AiSP

NEWSLETTER

May 2022

NEWS & UPDATE

New Partners

AiSP would like to welcome Elastic and Mimecast as our new Corporate Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

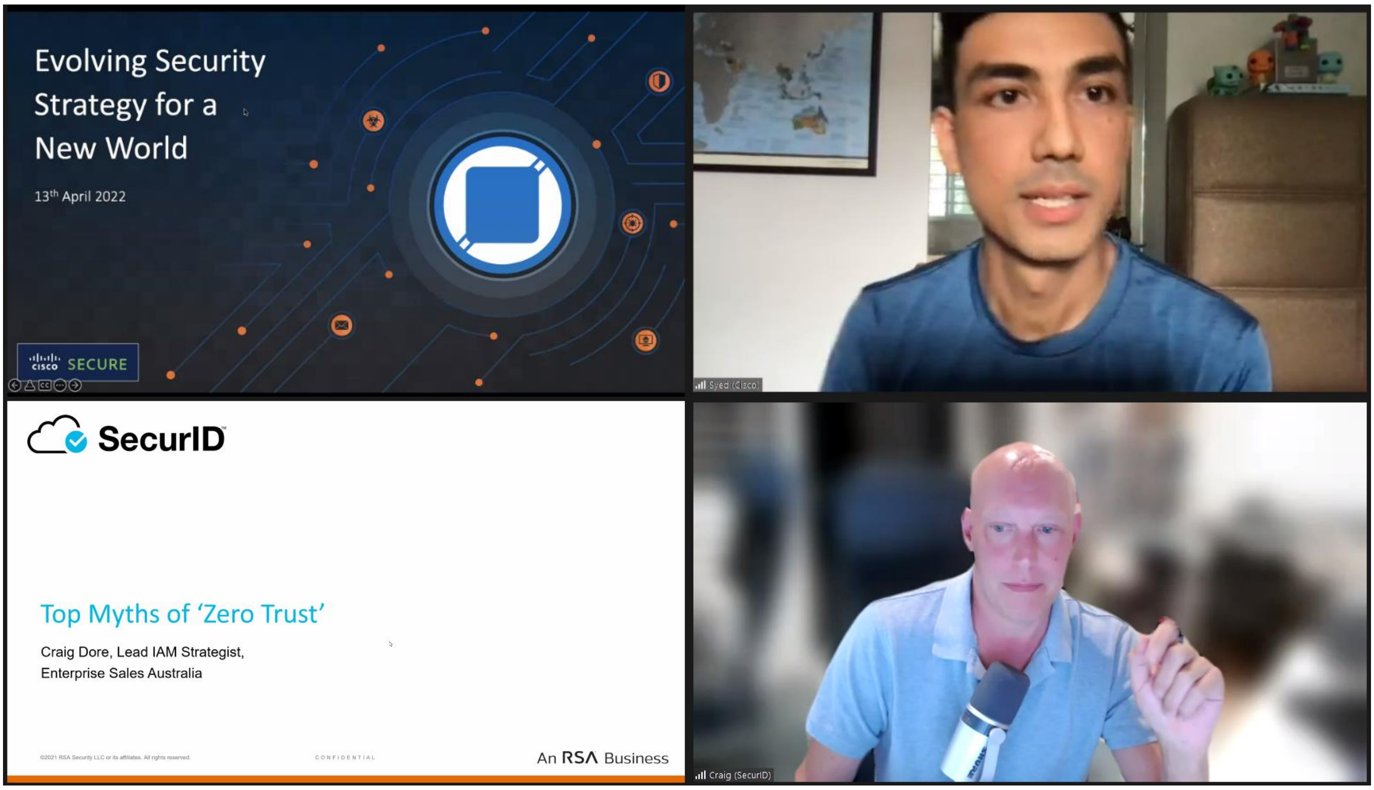
Continued Collaboration

AiSP would like to thank DBS and Mircofocus for their continued support in developing the cybersecurity landscape:

Knowledge Series Events

Cloud Security on 13 Apr 22

As part of Digital for Life movement, knowledge series focusing on Cloud Security was held on 13 April. Our Corporate Partners, Cisco and SecurID were invited to share insights with our members. We would like to thank Syed Abdul Rahman Alsagoff and Craig Dore for sharing insights on Cloud Security.



Evolving Security Strategy for a New World

13th April 2022

SecurID

Top Myths of 'Zero Trust'

Craig Dore, Lead IAM Strategist,
Enterprise Sales Australia

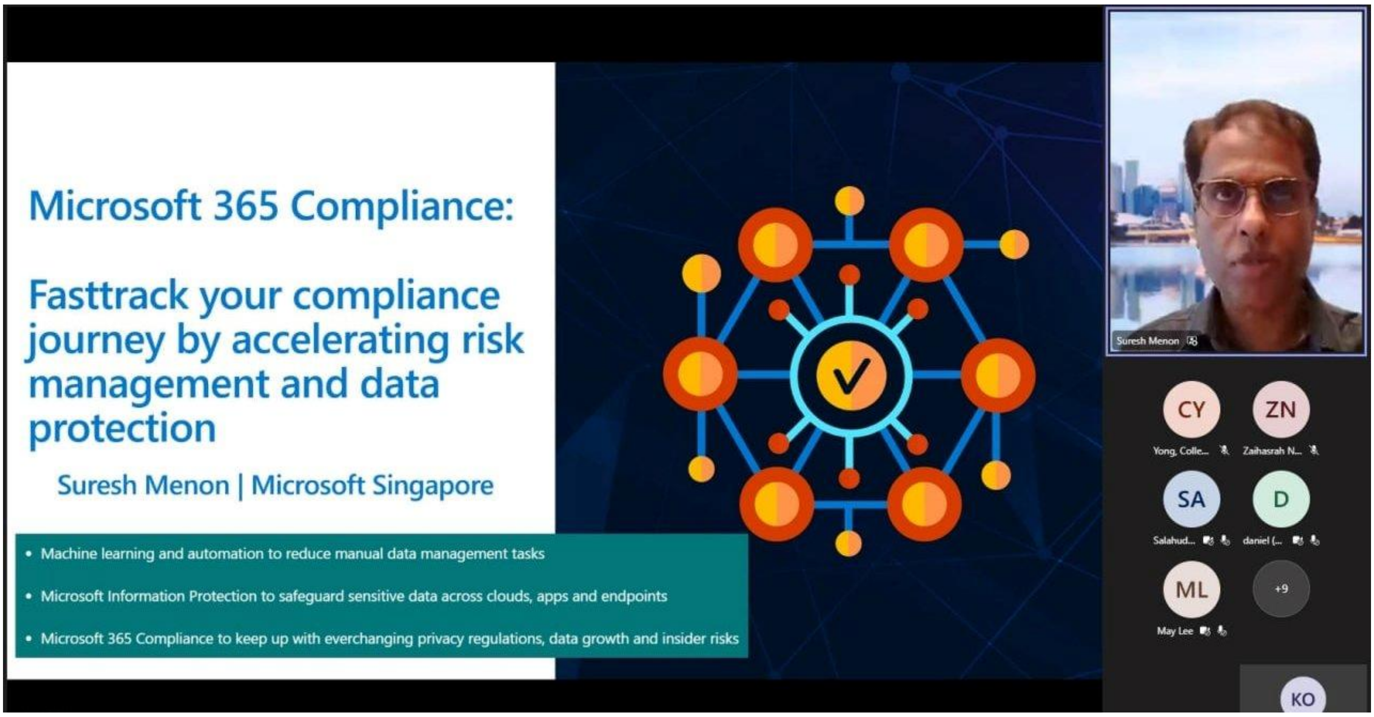
An RSA Business

back to top

IS Governance on 28 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 28 April, Mr Suresh Menon from Microsoft shared on the Information Security Governance and on Fasttrack your Compliance Journey. AiSP would like to thank Suresh for sharing the insights with our participants and Microsoft for supporting this webinar.



