security vulnerabilities.
4. **Privileged Access Management (PAM) software solutions-** PAM software solutions mitigate privileged access risks. PAM solutions protect organizations against privilege escalation attacks by identifying, monitoring, and detecting unauthorized access to sensitive information. **JumpCloud**, **Ping Identity**, and **Foxpass** are popular PAM solutions.

Privilege escalations can be a major security concern as they allow attackers to control the system and access sensitive information. While the use of these tools helps in the early detection and mitigation of privilege escalation attacks, it is important to note that these tools should be used as a part of a comprehensive security strategy and not relied upon as a sole solution.
For any enquiries, please contact aisp@wissen-intl.com

back to top

Article from our TCA 2022 Winner, Stanislav Protassov

TCA AWARDS 2022 – Leadership category: Winner, Stanislav Protassov

Sharing experience on winning the award and contributions to the cybersecurity ecosystem, future plans moving forward

Experience on winning Award

It is a great honour and proud personal achievement for me to receive the Cybersecurity Awards 2022 Leaders category award. I must say that the competition was tough, with many other good candidates ultimately shortlisted for the award. Winning this prestigious award is therefore especially dear to me. The award is also very eminent because it was conferred by the Association of Information Security Professionals (AiSP), and endorsed by the Cybersecurity Agency of Singapore (CSA).

With my new role as the Executive Board Member of Acronis, and President at Constructor University, I would like to take this opportunity in this article to share some ideas on how I could continue to make a difference and contribute to Singapore's recognition as a leader in cybersecurity and on talent and skills development.

Uncertainty in the current global economic & geopolitical situation

Since Covid-19 struck, there has been uncertainty in the global economic situation, which is looking less than rosy. With rising inflation and interest rates, many global economies are experiencing slower GDP growth rates. In the financial markets, investors have become more averse to taking risks, for fear of lower returns and financial instability across markets.

back to top

This has a ripple effect on the technology sector, where startups and small to mid-sized tech companies have been forced to lay off staff. Big tech companies have also not been spared, with even high-demand technical roles facing layoffs.

The economic outlook in Singapore

In Singapore, the situation is faring slightly better. GDP growth for 2022 had slowed to 3.6%, and the outlook in 2023 slowed down to a modest 2.5%. The headline inflation in 2022 had rocketed to a high of 6.1%, while in 2021 it was 2.3%. Despite the less-than-ideal figures for GDP and headline inflation, the employment climate in Singapore has been relatively good, as unemployment rates hovered at 2% (Jan 2023), the lowest in 3 years.

The onset of Digital Transformation / Smart Nation and what it means for the world

Many of us would by now be familiar with Singapore's plans to become a smart nation. A recent report by IMD ranked Singapore as the Number 1 Asian Smart City and number 7 globally. With these plans, the Singapore government has supplied massive investments to roll out new technologies, putting in place infrastructure for 5G and Machine Intelligence, as well as test-bedding Quantum technologies. Post Covid-19, many companies have successfully transformed their operations digitally, and many of us still adopt a hybrid work arrangement, which means we are more plugged in and reliant on digital devices than ever. All these developments have increased the possible cyber-attack surfaces for bad actors. As a result, cybersecurity will continue to grow in importance, amidst the backdrop of economic and geopolitical instability.

Why talent development is so important for Singapore

As a small country, Singapore's only natural resource is its people, or human capital. It can also be acknowledged that Singapore has weathered several previous economic turmoils, and has a low unemployment rate, thanks largely to its hardworking, adaptable, and intelligent workforce able to adapt to changing demands of employers.

However, the recent spate of layoffs in the tech sector showed that the tech sector and tech jobs, in general, are not immune to economic downturns and job security. Despite this, if Singaporeans stay focused and continuously find ways to improve and upskill themselves, they can ride this storm and continue to have good jobs in the technology sector, while contributing enormously to their companies.

Acronis is here to help train and develop not just tech talent, but all-rounded individuals

Over at Acronis, we are looking to train our staff with a similar mindset when it comes to talent development. The core skills of being hardworking, responsive, adaptable, and intelligent are skills that we try to inculcate in our employees.

