NEWSLETTER

March 2023

NEWS & UPDATE

New Partners

AiSP would like to welcome Eclypsium, KnowBe4 and IQPC 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 ABP Group and Blackpanda for their continued support in developing the cybersecurity landscape:

News & Updates

Prime Minister's Chinese New Year Garden Party on 5 February

AiSP and our Corporate Partner, Trend Micro were invited to the Prime Minister's Chinese New Year Garden Party on 5 February at Istana. Thank you People's Association for inviting us! Looking forward to more activities with PA in 2023!

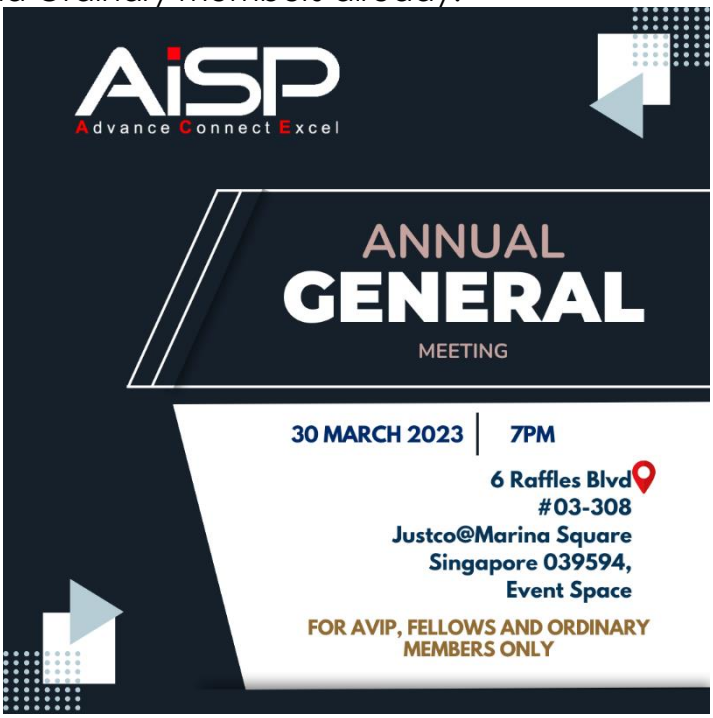
back to top

First Aid Course on 16-17 February for AiSP staff and SIT Lecturers

AiSP staff and Singapore Institute of Technology (SIT) Lecturers went on a 2-day course for First Aid Training on 16-17 February. A big thank you to People's Association (PA) for organising the course and getting us certified as First Aiders.

Annual General Meeting

AiSP cordially invites all AVIP, Fellows and Ordinary members to the Annual General Meeting which will be held on 30 March, 7pm. Details and agenda had been sent out to all AVIP, Fellows and Ordinary members already.



We would appreciate if you could confirm your attendance here latest by **5:00 PM, 16 March 2023**

back to top

Knowledge Series Events

Data & Privacy on 22 February

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 22 February, we held our Knowledge series on Data & Privacy, Personal Data Protection Commission. Thales Cloud Security shared insights to our attendees on Data & Privacy.

Our Data & Privacy SIG Lead, Wong Onn Chee moderated the panel discussion on DPTM - The Good, The Bad and The Future together with our panellists, Mr Shaun Chen, Ms Trina Swee, Mr Dominic Ng and Mr Hoi Wai Khin. Thank you all attendees who came down to Justco for the sharing.

back to top

Upcoming Knowledge Series

Cloud Security on 12 April

AiSP Knowledge Series – Cloud Security

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 around risk assessment, identity, and access management, data management and encryption, application security, disaster recovery, etc. The current webinar aims at explaining the need

back to top

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

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

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)

School Talk at Unity Secondary School on 24 February

As part of Digital for Life Movement, AiSP conducted a school talk to the whole cohort of students at Unity Secondary School. AiSP EXCO Member, Mr James Tan shared insights on Cybersecurity awareness and Careers Opportunities in Cybersecurity to the students.

back to top

AiSP Bug Bounty Workshop on 13 April

AiSP Advance Connect Excel

AiSP Bug Bounty Workshop

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 $150 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 Surface with Exposure Management**

back to top

1st Prize: Worth $150 gift prizes
2nd Prize: Worth $100 gift prizes
3rd Prize: Worth $75 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.