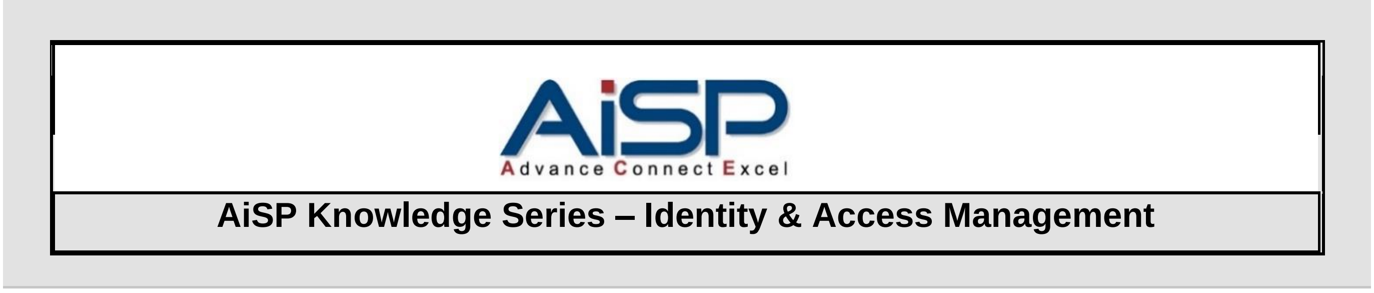
Microsoft 365 Compliance:

Fasttrack your compliance journey by accelerating risk management and data protection

Suresh Menon | Microsoft Singapore

- Machine learning and automation to reduce manual data management tasks
- Microsoft Information Protection to safeguard sensitive data across clouds, apps and endpoints
- Microsoft 365 Compliance to keep up with everchanging privacy regulations, data growth and insider risks

Identity & Access Management on 24 May 22



AiSP Advance Connect Excel

AiSP Knowledge Series – Identity & Access Management

back to top

In this Knowledge Series, we are excited to have Microsoft to share with us insights on identity and access management. 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.

Five steps to securing your identity infrastructure
Speaker: Yasser Ahmed, Sr. Technical Specialist, Cloud-Security, Microsoft Singapore

Many consider identity to be the primary perimeter for security. This is a shift from the traditional focus on network security. Network perimeters keep getting more porous, and that perimeter defence can’t be as effective as it was before the explosion of BYOD devices and cloud applications.

During this session we will talk about the 5 steps in securing this critical aspect of Identity security:

- Strengthen your credentials
- Reduce your attack surface area
- Automate threat response
- Utilize cloud intelligence
- Enable end-user self-service

Finally manage a secure score for identity to constantly monitor and improve it.

Date: 24th May 2022 (Tues)
Time: 3PM – 4.30PM
Venue: MS Teams
Registration: https://forms.office.com/r/TrcZ3FkFJF

back to top

About our Knowledge Series

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 2022 are as follows (*may be subjected to changes*),

1. Identity & Access Management, 24 May 22

Please let us know if your organisation is keen to be our sponsoring speakers in 2022! AiSP members who registered for the event, can playback the recorded event via their member profile in Glue Up. If you did not sign up for the event, please email secretariat@aisp.sg for assistance. Please refer to our scheduled 2022 webinars in our event calendar.

Cybersecurity Awareness & Advisory Programme (CAAP)

Huawei Roundtable on 1 April

In support of the Cyber Essentials mark (recently launched by Cyber Security Agency of Singapore - CSA), AiSP collaborated with Huawei Singapore to organise our first session to share insights on the mark. We would like to thank Ms Veronica Tan, Mr Johnny Kho, Mr Yang Liu and Mr John Yong for participating in the panel discussion on "SME: Are You Cyber-Safe?" and Mr Dennis Chan for moderating the discussion.

back to top

Upcoming CAAP Event

AiSP hope to elevate Cyber Security Awareness as integral part of SME Business Owner Fundamentals and Establish a Self-Sustainable Support Ecosystem programme with active participation from Agencies, Business Associations, Security Communities and Vendors.

AiSP x Microsoft CAAP Roundtable on 5 May

AiSP Advance Connect Excel

AiSP x Microsoft CAAP Roundtable

AiSP x Microsoft
CAAP Roundtable
5 May | NTUC, 1 Marina Boulevard, #08-01, Singapore 018989 | 3PM - 5PM

Veronica Tan
Director of Safer Cyberspace
Cyber Security Agency of Singapore

Richard Koh
Chief Technology Officer
Microsoft Singapore

Alison Heng
Sales Lead of Security Solutions
Microsoft Singapore

Organised By: AiSP Advance Connect Excel
Supported By: CSA Singapore, Microsoft Security
SMECYBERSAFE.SG
AiSP | CAAP

In recent years, we've witnessed an exponential increase in cyberattacks that have disrupted organizations across the world. From large-scale data breaches to smaller security incidents, every organization is equally vulnerable in the face of rapidly evolving cyber threats.

While digitalisation offers tremendous benefits to enterprises, they are also more exposed to digital risks that could cause disruption to their business. The recent spate of supply chain cyber-attacks has elevated the need for enterprises to strengthen their cybersecurity and demonstrate their

<u>AGENDA</u>

1500: **Welcome Address & Sharing on AiSP CAAP Programme**
Tony Low, CAAP EXCO Lead, AiSP

1515: **Staying cyber safe with Cyber Trust and Cyber Essentials**
Veronica Tan, Director of Safer Cyberspace Division,

back to top

cybersecurity posture. Find out how enterprises can leverage CSA's cybersecurity certification scheme as a competitive advantage for their business.

In this session, security experts and advocates at Microsoft will discuss:

- The state of cybercrime: from emerging threats to the growing market for cybercrime services
- The vulnerabilities found in IoT, operational technology and supply chain ecosystems
- Common methods that are used by cybercriminals to target the hybrid workforce
- How Microsoft Detection and Response Team (DART) is helping organizations become cyber-resilient
- Why implementing a Zero Trust strategy is key to improving your organization's security posture

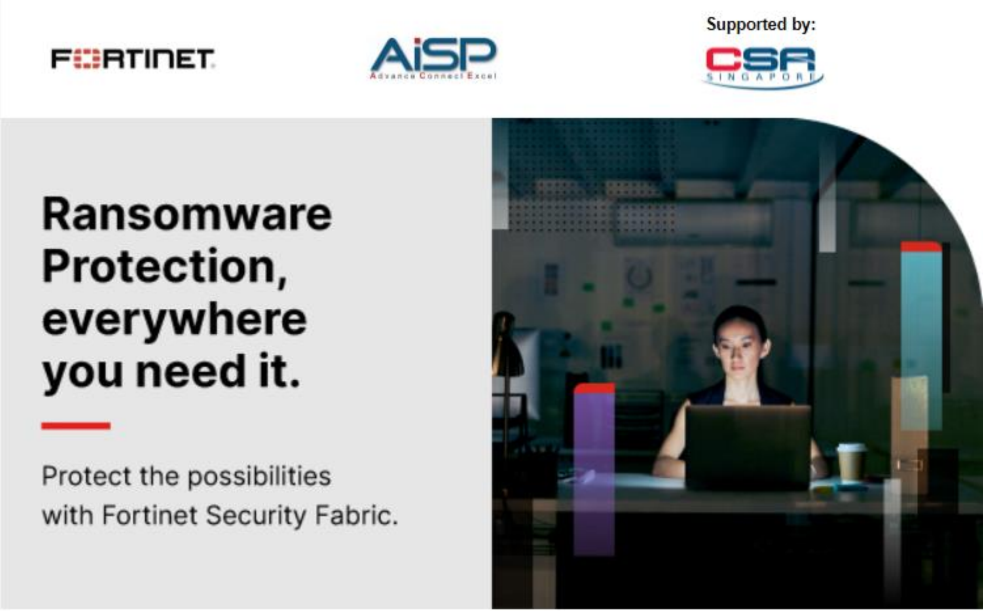
	Cyber Security Agency of Singapore
1530:	**Formulating a proactive cyber defense** Richard Koh, CTO, Microsoft Singapore and Alison Heng, Sales Lead of Security Solutions, Microsoft Singapore
1615:	Q&A
1630:	Tea break
1700:	End

Date: 5th May 2022 (Thursday)
Time: 3PM – 5PM
Venue: NTUC, 1 Marina Boulevard, #08-01, Singapore 018989
Registration: https://forms.office.com/r/KBjhiNghA2

back to top

Anti-Ransomware Day 2022 on 12 May

On this Anti-Ransomware Day, it is a timely reminder for organisations to review their existing cybersecurity architecture to mitigate against modern day threat attacks. As an advocate partner with Cyber Security Agency of Singapore (CSA) SG Cybersafe Partnership Programme, Fortinet together with our industry partners will share more about the ransomware attack trends and the importance of practicing good cyber hygiene to strengthen your cybersecurity posture.