In Singapore, Acronis' Singapore R&D team is a core development Centre for Acronis globally and has grown exponentially from 5 staff in 2015 to 160 in 2022, with a 60%

back to top

localization rate. Acronis also has the largest cybersecurity R&D team of any company, in Singapore. The Singapore R&D office manages several product charters such as the Acronis Cyber Platform.

We will continue with the organic growth of our Singapore R&D team and also focus on providing strong training to the team. My strong belief is that every engineer or developer should be trained in multidisciplinary skills, and be versatile in handling a variety of tasks.

Rewarding and progressing our staff

Over the years, we have also allowed our staff to rise and grow in the company. In our Singapore office, we have drawn up a progression roadmap for high-potential performers to rise through the organization. We have also put in place the Women in Tech (WiT) mentorship program, to empower our female engineers to learn from other female leaders in the company. We have also trained and converted mid-career professionals from other industries, in partnership with the DigiPen Institute of Singapore. We have rolled out incentive programs to help our bright staff continue growing, such as through the Acronis Cyber Dragon Award, which provides prize money, incentive trips, and stock options.

Lending my years of experience and leadership to help Singapore become a global leader in the tech sector

My personal goal is to help not just Acronis train and develop talent, but also for Singapore to become a recognized leader in the tech sector. This includes the fields of cybersecurity, machine intelligence, data protection, data privacy, and so on. To achieve this, there are several methods to choose from. We will need to continue being a leader in innovation. Additionally, we will need our R&D teams to continue developing new technologies that will fit into our product roadmap, for the global markets. By having provided great products for our customers and extending our leadership in cyber protection, we will be able to put Singapore on the world map for cybersecurity, given that the core of our global R&D teams is based in Singapore.

The onset of smart nations, the proliferation of robots, and the pervasive use of machine intelligence will result in new job roles being created for IT systems and infrastructure. These are jobs that our future engineers and technicians can look forward to. Therefore, I believe that besides understanding how to code, we should help our engineers and young children understand how basic IT infrastructures operate. This will help them frame their knowledge of technology from an early stage and could help them become better engineers upon entering the workforce. I am currently exploring ideas on how to co-develop such a curriculum with the schools in Singapore.

R&D Leadership and Innovation

Through my leadership of Acronis' Singapore R&D team, we have successfully grown our R&D headcount by more than 30 times since its establishment in 2015. With my extensive

back to top

knowledge in innovation and patenting (212 patents under my name, with 140 pending patents), I share with the Singapore team strategies on how to develop novel yet practical innovations. As a result, our local R&D team has successfully registered patents, which has increased twofold over the past two years.

PR

On the PR front, Acronis has done extensive publicity to showcase Singapore as a leader in cyber protection. For example, we received around 17,500 media coverage per year about Acronis as a Singapore-founded cyber protection company. I have also done over 30 interviews for international and local media as a cybersecurity expert based in Singapore.

Participation in Global Conferences

We have also worked on other fronts to enable Acronis' brand name to shine bright on the world stage. For example, we participated in many international conferences, such as WEF, Interpol, Europol, Black Hat, and many more. We published several white papers for WEF to place us on the map as thought leaders.

Looking to the future

Moving forward, I hope to continue guiding the Acronis team to new heights. We need to continue training, innovating, and trying to better understand our customers while leveraging our government relations, PR, and marketing campaigns to help us extend our reach.

In addition, we must explore new business opportunities in areas such as AI for cybersecurity, automation, performance enhancement, etc. We will also need to find new opportunities in research areas such as privacy-enhancing technologies, IoT security, network security, the Metaverse, quantum computing, and more.

On the product front, we will continue to innovate, for products that will better serve our managed serviced providers and make it more seamless for our products to integrate with their systems.

We will continue to train and develop local talent, including an upcoming project to train highly skilled security operations analysts for diploma holders and mid-career hires.

I will also lend my experience as the President, Constructor University, which is a German University founded in Bremen, to the education system in Singapore, and we are ready to work with the Singapore government as advisors and collaborators, on helping to design the best curriculum for schools in Singapore.

It is also important for us to continue working closely with our existing government partners, like the Cybersecurity Agency of Singapore, EDB, and IMDA to identify areas where we

back to top

can help Singapore, such as on research projects, promoting cyber awareness, and advising on national cyber strategies.

With the above efforts, we can help advance Singapore's position as a leader in cybersecurity, to become number one in the region and top three in the world, on par with countries such as Israel and the US.