	Dick Bussiere, Technical Head, APAC, Tenable
1630:	**Prize Presentation**
1700:	**End of Event**

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

back to top

AiSP Advance Connect Excel

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

back to top

AiSP Advance Connect Excel

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

Example B
- Leadership: 0 Hour
- Skill: 18 Hours
- Outreach: 18 Hours

Example C
- Leadership: 0 Hour
- Skill: 36 Hours
- Outreach: 0 Hour

Example D
- Leadership: 0 Hour
- Skill: 0 Hour
- Outreach: 42 Hours

Scan the QR Code for the Nomination Form

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

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

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

back to top

AiSP Cyber Wellness Programme

Click here to find out more!

back to top

Ladies in Cybersecurity

AiSP Ladies In Cyber Learning Journey To SIT@NYP on 8 March 2023

We are honoured to have Ms Nadia (Member of Parliament for Ang Mo Kio GRC) as our Guest of Honour for the dialogue session together with Ms Sandy Cheong (Assistant Director at iHIS) and Dr Purnima (Assistant Professor at SIT@NYP). Ms Soffenny Yap, AiSP Secretary & EXCO Lead for Student Volunteer Recognition Programme (SVRP) will be the moderator for this event. The event is open to only female students in tertiary level and female PMETs.

Join us on 8 Mar 23 from 6.30pm to 9pm at SIT@NYP for the International Women Day Celebrations and get to find our more on what SIT can offer for the Cybersecurity courses that you can embark on and latest research in cyber through the booths setup by SIT and speak to the SIT staff on the University life / Life Long Learning Education in cyber. You will also be able to view their innovation lab as part of the learning journey.

You can sign up by clicking here.

back to top

Ladies in Cyber Symposium on 18 March

As part of AiSP Ladies in Cyber Charter 5years Anniversary Celebration happening from 1 Mar 23 to 30 Nov 23, AiSP will be organising a series of events to celebrate the Anniversary. We will be organising our second AiSP Ladies in Cyber Symposium 2023 on 18 Mar 23 at Big Picture at CapitaLand - Capital Tower Level 9 located at 168 Robinson Road, Singapore 068912 from 12.30pm to 3.30pm where we will invite about 120 to 150 female Youths & female PMETS for a afternoon symposium and join our Guest of Honour in a dialogue session. The theme for this year symposium is Pioneering AI and Cybersecurity ; Women Charting the course.

In today's world where AI technology is rapidly transforming the cybersecurity landscape, women are emerging as key players, breaking down barriers and driving innovation. In this symposium, AiSP brings together leaders and experts in the fields of AI and cybersecurity to discuss the role of women in shaping the future of these industries. The event will feature keynote

back to top

speeches, a panel discussion, and interactive sessions designed to explore the challenges and opportunities facing women in these fields. It will also highlight the important contributions they are making to drive innovation and progress.

Whether you are a seasoned professional, a student, or simply interested in learning more about the intersection of AI and cybersecurity, this symposium is a must-attend event for anyone looking to deepen their understanding of these critical fields and to connect with others who are committed to driving positive change through technology. AiSP will also be launching the Ladies in Cyber Bear during the Symposium too. All attendees will get our limited edition bear after completing a survey on the day itself.

Front Side Back

The details for the event are as follow:
Date: 18 Mar 23 (Sat)
Time: 12.30pm to 3.30pm
Venue: Big Picture at CapitaLand - Capital Tower Level 9 located at 168 Robinson Road, Singapore 068912
Dress code: Smart Casual
Guest of Honour: Minister Josephine Teo, Minister for Communications and Information and Minister-in-Charge of Smart Nation and Cybersecurity

Please sign up by 10 Mar 23. Please note that the registration is based on first come first serve basics.

Register here

back to top

Special Interest Groups

CTI Networking Session on 10 March

Hi Everyone, we are organising a networking session for the CTI SIG
Date: 10 Mar 2023, Fri from 5.30pm - 7.30PM at JustCo @ Marina Square, 6 Raffles Boulevard, JustCo, Marina Square, #03-308, Singapore 039594
Register here

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 will start 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! Limited sponsorship packages are available.

TCA 2023 CALL FOR NOMINATION IS NOW OPEN TILL 14 APRIL 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 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

THE CYBERSECURITY Awards 2023

Organised by

AiSP Advance Connect Excel

Supported by

image engine

SFA SINGAPORE FINTECH ASSOCIATION

Supporting Associations

CSCIS CSA cloud security alliance HTCIA

ISACA Singapore Chapter (ISC)2 SINGAPORE OT-ISAC

SINGAPORE COMPUTER SOCIETY SGTECH THE LAW SOCIETY OF SINGAPORE

back to top

Platinum Sponsors

Gold Sponsors

Silver Sponsors

Digital for Life

Celebrate Digital @ Nee Soon on 12 February

AiSP would like to thank Minister for Manpower Dr Tan See Leng for visiting AiSP and Corporate Partner Grab's booth on 12 February for the Celebrate Digital @ Nee Soon. Big shoutout to our AiSP EXCO Lead for Cyberwellness, Mr Dennis Chan for sharing with the residents in Nee Soon on the importance of Cyberwellness on 网络安全人人有责.