FORTINET
AiSP Advance Connect Excel
Supported by:
CSA SINGAPORE
Ransomware Protection, everywhere you need it.
Protect the possibilities with Fortinet Security Fabric.

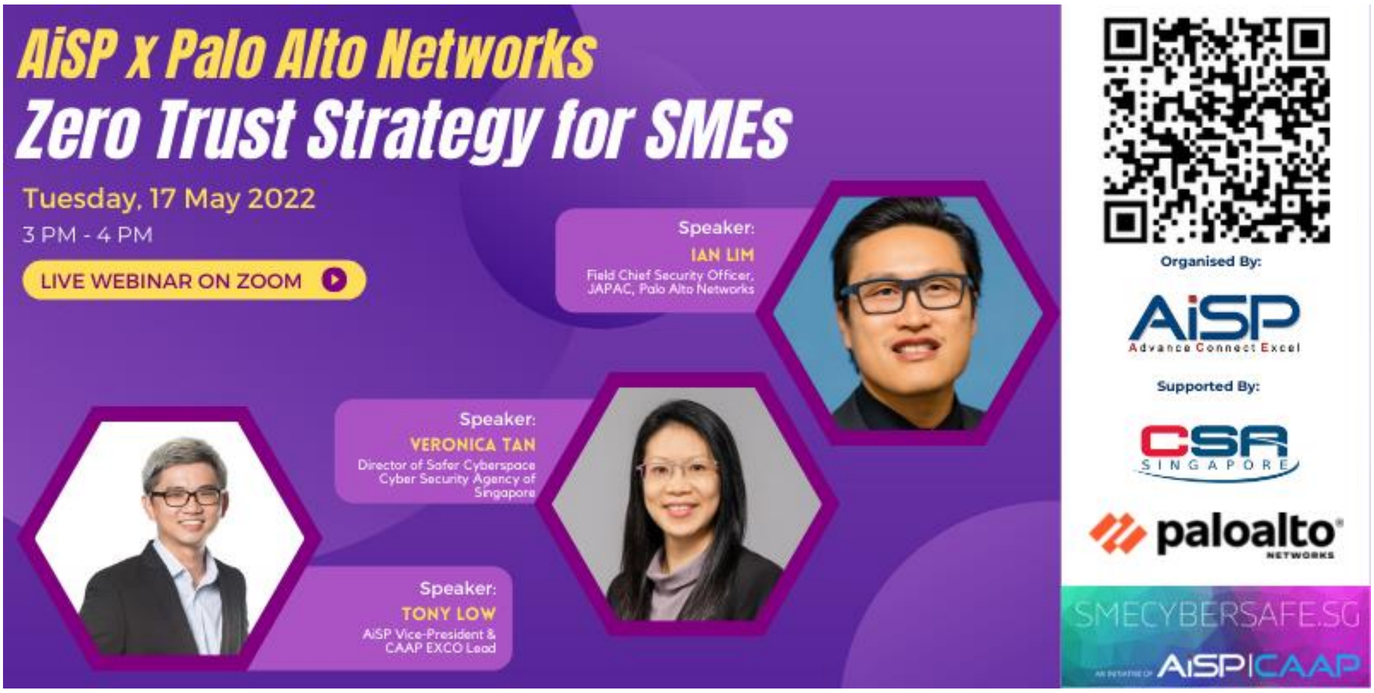
Click here to register.

back to top

AiSP x Palo Alto Networks - Cyber Safe Trustmark Awareness on 17 May

While digitalisation offers tremendous benefits to enterprises, they are also more exposed to digital risks that could cause disruption to their business. The recent spate of supply chain cyber-attacks has elevated the need for enterprises to strengthen their cybersecurity and demonstrate their cybersecurity posture. Find out how enterprises can leverage CSA's cybersecurity certification scheme as a competitive advantage for their business.

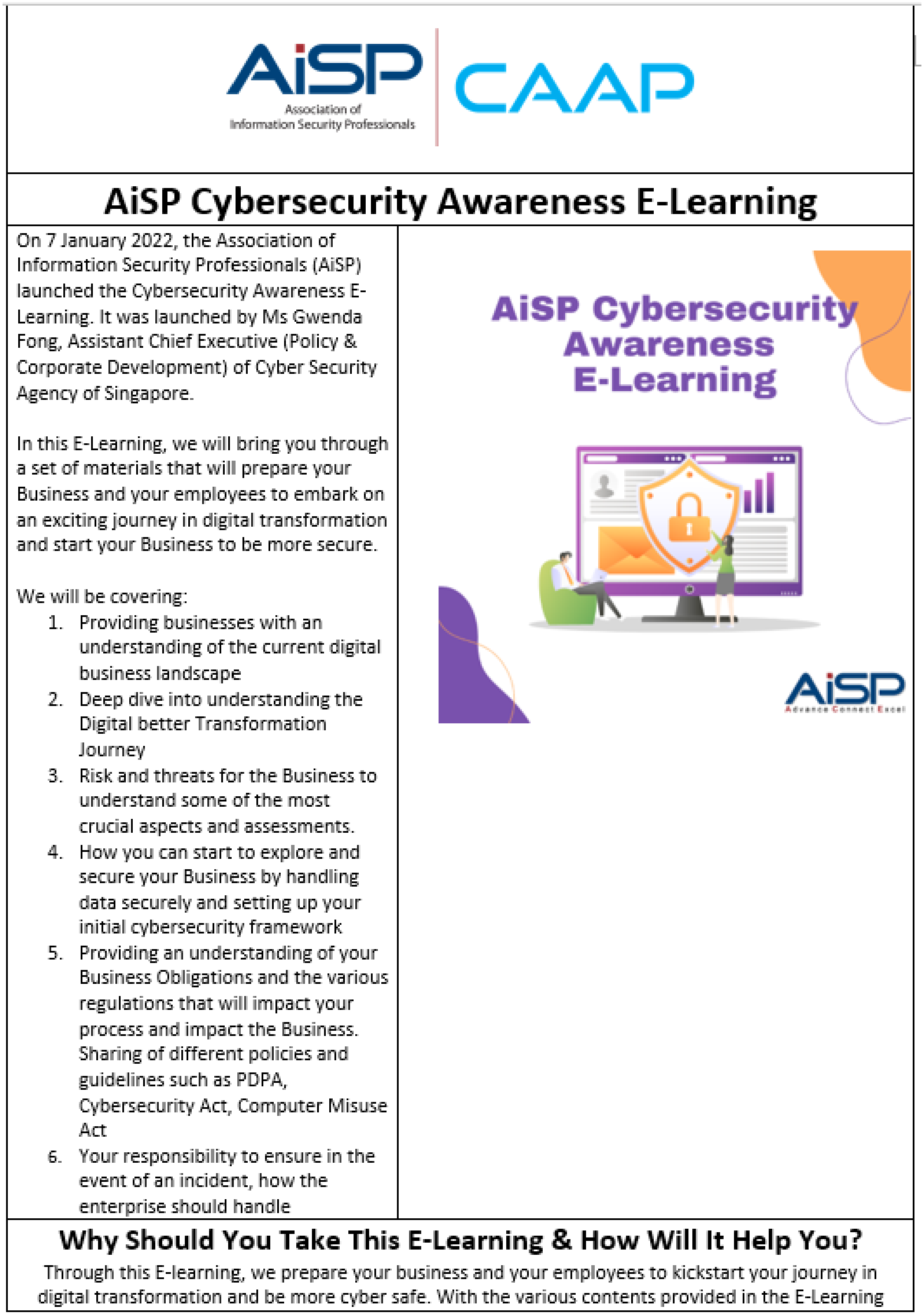
As an Advocate partner with Cyber Security Agency of Singapore (CSA) in their SG Cybersafe Partnership Program, Palo Alto Networks will also share how SMEs can build a new cybersecurity paradigm to defend against ever-evolving attacks and secure digital transformation initiatives. Register here today!