In conclusion, reaching the top can only be possible through continuous investment in attracting and training talent – through a strong pipeline of developing and training local talent, augmented with top cybersecurity talent from all around the world to share their expertise. Acronis is therefore strongly committed to working closely with the Singapore government and our partners, to help Singapore become a leader not just in cybersecurity, but in the tech industry as a whole!

Thank you very much, and once again, it is my great honour to be a recipient of this Award

back to top

Reflection from our SVRP 2022 Winner, Skyler Lee

I am honored to receive such a prestigious award. As a student volunteer, I have had the privilege of collaborating with a diverse range of organizations and individuals to advance the cause of cybersecurity. One of my most rewarding experiences has been leading weekly workshops for Polytechnic students, helping them to upskill themselves on the latest cybersecurity topics and promoting a culture of cybersecurity awareness.

In these workshops, I have covered a wide range of topics, including penetration testing, cryptography, threat intelligence and more. Through interactive and engaging sessions, I have encouraged students to develop their technical skills and critical thinking abilities, while also emphasizing the importance of ethical behavior and responsible use of technology. One of the more meaningful experiences would be working with CSA to conduct the yearly Youth Cyber Exploration Programme where we conducted a 3-day camp for secondary school students to get them interested in cybersecurity. This helps to reinforce the future cybersecurity talent pipeline and ensure that we will have more talented professionals in the industry.

Beyond the classroom, I have actively participated in various outreach and awareness-raising activities to promote cybersecurity. One of the highlights of my involvement has been organizing the recent Lag and Crash 3.0 capture the flag (CTF) competition. As one of the organizers, I helped to design the CTF challenges and event. This was a great opportunity to bring together students and professionals from different backgrounds and skill levels to compete in a friendly and collaborative environment. Through this event, we were able to promote cybersecurity awareness and encourage participants to develop their technical skills and critical thinking abilities. We also fostered a sense of community

back to top

and collaboration among the participants, as they worked together to solve challenging problems and learn from one another.

Aside from my volunteer work, I have pursued academic and research opportunities in the cybersecurity field. Completing my diploma in Infocomm Security Management has provided me with foundational knowledge, while my research on upcoming cybersecurity trends such as Operational Technology and Purple Teaming has been shared with other industry professionals.

Moving forward, I hope that I will be able to join the Digital and Intelligence Service during my National Service and pursue a degree in Infocomm Security after NS. My goal is to learn and research more on cybersecurity trends and how we can use new technology to reduce threats. I believe that Artificial Intelligence is one such example of a tool that could be utilized for predictive networking and help to further secure our digital infrastructure.

Overall, my experiences as a student volunteer have taught me the importance of promoting cybersecurity awareness and education, while also providing me with opportunities to learn, grow and make a positive impact in the cybersecurity ecosystem.

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.

back to top

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!

back to top

Listing of Courses by ALC Council

Stand out from the crowd

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

We offer the most in-demand cyber certifications including:

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

The right training makes all the difference

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

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

AiSP Member Pricing – 15% discount

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

back to top

Upcoming Training Dates

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

Special Offers.

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

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

Thank you.

The ALC team

ALC Training Pte Ltd
3 Phillip Street, #16-02 Royal Group Building, Singapore 048693
T: (+65) 6227 2883 | E: learn@alctraining.com.sg | www.alctraining.com.sg

back to top

Qualified Information Security Professional (QISP®)

Promotion for Qualified Information Security Professional (QISP) Exam until 31 May!

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 31 May 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:

back to top

- 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 (Physical)

Physical

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.

back to top

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

Transformists NETWORK

Delivery Partners

Ai Network 360 | OPUS ACADEMY | NETASSIST

back to top

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

back to top

- 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.

back to top

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

For any enquiries, please contact secretariat@aisp.sg

back to top

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.

back to top

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

back to top

back to top

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

AiSP Academic Partners

back to top

Our Story…

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

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

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

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

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

AiSP Secretariat Team

Vincent Toh
Associate Director

Elle Ng
Senior Executive

Karen Ong
Executive

www.AiSP.sg
secretariat@aisp.sg
+65 8878 5686 (Office Hours from 9am to 5pm)
6 Raffles Boulevard, JustCo, Marina Square, #03-308, Singapore 039594
Please email us for any enquiries.

back to top