back to top

Celebrate Digital @ Bukit Panjang on 11 March

Join us on 11 March at Celebrate Digital @ Bukit Panjang for digital talks listed below. Walk away with free gifts when you visit the booths!

back to top

Corporate Partner Events

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

Navigating the Bug Bounty Landscape: Best Practices and Lessons Learned

Bug Bounty programs have revolutionised the way organisations approach cybersecurity by tapping into a global community of ethical hackers to identify and report vulnerabilities. As cyber threats continue to proliferate, Bug Bounty programs have become an essential part of any organisation's cybersecurity strategy.
Bug Bounty is often mistaken to be only accessible to larger companies with significant resources. However, in actuality, even small to medium businesses can participate and reap the benefits. By offering incentives to ethical hackers, Bug Bounty provides an efficient and cost-effective way to identify and remediate vulnerabilities.

Join us on 7 March, 10:00 am SGT, for an engaging workshop on Navigating the Bug Bounty Landscape, featuring expert insights from YesWeHack and Talenox:

- Eileen Neo, APAC Team Manager of YesWeHack, will introduce the benefits of Bug Bounty programs and how they can drive cost savings and achieve measurable ROI.

back to top

- Edwin Feng, Co-Founder & CTO of Talenox, will provide a real-world case study by sharing his experiences in setting up and evolving Talenox's Bug Bounty program.

With a focus on best practices and lessons learned, this workshop will provide a comprehensive understanding of the key elements of a successful Bug Bounty program! Don't miss this opportunity to learn from the experts and take your cybersecurity strategy to the next level.

Date: 7th March 2023, Tuesday
Time: 10AM – 12PM
Venue: JustCo @ Marina Square, 6 Raffles Boulevard, JustCo, Marina Square, #03-308, Singapore 039594
Registration: https://forms.office.com/r/bBfeyRyTG4
**Lunch will be served after the event.

back to top

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

Threats have evolved. So must your Privileged Access Management.

Excessive or poorly managed privileges are a cybersecurity headache that many organisations struggle with. Past data from Forrester Research has shown that privileged credentials were implicated in 80% of data breaches.

In a recent survey conducted by BeyondTrust, 54% of Singapore IT-leaders believe that users in their organisations have excessive privileges beyond what is required to do their jobs.

So, what can be done to better manage privileges? How can organisations guard against common threats while helping employee productivity?

Join experts from AiSP, BeyondTrust, Deloitte, GovTech as they discuss the evolving cybersecurity threat landscape, the perils of excessive privileges and how modern Privileged Access Management (PAM) can fortify your security posture.

back to top

When
Thursday, March 9, 2023
1.30pm to 5:00pm

Where
HUONE Singapore, Runway Room
3D River Valley Road, #03-01, Block D, (S)179023

Agenda

- Security in the perimeter-less World
  Johnny Kho, President, AiSP
- Privileged attack Vectors: Building Effective Defence Strategies (Live Demo)
  Chris Lee, PAM Evangelist, BeyondTrust
- A Holistic approach to Securing Digital Identities and Interactions
  Eric Lee, Executive Director, Deloitte
- Panel Discussion
  Guest Panelist: Mathew Soon, Director - Detection and Response Operations, GovTech

Register Now

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
1-3 Mar	XCION in Bali	Partner
1 Mar	HPC Cybersecurity Workshop at SCA2023	Partner
2 Mar	Mimecast Connect Event	Partner
7 Mar	Event with YesWeHack	AiSP & Partner
8 Mar	International Women Day Celebration @ SIT@NYP	AiSP & Partner
9 Mar	Threats have evolved. So must your Privileged Access Management.	AiSP & Partner

back to top

9 Mar	MFA CSC Talk by Sugar Chan	Partner
10 Mar	CTI SIG Networking Event	AiSP
11 Mar	Celebrate Digital @ Bukit Bangkit	AiSP & Partner
18 Mar	Ladies in Cyber Symposium	AiSP
23 Mar	Cyfirma Event	Partner
26 Mar	Celebrate Digital @ CCK	AiSP & Partner
30 Mar	Annual General Meeting	AiSP
30 Mar	AVIP Event with CE	AiSP
30 Mar – 1 Apr	CYSummit	Partner
4- 5 Apr	CISO Perth	Partner
12 Apr	Knowledge Series – Cloud Security	AiSP & Partner
13 Apr	AiSP Bug Bounty Workshop	AiSP & Partner
17 – 21 Apr	Learning journey to Hanoi, Vietnam	AiSP & Partner
18 Apr	PDD Connecting Smartness	Partner
25 Apr	AiSP x WiSAP MOU Signing	AiSP & Partner
25 Apr	School talk at SJI	AiSP

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

back to top

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

SMEs are taking a Cloud-First approach, but are they prepared to handle cyber incidents?