AiSP x Palo Alto Networks
Zero Trust Strategy for SMEs
Tuesday, 17 May 2022
3 PM - 4 PM
LIVE WEBINAR ON ZOOM
Speaker:
IAN LIM
Field Chief Security Officer, JAPAC, Palo Alto Networks
Speaker:
VERONICA TAN
Director of Safer Cyberspace Cyber Security Agency of Singapore
Speaker:
TONY LOW
AiSP Vice-President & CAAP EXCO Lead
Organised By:
AiSP
Advance Connect Excel
Supported By:
CSA SINGAPORE
paloalto NETWORKS
SMECYBERSAFE.SG
AiSP|CAAP

Click here to register.

back to top

AiSP Cybersecurity Awareness E-Learning



AiSP Association of Information Security Professionals | CAAP

AiSP Cybersecurity Awareness E-Learning

On 7 January 2022, the Association of Information Security Professionals (AiSP) launched the Cybersecurity Awareness E-Learning. It was launched by Ms Gwenda Fong, Assistant Chief Executive (Policy & Corporate Development) of Cyber Security Agency of Singapore.

In this E-Learning, we will bring you through a set of materials that will prepare your Business and your employees to embark on an exciting journey in digital transformation and start your Business to be more secure.

We will be covering:

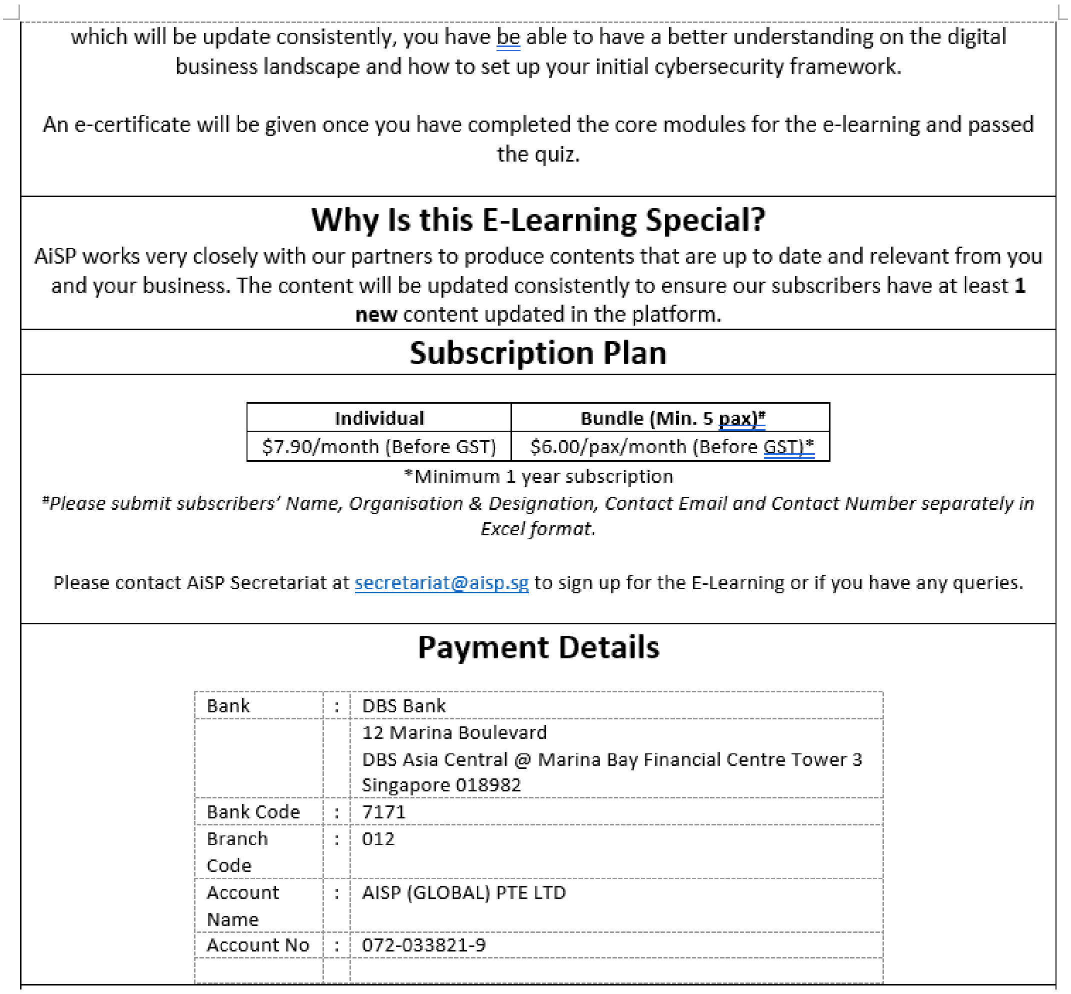
1. Providing businesses with an understanding of the current digital business landscape
2. Deep dive into understanding the Digital better Transformation Journey
3. Risk and threats for the Business to understand some of the most crucial aspects and assessments.
4. How you can start to explore and secure your Business by handling data securely and setting up your initial cybersecurity framework
5. Providing an understanding of your Business Obligations and the various regulations that will impact your process and impact the Business. Sharing of different policies and guidelines such as PDPA, Cybersecurity Act, Computer Misuse Act
6. Your responsibility to ensure in the event of an incident, how the enterprise should handle

AiSP Cybersecurity Awareness E-Learning
AiSP Advance Connect Excel

Why Should You Take This E-Learning & How Will It Help You?

Through this E-learning, we prepare your business and your employees to kickstart your journey in digital transformation and be more cyber safe. With the various contents provided in the E-Learning

back to top



which will be update consistently, you have be able to have a better understanding on the digital business landscape and how to set up your initial cybersecurity framework.

An e-certificate will be given once you have completed the core modules for the e-learning and passed the quiz.

Why Is this E-Learning Special?

AiSP works very closely with our partners to produce contents that are up to date and relevant from you and your business. The content will be updated consistently to ensure our subscribers have at least **1 new** content updated in the platform.

Subscription Plan

Individual	**Bundle (Min. 5 pax)#**
$7.90/month (Before GST)	$6.00/pax/month (Before GST)*

*Minimum 1 year subscription

#Please submit subscribers' Name, Organisation & Designation, Contact Email and Contact Number separately in Excel format.

Please contact AiSP Secretariat at secretariat@aisp.sg to sign up for the E-Learning or if you have any queries.

Payment Details

Bank	:	DBS Bank
		12 Marina Boulevard DBS Asia Central @ Marina Bay Financial Centre Tower 3 Singapore 018982
Bank Code	:	7171
Branch Code	:	012
Account Name	:	AISP (GLOBAL) PTE LTD
Account No	:	072-033821-9

SME Cybersafe provides

Enhanced Security Awareness & Training

Cohesive Security Knowledge Resources

Security Solutions & Services Support

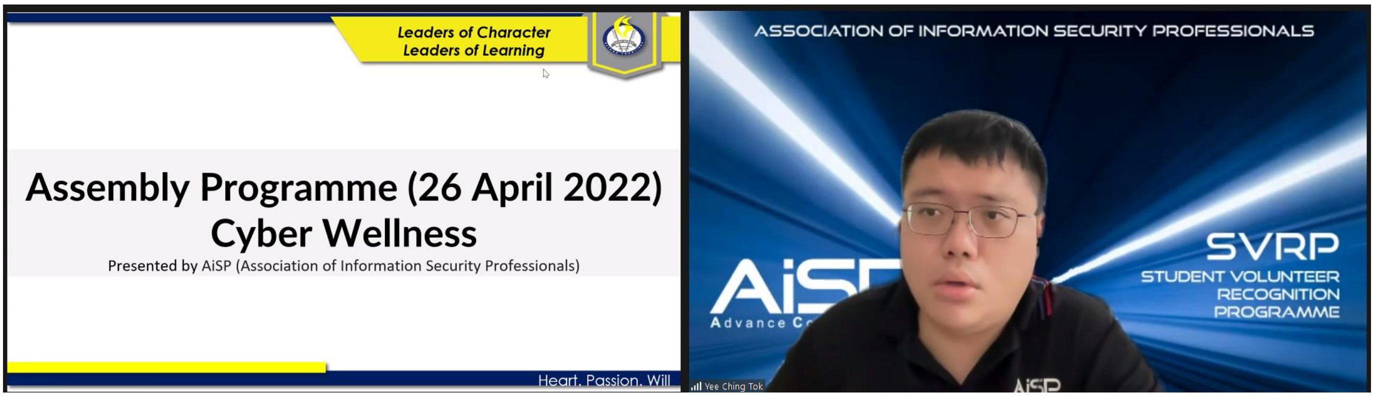
Click here to find out more about the E-Learning.

back to top

Student Volunteer Recognition Programme (SVRP)

School Talk with Kent Ridge Secondary School
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 26 April, AiSP EXCO Member, Mr Tok Yee Ching did a sharing to about 1000 students in Kent Ridge Secondary on phishing and scams. It was an insightful sharing for the students as they learned more about the phishing and scams.



Leaders of Character
Leaders of Learning

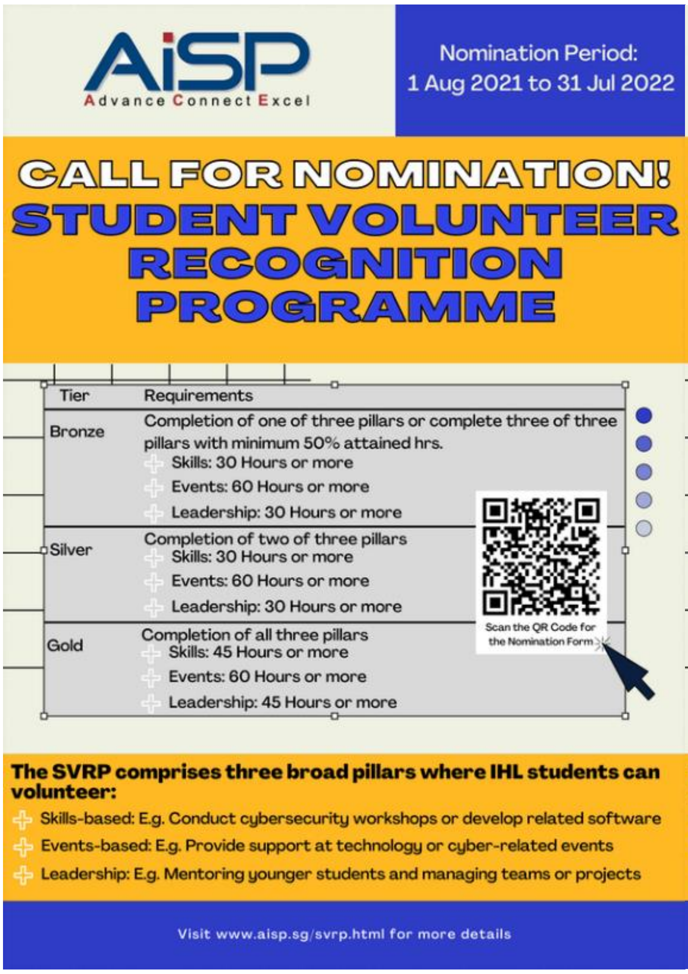
Assembly Programme (26 April 2022)
Cyber Wellness
Presented by AiSP (Association of Information Security Professionals)

Heart. Passion. Will

ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
SVRP
STUDENT VOLUNTEER RECOGNITION PROGRAMME
Yee Ching Tok

back to top

SVRP Nomination has officially concluded, and results have been released on our website here. Our student volunteer drive is ongoing till Dec 2022 for those who are interested to volunteer but not sure where to start. Please click here to apply today. Nomination period is from 1 Aug 2021 to 31 Jul 2022.



AiSP Advance Connect Excel

Nomination Period:
1 Aug 2021 to 31 Jul 2022

CALL FOR NOMINATION!
STUDENT VOLUNTEER RECOGNITION PROGRAMME

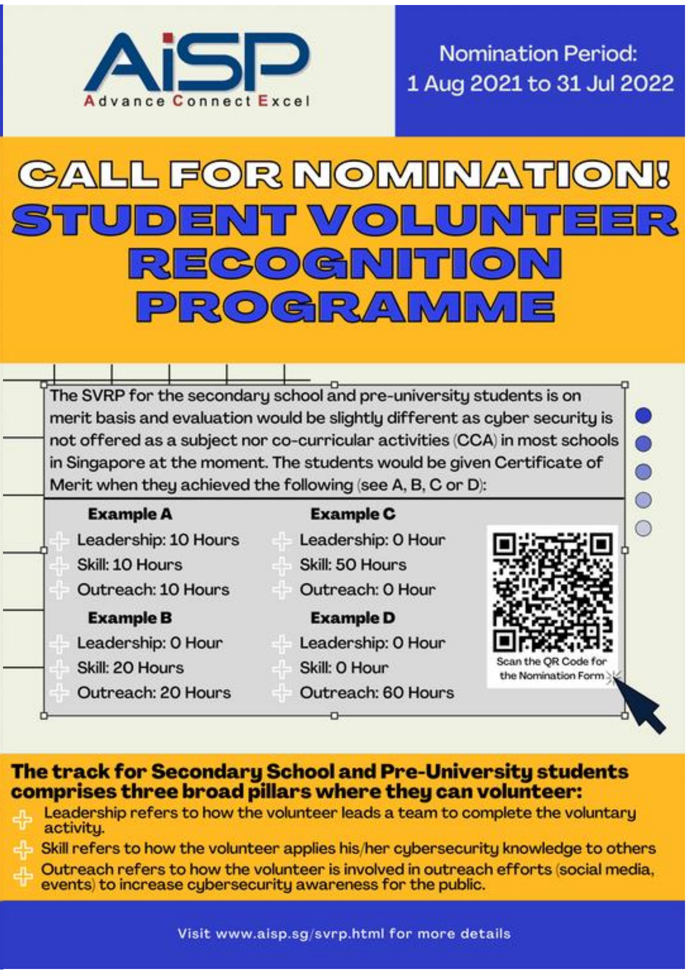
Tier	Requirements
Bronze	Completion of one of three pillars or complete three of three pillars with minimum 50% attained hrs. Skills: 30 Hours or more Events: 60 Hours or more Leadership: 30 Hours or more
Silver	Completion of two of three pillars Skills: 30 Hours or more Events: 60 Hours or more Leadership: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



AiSP Advance Connect Excel

Nomination Period:
1 Aug 2021 to 31 Jul 2022

CALL FOR NOMINATION!
STUDENT VOLUNTEER RECOGNITION PROGRAMME

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

Example A	Example C
Leadership: 10 Hours Skill: 10 Hours Outreach: 10 Hours	Leadership: 0 Hour Skill: 50 Hours Outreach: 0 Hour
Example B	**Example D**
Leadership: 0 Hour Skill: 20 Hours Outreach: 20 Hours	Leadership: 0 Hour Skill: 0 Hour Outreach: 60 Hours