Cloud services are an easy pathway to set up a business, and startups and SMEs know this.

Singapore has been adopting cloud solutions at an accelerated pace. In recent years, most of the businesses that reach out to Blackpanda for cyber preparation services and incident response have been SMEs and startups which are entirely reliant on cloud-based platforms.

In fact, 98% of business systems currently operate either fully or partially in a cloud computing environment, which may include a combination of networks, storage, virtualization, and management software.

Nowadays, business networks typically consist of a combined cloud infrastructure from a number of cloud providers, including Software as a Service (SaaS) and Platform as a Service (PaaS). There are many challenges related to this, including data volume, accessibility, and the rapid evolution of threats. This has meant that since the transition from on-premises to cloud computing over a decade ago, incident response has changed drastically.

This year alone, 27% of businesses experienced a cyber attack to their cloud environment, according to CheckPoint. In order to stay in business, organizations that adopt a cloud-first approach need to keep themselves prepared in case of critical, service-disrupting incidents. With cyber attackers increasingly targeting the cloud, organizations should prepare themselves to respond to this type of cyber breaches.

This article will look at cloud adoption in Asia, cyber security responsibility in the cloud, and common cloud cyber attacks, highlighting how organizations should be prepared to handle cyber attacks to their cyber infrastructure, software and platforms.

Singaporean companies love the Cloud

The business-friendly environment and a robust infrastructure setup make Singapore a leader in the use of cloud computing in the ASEAN region. In particular, there has been a push from the government to adopt cloud services, which has contributed to 60% of

back to top

Singaporean IT leaders not foreseeing owning a data center within the next five years according to a survey.

Another study found that 90% of companies worldwide are currently using the cloud for at least some of their operations.

If cloud adoption has definitely been growing, experience indicates that cloud security is still lagging behind. Studies have shown that most companies that utilize cloud solutions get breached. A 2021 survey conducted by the International Data Corporation (IDC) found that globally, **98% of businesses experienced at least one cloud data breach** between 2020 and 2021, and the trend is growing.

Who is responsible for data management in the cloud?

Companies are often using third party vendors to handle all their services. This may come with the assumption that the responsibility for data stored in the cloud is also given away to the service provider. But this is not entirely true.

It is important to note that cloud security refers to the entire ecosystem of people, processes, policies, and technology that handles and protects cloud-based data and applications. All stakeholders are responsible for its security, including the organization, the cloud provider, and its users. In the cloud, data can be protected, but the people who have access to it determine whether it is secure.

This shared responsibility model is at the core of cloud cyber security, and depending on how enterprises distribute cloud-based applications among varying environments, the level of responsibility each stakeholder has will be different.

Here are three models of cloud infrastructure:

- Public cloud - whereby the cloud vendor owns infrastructure with the business retaining ownership of the data and virtual network. Here, responsibility for security is fully shared

- Private cloud – whereby the cloud is hosted in an enterprise's data center, with the sole responsibility of security vested in the corporation. In this case, the operating business is responsible for the protection of its infrastructure, as well as the applications and data that run on it

- Software-as-a-Service (SaaS) – in this popular model the cloud vendor hosts applications and makes them available to businesses via the internet. Users have instant access to documents without the inconvenience of installing applications

back to top

on personal devices, and synchronizing data across many devices. Each SaaS has a specific policy dictating who is responsible for which specific security tasks

As a rule of thumb, organizations are usually responsible for managing the platform, identity and access management, application security, operating system (OS) security, network traffic encryption, server-side encryption and data integrity. On the other hand, cloud providers are generally responsible for the security of the database, computing power, storage, networking, and managing availability zones and edge locations.