Scan the QR Code for the Nomination Form

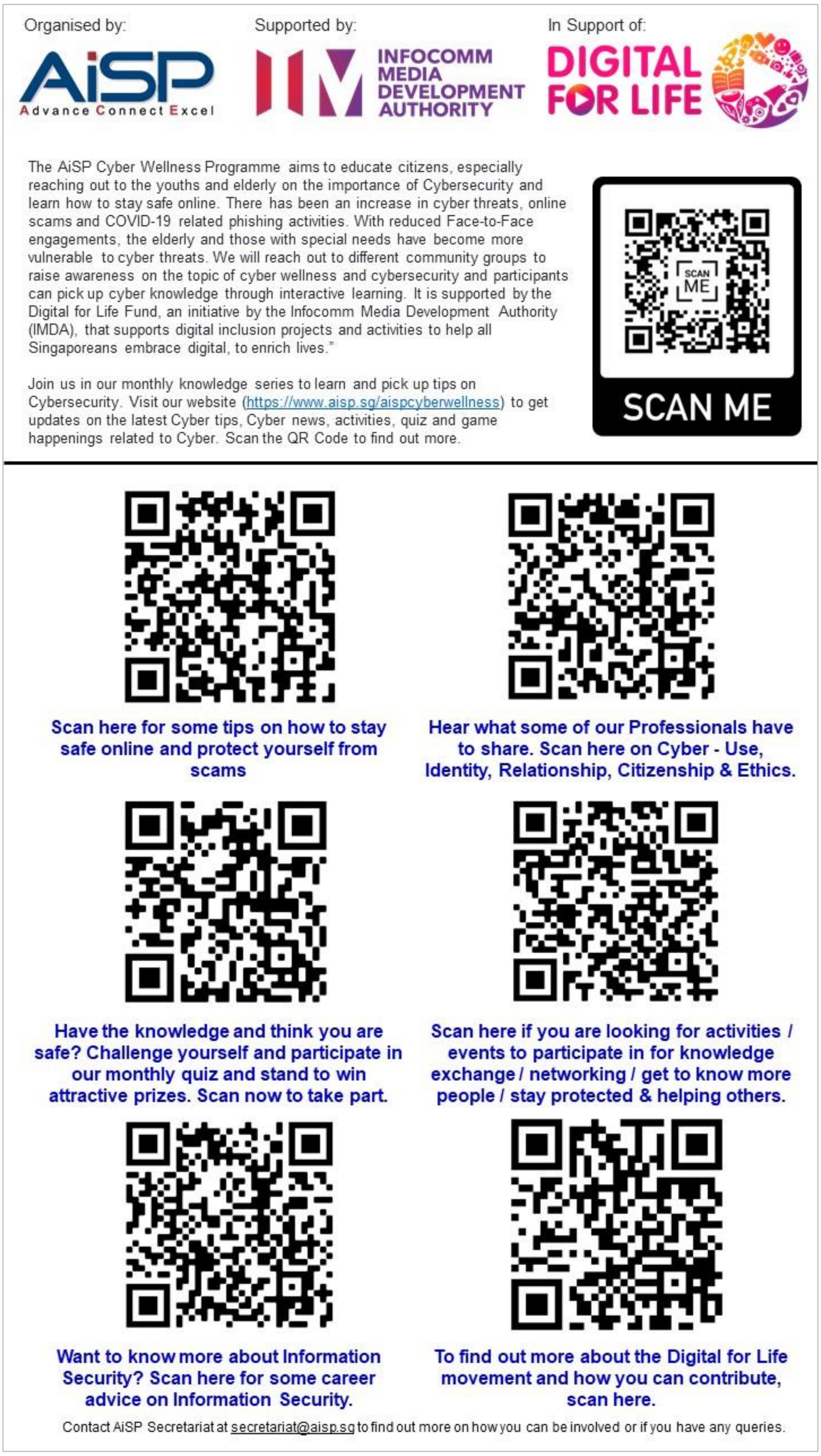
The track for Secondary School and Pre-University students comprises three broad pillars where they can volunteer:

- 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



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 ME

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 some career advice on Information Security.

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

https://www.aisp.sg/ladies_about.html
NETWORKING | MENTORING | SPECIAL PROGRAMMES
LADIES IN CYBER
AiSP
'Ladies Talk Cyber' Series
May 2022 Edition
Interview of Ms Lim Ee Lin

Ladies Talk Cyber Series

For the Twelfth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Lim Ee Lin who is one of the leaders in the Cybersecurity Programme Centre (CSPC) of the Cyber Security Agency (CSA) of Singapore. Her role is to lead the Government and People & Enterprise clusters, responsible for securing government networks and systems and implementing programmes to create a safer, secure and resilient cyberspace.

How to be successful in cybersecurity field

In celebration of SG Women year, AiSP's secretariat decided it was timely to launch a series of interviews of female leaders across industries who fulfil high impact roles, and learn about their journeys, experiences and insights. The initiative aims to shed some light on what it takes to make it in this field. The interviews can be source of invaluable career insights as well as opportunities for those in the field to get a deeper understanding of the industry, and how its leaders are innovating to disrupt the cyber landscape.

Introducing women with a deep interest in cybersecurity

Ee Lin is one of the leaders in the Cybersecurity Programme Centre (CSPC) of the Cyber Security Agency (CSA) of Singapore. My role is to lead the Government and People & Enterprise clusters, responsible for securing government networks and systems and implementing programmes to create a safer, secure and resilient cyberspace.

Please click here to view the full details of the interview.

back to top

AiSP Advance Connect Excel | LADIES IN CYBER

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

AiSP Advance Connect Excel SIG CLOUD SECURITY

AiSP Advance Connect Excel SIG CYBER THREAT INTELLIGENCE

AiSP Advance Connect Excel SIG DATA AND PRIVACY

AiSP Advance Connect Excel SIG INTERNET OF THINGS

AiSP x Cycognito CTI SIG Event on 29 April

On 29 April, AiSP held our second CTI SIG event. AiSP would like to thank CyCognito for sharing insights on Attack Surface Visibility - The Foundation of Effective Cybersecurity. It was a fruitful and insightful sharing for the participants. AiSP would like to thank all participants who joined us physically at Lifelong Learning Institute for the event.

Special thanks to Mr Kunal Sehgal, Mr Sukhdev Singh, Mr Kok Kiat Han & Mr Lawrence Wong for joining the panel discussion.

back to top

AiSP Cyber Threat Intelligence SIG Event
29 April | 10AM - 12PM | Hybrid
Lawrence Loh
Kok Kiat Han
Sukhdev Singh
Kunal Sehgal

CYCOGNITO
Attack Surface Visibility – The Foundation of Effective Cybersecurity
Lawrence Loh, Channel Director APJ

back to top

The Cybersecurity Awards

THE CYBERSECURITY 2022 Awards

TCA 2022 Call for Nominations is now open!

AiSP Advance Connect Excel

THE CYBERSECURITY 2022 Awards

Nomination open until 17 June 2022

Nominate your Cybersecurity Heroes now!!

PROFESSIONALS

- Hall of Fame
- Leader
- Professional

ENTERPRISES

- MNC (Vendor)
- MNC (End-User)
- SME (Vendor)
- SME (End-User)

STUDENTS

For more information, Visit
www.thecybersecurityawards.sg

Visit www.thecybersecurityawards.sg for more information.

The Cybersecurity Awards has three (3) award categories: Professionals, Enterprises and Students -a total of eight (8) awards:

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)

back to top

Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors! Limited sponsorship packages are available.

THE CYBERSECURITY Awards 2022
Organised by
AiSP Advance Connect Excel
Supported by
CSA SINGAPORE
Supporting Associations
CSCIS
cloud security alliance CSA SINGAPORE CHAPTER
HTCIA SINGAPORE CHAPTER
ISACA Singapore Chapter
OFFICIAL (ISC)² CHAPTER SINGAPORE
SINGAPORE SCS COMPUTER SOCIETY
SGTECH
THE LAW SOCIETY OF SINGAPORE
Community Partner
image engine
Supporting Organisation
SFA SINGAPORE FINTECH ASSOCIATION
Platinum Sponsors
BeyondTrust
CISCO
ENSIGN INFOSECURITY
HUAWEI
ST Engineering
TREND MICRO
Gold Sponsors
CyberProof A UST Global Company
CSIT Centre for Strategic Infocomm Technologies
DBS
kaspersky
Singtel
wizlynx group
Silver Sponsors
PCS SECURITY
RSA
SIT SINGAPORE INSTITUTE OF TECHNOLOGY
THALES Building a future we can all trust
wsg Workforce Singapore

back to top

IOT Innovation Day

The AiSP IoT Innovation Day & Exhibition is the can't-miss event of the year as professionals come together for a day of sharing on Smart City, Driverless Transportation and Health Technology Ecosystem connect for the education, innovation, and collaboration they need to reimagine as part of innovation and smart nation for everyone, everywhere. This event which will be held on 11 May 2022 is targeting at professionals from CIOs and senior executives to providers and payers to IT consultants and entrepreneurs to join in and attend this influential to get the information and solutions they need to reimagine on a Smart City for everyone, everywhere.

Sponsors:
CISCO, ExtraHop, Elastic, SecureCraft, and Vectra AI

AiSP IoT Innovation Day
11 May 2022 | 10AM - 3.30PM
Suntec Convention Centre
Reimagining a Smart City for everyone, everywhere
Organised by:
AiSP
Association of Information Security Professionals
Register Now!

Click here to register

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

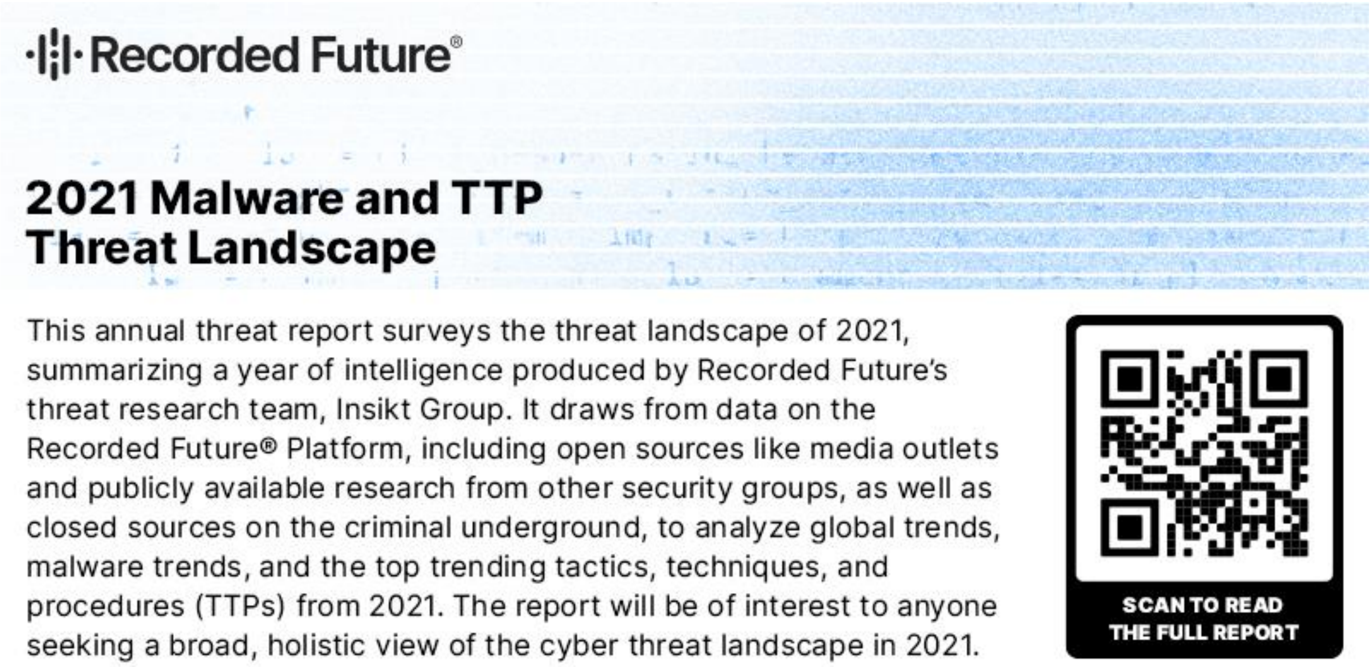
Date	Event	Organiser
5 May	World Password Day - AiSP x Microsoft CAAP Roundtable	AiSP & Partner
10 – 13 May	Blackhat Asia	Partner
11 May	IoT Innovation Day	AiSP
12 May	CAAP with Fortinet	AiSP & Partner
17 May	CAAP Roundtable with Paolo Alto Webinar	AiSP & Partner
23 May	DFL Webinar with Pathlight	AiSP & Partner
24 May	Knowledge Series With Microsoft	AiSP & Partner
25 May	Learning Journey to Singtel for RP	AiSP & Partner
26 May	Learning Journey to Acronis for Pathlight	AiSP & Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Cyber Threat Intelligence SIG



Recorded Future®

2021 Malware and TTP Threat Landscape

This annual threat report surveys the threat landscape of 2021, summarizing a year of intelligence produced by Recorded Future's threat research team, Insikt Group. It draws from data on the Recorded Future® Platform, including open sources like media outlets and publicly available research from other security groups, as well as closed sources on the criminal underground, to analyze global trends, malware trends, and the top trending tactics, techniques, and procedures (TTPs) from 2021. The report will be of interest to anyone seeking a broad, holistic view of the cyber threat landscape in 2021.

SCAN TO READ THE FULL REPORT

Article from our CPP Partner, Securecraft

A bridge to Zero Trust

blog.cloudflare.com/bridge-to-zero-trust

March 18, 2022

03/18/2022

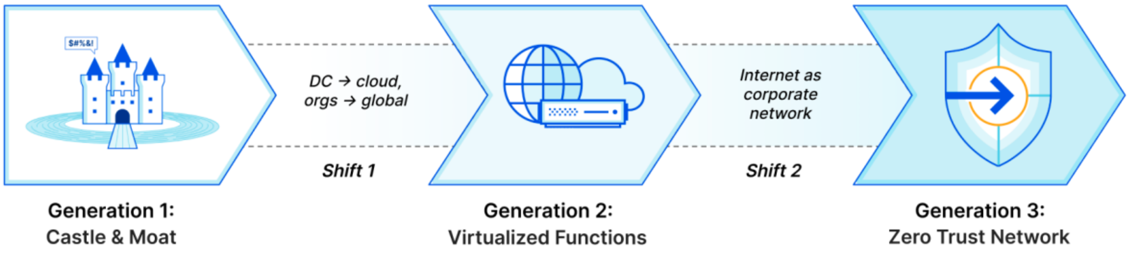
SecureCraft is a distributor of Cloudflare since 2017 and has definitely seen organisations shift **towards a more comprehensive IT security model that allows organizations to restrict access controls to networks, applications, and environment without sacrificing performance and user experience.**

Zero Trust approach simply means trust no one.

Cloudflare One enables customers to build their corporate networks on a faster, more secure Internet by connecting any source or destination and configuring routing, security, and performance policies from a single control plane. Today, we're excited to announce another piece of the puzzle to help organizations on their journey from traditional network architecture to Zero Trust: the ability to route traffic from user devices with our lightweight roaming agent (WARP) installed to any network connected with our Magic IPlayer tunnels (Anycast GRE, IPsec, or CNI). From there, users can upgrade to Zero Trust over time, providing an easy path from traditional castle and moat to next-generation architecture.

The future of corporate networks

Customers we talk to describe three distinct phases of architecture for their corporate networks that mirror the shifts we've seen with storage and compute, just with a 10 to 20 year delay. Traditional networks ("Generation 1") existed within the walls of a datacenter or headquarters, with business applications hosted on company-owned servers and access granted via private LAN or WAN through perimeter security appliances. As applications shifted to the cloud and users left the office, companies have adopted "Generation 2" technologies like SD-WAN and virtualized appliances to handle increasingly fragmented and Internet-dependent traffic. What they're left with now is a frustrating patchwork of old and new technologies, gaps in visibility and security, and headaches for overworked IT and networking teams.
We think there's a better future to look forward to:the architecture Gartner describes as SASE, where security and network functions shift from physical or virtual appliances to true cloud-native services delivered just milliseconds away from users and applications regardless of where they are in the world. This new paradigm will mean vastly more secure, more performant, and more reliable networks, creating better experiences for users and reducing total cost of ownership. IT will shift from being viewed as a cost center and bottleneck for business changes to a driver of innovation and efficiency.



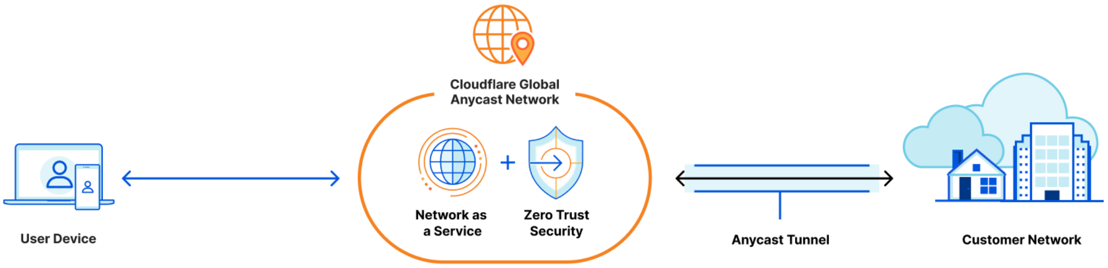
Generation 1: Castle and Moat; Generation 2: Virtualized Functions; Generation 3: Zero Trust Network

But transformative change can't happen overnight. For many organizations, especially those transitioning from legacy architecture, it'll take months or years to fully embrace Generation 3. The good news: Cloudflare is here to help, providing a bridge from your current network architecture to Zero Trust, no matter where you are on your journey.

back to top

How do we get there?