It is important to note that according to Gartner, approximately 95% of cloud security breaches will be caused by organizational security failures by 2025. Shared responsibility models require both parties to understand their responsibilities and roles. Cloud providers should ensure their security standards are acceptable based on an enterprise's industry, company requirements, regulations, and risk profile. At the same time, organizations should prepare themselves to respond to the very likely occurrence of a cyber attack to their cloud databases and systems. The main threats affecting cloud-based companies include:

- Account hijack – a type of attack that compromises users credentials
- Insider threat – a violation that happens as a result of employees who misusing authorized access
- Malware injection – a type of attack whereby codes or scripts used for malicious activities are inserted into a webpage
- Abuse of cloud services – this occurs when users store illegal software in the cloud, including pirated music and videos
- Insecure Application Programming Interfaces (APIs) – often used to customize the features of the cloud. If not properly secured, API can become vulnerable because of inadequate authentication or encryption
- Denial of Service (DoS) – cyber attacks that overwhelm servers with junk activity, making them unavailable
- Data breaches – cyber attacks where sensitive data is captured and exfiltrated by a criminal
- Insufficient due diligence – cloud security is compromised when there is inadequate owing diligence done when organizations are not clear about their policies
- Cloud ransomware – malicious data encryption on the cloud has been historically rate, but is more and more often seen as one of the biggest threats to the future of cloud computing

back to top

In the next section, we will take a deeper look into the threat of cloud ransomware, and how organizations of all sizes should prepare themselves to respond to cyber attacks on their cloud infrastructure, software and platforms.

Cloud Ransomware

Cloud ransomware, which was previously extremely rare, is now growing in frequency. According to a study by Netskope, most (66.4%) of malware instances in Q2 2021 started with cloud storage apps.

Traditional ransomware cannot attack API-based cloud storage systems, as these do not have access to file systems. As a result, threat actors are developing new TTPs to launch ransomware attacks more easily in cloud environments. These are highly challenging to predict, which is why only the most experienced incident responders are able to anticipate what these TTPs might entail in order to best prepare for and respond to them.

In order to encrypt persistent data in cloud resources, cloud ransomware actors are likely to use cloud APIs to find and access cloud resources that contain persistent data.

A threat actor may target specific cloud services based on the APIs for accessing them, or they may develop different payloads for each targeted service (just like some traditional ransomware actors have previously developed different payloads targeting different operating systems).

Last year, the average ransomware demand was USD 2.2 million, according to Palo Alto Networks, and as attackers start targeting the cloud, this is only predicted to rise.

Cloud incident response

As cloud workloads rapidly evolve, organizations require experienced incident responders, who have a deep understanding of cloud security, investigations, and specialized tools and processes.

By engaging an experienced team of cloud incident responders, organizations can cut down the dwell time of cyber attacks–that is, the time that intercurs between the start of an attack and when it is eradicated–comply with legal requirements, ensure business continuity, and limit the damages that such breaches may cause. This way, having a cloud incident response strategy helps organizations deliver their cloud-based services and products reliably and efficiently.

Cloud incident response involves the alignment of critical resources, operations, and services necessary to manage incidents within a cloud infrastructure. Knowing who to contact in case of a cloud cyber attack, and having a comprehensive cloud incident

back to top

response plan allow cloud technicians to quickly restore the operations of a downed service.

Conducting frequent compromise assessments is also vital to ensuring cloud cyber security. By detecting and containing malware through proactive threat hunting, organizations can limit their impact on electronic data and valuable networks, and eradicate cyber incidents prior to their escalation into full blown cyber crises.

About the Author

Larabella Myers is a cyber security specialist and technical communicator from the UK and Italy, and her work has always had a deep focus on the Asian cyber threat landscape. As Senior Cyber Security Analyst at Blackpanda, her focus is on producing cyber thought leadership, as well as on assisting clients with technical cyber security guidance and support.

She has worked in the technology industry for over 5 years, first within the IT space and then supporting the British government through cyber security research and consulting. Larabella studied Philosophy, Politics and Economics at the University of Warwick, and she leverages her social sciences insights to bring a multidisciplinary nuance to the field of cyber security.

She is the author of three published papers on technology geopolicy in academic journals, and is active in the cyber security scholarship community. She also holds several certifications in cyber security, including Security+ and CySa+ (CompTia), Cyber Security for Business Leaders (Oxford Saïd Business School) and Cloud Practitioner (AWS). In 2022, she was recognised as Woman of The Future for Technology and Digital.

back to top

Article from our SME Conference Sponsor, Globalsign

We hear you. Electronic signatures are a new thing, and for a company that has long been signing documents using wet-ink on paper, it feels intimidating to try out something new.

But did you know that in contrast to traditional wet-ink signatures, e-signatures have a history of action taken with the document (also known as audit trail), so that there is valid proof of the time the document was opened, viewed, and signed?

And let's be real, while wet signatures are tried and tested through time, they do present some problems. For example, they can be forged if not signed in person. Paper-based processes are slow and often costly due to logistics reasons. They also use up a lot of paper, which isn't exactly good for the environment.

back to top

To overcome the weakness of paper-based signing, electronic and digital signatures are becoming the method of choice for a lot of companies in getting important documents signed such as contracts, agreements, client forms, authorizations, and more.

In this blog, we will discuss the integrity and legitimacy of electronic and digital signatures, as well as answer the big question: Can digital signatures be forged?

But first, let us define electronic and digital signatures, how they work, their features, and the laws governing them.

Digital Signature vs Electronic Signature

Why is it important to distinguish the difference between digital and electronic signatures?

Knowing the difference between electronic and digital signatures can help your company find the right document management and signing platform that will best suit your needs.

What are Electronic Signatures?

An electronic signature can be a signature in the form of an image, fingerprint, symbol, or even process. Its main goal is to verify a document. It is also a good alternative to wet-ink signatures as it is more flexible and convenient.

That said, not all electronic signatures include digital certificate. In such cases, they can still be legally binding if all parties agree so.

Standard e-signatures without digital certificates are fine to use for agreements and approvals without strict compliance standards. For example, companies can use standard e-signatures for signing internal documents such as leave forms and other requests.

- **How Electronic Signatures Work**

  While e-signing itself is straightforward, it is built upon a complex backend process to ensure its efficacy. The complexity also varies depending on the option you are using.

back to top

Electronically signing a document can be as straightforward as signing with a stylus and a tablet or as advanced as using verification technology such as encryption and digital IDs under a digital certificate. The first method is often used in hotel lobbies and cash registers. In this case, the signature is captured and appended to the document.

The second method, or the more advanced form of electronic signatures, is the preferred method for most industries with more stringent signing requirements. Since the process requires the user to confirm their identity to bind their signatures to an identity through a digital certificate, the parties can ensure that the document and signatures are verified and authentic.

- **Are Electronic Signatures Safe?**

Electronic signatures are safer than paper-based signatures. While paper-based signatures are subject to forgery and tampering, electronic signatures are supported with many layers or security processes that make them difficult to forge and tamper with.

As such, electronic signatures are recognized by international regulations and are legally binding. In Europe, the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation recognizes electronic signatures along with varying degrees of security: standard, advanced, and electronic.

What are Digital Signatures?

Now, let's dive into digital signatures. How do they differ from electronic signatures?

Sometimes, industry-specific regulations require a digital certificate to ensure e-signatures are compliant. We can say that digital signatures are the more "secure" subset of electronic signatures.

This is because the signature is bound to a digital certificate for encryption. You can think of it as an electronic fingerprint. Digital signatures verify a signer's identity, which is why they are often used within industries with stringent standards such as healthcare and legal institutions. Digital signatures are often used for contracts, tax documents, and insurance forms.

In short, **digital signatures are legally binding and authenticate the document stronger than a standard electronic signature would**.

back to top

When dealing with documents that require stringent security measures and strict compliance standards, then a digital signature is the best option.

- **Digital Signature Features**

  As mentioned above, digital signatures offer a more secure way of electronically signing documents.

  First, it provides **authenticity**, solid proof that the person who signed the document is really who they claim to be, thanks to digital certificates linking the users signature to an actual identifiable entity.
  Second, it ensures **integrity**, proof that the documents have not been tampered with or altered in any way since the document was signed.
  Third, it ensures **non-repudiation**, proof of the sender's identity such that the signature's validity cannot be denied nor disputed.

  These key features ensure the signed document is safe, legitimate, and legally admissible.

E-Signature Law Requirements in Asia

E-signatures are valid and recognized under the governing electronic transactions laws within the Asia-Pacific.

For example, the Corporations Amendment (Meetings and Documents) Bill 2021 was recently passed, amending the Corporations Act 2001 in Australia to allow companies to legally execute, sign, and share documents electronically.

In Singapore, Malaysia, Vietnam, Philippines, Thailand, and Indonesia, electronic and digital signatures are as valid and enforceable as handwritten signatures.

There are various laws governing electronic and digital signatures within APAC depending on the country. As such, certain requirements must be met for the validity and admissibility of electronic and digital signatures.

Are Digital Signatures Secure?

A common question people may have is, "Can my digital signature be forged?"

back to top

Here's a simple answer: As long as your digital certificate is valid with your private key kept secure, your digital signature cannot be forged.

Digital signatures are equipped with many layers of security and authentication at the backend, as well as court-admissible proof of transaction. They rely on public and private keys, which ensures safety and are used to avoid forgery. Signing a document with a digital certificate gives the signer assurance that the document is valid and recognized by law.

Digital Signing Service

Digital Signing PDF

Electronic documents often come in PDF form. PDF documents can be digitally signed with audit trail, encryption, and other backed tools to ensure the authenticity of the document.

GlobalSign's Digital Signing Service

Nowadays, it is imperative to use digital signatures for documents and contracts as they are subject to rigorous compliance standards that must be met.

GlobalSign's Digital Signing Service (DSS) is the perfect tool for digital signing as it is instant, portable, legally binding, and backed by technology that ensures the signature is authentic.

GlobalSign's DSS is a cloud-based signing solution that can be integrated into the top signing platforms including GMO Sign, SigniFlow, Adobe Sign, DocuSign, iText, ILovePDF, HelloSign, and more.

It lets you accelerate approvals and agreements by eliminating bottlenecks and idle periods. Signing a document is as easy as a click of a button.

With faster signing processing time, what used to take weeks to sign can only take hours, or even minutes!

Clients from all over the world are utilizing GlobalSign's DSS for their digital signing needs, as GlobalSign is one of the most trusted Certificate Authorities worldwide.

Conclusion

In conclusion, with the right digital signing solution, electronic and digital signatures are full-proof and ***cannot be forged as long as the private key is kept secure****. For basic e-signatures, there is an audit trail that tracks when the document was signed, and where it was signed, depending on the privacy permission of the signee. With multiple layers of*

back to top

security and authentication criteria that must be met build for speed processes, electronic and digital signatures are more secure and convenient than traditional wet-ink signatures.

With GlobalSign's Digital Signing Service, you can be sure that your digital signatures meet even the most stringent legal standards. Expedite and secure your digital contracts and agreements.

For further enquiries, please contact GlobalSign APAC at sales-apac@globalsign.com

Article from our TCA 2022 Winner, Ensign InfoSecurity

AiSP April 2023 Newsletter - TCA 2022 Winner Feature

Ensign InfoSecurity, the largest pure-play end-to-end cybersecurity service provider in Asia Pacific, was recently awarded the "MNC Vendor" award at the annual Cybersecurity Awards ceremony. This recognition is a testament to the company's dedication and commitment to excellence in the cybersecurity industry.

Ensign's cyber competencies are built with the goal of solving every cybersecurity challenge that our clients may face. The company has contributed significantly to the cybersecurity ecosystem through its people and expertise, combined with its innovative R&D capabilities. Ensign goes beyond the expected by not only providing cybersecurity solutions to clients, but also nurturing future cybersecurity professionals and advocating equal opportunity and sustainability culture in the workplace.

Our mission at Ensign is to secure the cyberspace of enterprises, sectors, and nations through world-class expertise and innovative technologies. To achieve this, we empower our customers to protect their assets from cyber threats by providing them with the knowledge, expertise, and technologies to defend themselves effectively. Tammie Tham, Group CEO, Ensign InfoSecurity, said, "Ensign is proud to be recognised as a leader in this industry. We understand the importance of cybersecurity in today's digital age, and we are committed to helping our customers navigate the complex and constantly evolving cyber threat landscape."

Ensign invests heavily in research and development to spur innovation and progress, translating them into tangible benefits and outcomes for our clients. The company also constantly shares technical papers, advisories, and threat intel reports with its clients to give them a comprehensive insight into current cyber risks and mitigation measures. Additionally, Ensign plays an active role in nurturing future cybersecurity professionals

back to top

by investing in training and development programs for employees and supporting the education of the next generation of cybersecurity experts.

Furthermore, Ensign continues to execute its community engagement strategy and collaborate with partners to bring impactful programs that engage, mentor, and support youths, working adults, women, and neurodiverse individuals. The company places a strong emphasis on promoting equal opportunity and a sustainability culture in the workplace. By fostering an inclusive culture that values diversity, creativity, and teamwork, Ensign hopes to attract and retain the best talent in the industry. Tammie added, "We believe that investing in the development of our employees and the next generation of cybersecurity professionals is essential to building a stronger and more secure future for all. We are also committed to fostering an inclusive culture that values diversity, creativity and teamwork."

In conclusion, the accolade received by Ensign reflects the company's dedication and commitment to excellence, innovation and inclusivity which sets us apart as a leader in the cybersecurity industry.

back to top

Reflection from our SVRP 2022 Winner, Jerry Tan

I am ecstatic to have attained the highest level of recognition in the Student Volunteer Recognition Program! For me, this award represents the culmination of years of hard work, a deep commitment to cybersecurity, and an unwavering belief in the power of knowledge sharing. To be recognized for my efforts and to be acknowledged as a leader in this field is a true honour.

My journey into the world of cybersecurity began at a young age, sparked by a fascination with technology that has never faded. As a child, I was captivated by movies like The Matrix, which showcased the incredible reach and power of cutting-edge technologies. This fascination would lay the foundation for my lifelong commitment to protecting Singapore's digital landscape. From the very beginning, I was driven by a sense of purpose, to become a defender of our digital world, and to make a positive impact in the lives of those around me. My journey into cybersecurity has been driven by a passion for technology and a desire to make a difference.

As I navigated my path in cybersecurity, I was fortunate enough to cross paths with a mentor who would change the course of my journey. This colleague, a seasoned expert in red teaming, took me under their wing, answering all my questions with patience and imparting their wealth of knowledge and experience.

It was through this mentorship that I came to fully understand the importance of knowledge sharing. My mentor was unencumbered by any limitations or reservations, and was willing to impart their expertise to me without hesitation. Their willingness to share their knowledge inspired me, and I came to believe that the more knowledge I gained, the more I could empower others.

back to top

This belief has guided me throughout my journey in cybersecurity, and has driven me to continue to pass on what I have learned. I have dedicated myself to sharing my expertise and insights with others, and have worked tirelessly to help build a brighter future for all. I believe that knowledge is power, and that it should be shared with all. By empowering others with the knowledge and skills necessary to defend our digital world, we can create a stronger, more resilient cybersecurity community that is better equipped to face the challenges of the future.

As a young cybersecurity enthusiast, I started volunteering when I was invited to join the community of Div0-N0H4TS as a Public Relations Lead. This opportunity allowed me to not only further my understanding of the industry, but also to share my knowledge with the wider community through various platforms, including the community's social media channels.

Through my role at Div0-N0H4TS, I have had the privilege of playing a key role in organizing and executing numerous events that align with my belief in knowledge is power and should be shared with all. These events have included the highly-anticipated STANDCON, and a state-of-the-art Capture the Flag competition, Cyber League.

STANDCON, a highly anticipated cybersecurity student conference that brings together experts from around the world to share their insights on the latest trends and developments in the field with our participants. With cutting-edge discussions on niche and upcoming domains within the cybersecurity realm, STANDCON was an incredible opportunity to ignite passion and inspiration in young individuals looking to make a positive impact in the world.

Cyber League, a state-of-the-art Capture the Flag competition that aimed to upskill Singapore's cybersecurity skillset and identify the strengths and weaknesses of the participants. This unique competition was designed to provide a mastery framework that allowed individuals to measure their progress and growth in the field. By participating in the Cyber League, individuals were given a chance to demonstrate their skills and receive valuable feedback, allowing them to continuously improve and become stronger defenders of Singapore's digital landscape.

My journey in the field of cybersecurity has been one of self-discovery, purpose, and impact. I firmly believe that knowledge is the greatest source of power and it is our obligation to share it with all. My work as a volunteer with Div0-N0H4TS, where I was honoured to serve as a Public Relations Lead, has allowed me to live this belief and make a difference in the lives of others. The recognition I received as a result of my tireless efforts, in the form of the highest tier recognition in the Student Volunteer Recognition Programme, is a true testament to my belief. I am proud to have been a part of this movement, and I am determined to continue blazing a trail for others to follow.

back to top

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

Become experts at building applications with both speed and security with the **EC-Council Certified DevSecOps Engineer (E|CDE) program**.
This lab-based program teaches candidates to excel with practical knowledge.

Learn to address cloud security issues and fix them directly at the source, identify security vulnerabilities at different stages of the development cycle and become proficient in leveraging innovative tools in both on-premises and cloud-native environments.

Build your #DevSecOps career today!

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®)

Sign up for Qualified Information Security Professional (QISP) Exam before 31 March!

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 March 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

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

back to top

- 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
- Securing the Network

back to top

- 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

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:

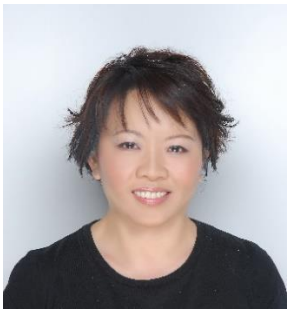
- promoting the integrity, status and interests of Information Security Professionals in Singapore.
- enhancing technical competency and management expertise in cybersecurity.
- bolstering the development, increase and spread of information security knowledge and its related subjects.

AiSP Secretariat Team

Vincent Toh
Associate Director

Elle Ng
Senior Executive

Karen Ong
Executive



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.

back to top