Cloudflare One, our combined Zero Trust network-as-a-service platform, allows customers to connect to our global network from any traffic source or destination with a variety of "on-ramps" depending on your needs. To connect individual devices, users can install the WARP client, which acts as a forward proxy to tunnel traffic to the closest Cloudflare location regardless of where users are in the world. Cloudflare Tunnel allows you to establish a secure, outbound-only connection between your origin servers and Cloudflare by installing a lightweight daemon.
Last year, we announced the ability to route private traffic from WARP-enrolled devices to applications connected with Cloudflare Tunnel, enabling private network access for any TCP or UDP applications. This is the best practice architecture we recommend for Zero Trust network access, but we've also heard from customers with legacy architecture that you want options to enable a more gradual transition.
For network-level (OSI Layer 3) connectivity, we offer standards-based GRE or IPsec options, with a Cloudflare twist: these tunnels are Anycast, meaning one tunnel from your network connects automatically to Cloudflare's entire network in 250+ cities, providing redundancy and simplifying network management. Customers also have the option to leverage Cloudflare Network Interconnect, which enables direct connectivity to the Cloudflare network through a physical or virtual connection in over 1,600 locations worldwide. These Layer 1 through 3 on-ramps allow you to connect your public and private networks to Cloudflare with familiar technologies that automatically make all of your IP traffic faster and more resilient.
Now, traffic from WARP-enrolled devices can route automatically to any network connected with an IP-layer on-ramp. This additional "plumbing" for Cloudflare One increases the flexibility that users have to connect existing network infrastructure, allowing organizations to transition from traditional VPN architecture to Zero Trust with application-level connectivity over time.



How does it work?

Users can install the WARP client on any device to proxy traffic to the closest Cloudflare location. From there, if the device is enrolled in a Cloudflare account with Zero Trust and private routing enabled, its traffic will get delivered to the account's dedicated, isolated network "namespace," a logical copy of the Linux networking stack specific to a single customer. This namespace, which exists on every server in every Cloudflare data center, holds all the routing and tunnel configuration for a customer's connected network.
Once traffic lands in a customer namespace, it's routed to the destination network over the configured GRE, IPsec, or CNI tunnels. Customers can configure route prioritization to load balance traffic over multiple tunnels and automatically fail over to the healthiest possible traffic path from each Cloudflare location.
On the return path, traffic from customer networks to Cloudflare is also routed via
Anycast to the closest Cloudflare location—but this location is different from that of the WARP session, so this return traffic is forwarded to the server where the WARP session is active. In order to do this, we leverage a new internal service called Hermes that allows data to be shared across all servers in our network. Just as our Quicksilver service propagates key-value data from our core infrastructure throughout our network, Hermes allows servers to write data that can be read by other servers. When a WARP session is established, its location is written

back to top

to Hermes. And when return traffic is received, the WARP session's location is read from Hermes, and the traffic is tunneled appropriately.

What’s next?

SecureCraft is a distributor of Cloudflare since 2017. To find out more about Cloudflare and SecureCraft, please email SecureCraft at sales@securecraftasia.com. Alternatively, you may call us at +65 6291 0508 or visit our website at www.securecraftasia.com.

Article from our CPP Partner, Numen Cyber

General introduction?

Digital forensics and incident response (DFIR) is a specialised field focused on identifying, remediating, and investigating cyber security incidents. Digital forensics includes collecting, preserving, and analysing forensic evidence to paint a complete, detailed picture of events. Incident response, meanwhile, is usually aimed at containing, stopping, and preventing an attack.

When combined, digital forensics and incident response get the organisation back up and running while identifying and closing security vulnerabilities — and it gives you the proof you need to press charges against the cybercriminals or support a cyber insurance claim.

DFIR has two main components:

Digital Forensics: A subset of forensic science that examines system data, user activity, and other digital evidence to determine if an attack is in progress and who may be behind the activity.
Incident Response: The overarching process that an organisation will follow to prepare for, detect, contain, and recover from a data breach.

What is Digital Forensics?

Digital forensics usually takes place once an IoC has been detected or an event/alert has been triggered on your systems that an attack is taking place or has already taken place.

The digital forensic process is the accepted method investigators follow to gather and preserve digital evidence, with the express intent of maintaining a chain of custody. It consists of three key steps:

1. **Acquisition:** In this step, investigators create an exact duplicate of the media, usually using a hard drive duplicator or specialized software tools. The original media is secured to prevent any tampering.
2. **Analysis:** Forensic specialists then analyse the duplicated files or technology, logging all the evidence they discover that supports or contradicts a hypothesis. The ongoing investigation is conducted to reconstruct events and actions in an incident, helping them reach conclusions about what happened and how hackers compromised systems.
3. **Reporting:** Once a digital forensics investigation is completed, the findings and conclusions analysts uncovered are delivered in a report that non-technical personnel can understand.

During the acquisition phase of the digital forensic process, analysts look for a variety of forensics data to help them in their investigation:

back to top

- **File System Forensics:** Analysing file systems within the endpoint for signs of compromise.
- **Memory Forensics:** Analysing memory for attack indicators that may not appear within the file system.
- **Network Forensics:** Reviewing network activity, including emailing, messaging, and web browsing, to identify an attack, understand the cybercriminal's attack techniques and gauge the scope of the incident.
- **Log Analysis:** Reviewing and interpreting activity records or logs to identify suspicious activity or abnormal events.

What is incident response?

Incident response (IR) is a set of activities a business engages in when they're amidst a cyber security incident. For IR, a cyber incident can be defined as any event that compromises information confidentiality, integrity, and/or availability – core principles of information security that are often referred to as the "CIA triad."

IR activities will generally be informed by an IR plan that's designed to get IT infrastructure back up and running as quickly as possible while mitigating the overall damage of an incident. These frameworks are designed to support recovery efforts, but they also help organizations build cyber maturity and proficiency in a broader sense. This may help enhance defences, stopping attacks and incidents from affecting businesses in the first place.

Six Steps of Incident Response are as follows:

- Preparation
- Identification and Scoping
- Containment/Intelligence Development
- Eradication/Remediation
- Recovery
- Lesson Learned and Post Incident Review

Usually, the detection is originated by the threat-detection or security operation team. The aim of the organization should be to manage the entire incident in-house. To prepare for successful incident management, the security team must develop a set of checklists/playbooks for every six steps.
The Incident management should also focus on understanding the motivation of the adversaries.

Why is DFIR important in cyber security?

For organisations targeted by a cyber security attack, recovery is the top-of-mind concern — but beyond getting back up and running, it's also essential to understand the how and why behind an incident.

DFIR delivers more profound understanding through a comprehensive and intricate forensic process. DFIR professionals gather and inspect a vast amount of information to determine who attacked them, how the compromise happened, the exact steps attackers took to compromise their systems, and what they can do to close those security gaps.

This information is also frequently used to help build a legal case against the identified attackers. The data is gathered using the digital forensic process, allowing investigators to uncover and preserve digital evidence.

What Is the MITRE ATT&CK Framework?

The MITRE ATT&CK matrix contains a set of **techniques** used by adversaries to accomplish a specific objective. The objectives are presented linearly from the point of reconnaissance to the final goal of exfiltration or "impact". Those objectives are categorized as tactics in the ATT&CK Matrix. Looking at the broadest version of ATT&CK for Enterprise, which includes Windows, MacOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS, and Network environments, the following adversary tactics are categorized:

back to top

1. **Reconnaissance:** gathering information to plan future adversary operations, i.e., Vulnerability Scanning, OSINT
2. **Resource Development:** establishing resources to support operations, i.e., setting up command and control infrastructure, buying fake Domain
3. **Initial Access:** trying to get into your network, i.e., phishing, Supply Chain Compromise
4. **Execution:** trying the malicious run code, i.e., running a remote access tool
5. **Persistence:** trying to maintain their foothold, i.e., changing configurations, Account Manipulation, Create or Modify System Process
6. **Privilege Escalation:** trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate Access, Abuse Elevation Control Mechanism
7. **Defence Evasion:** trying to avoid being detected, i.e., using trusted processes to hide malware, Abuse Elevation Control Mechanism, Disable logs, Hide Artifacts
8. **Credential Access:** stealing accounts names and passwords, i.e., keylogging, Brute Force, Force Authentication
9. **Discovery:** trying to figure out your environment, i.e., exploring what they can control, Account Discovery, Permission Groups Discovery
10. **Lateral Movement:** moving through your environment, i.e., using legitimate credentials to pivot through multiple systems, Internal Spear phishing
11. **Collection:** gathering data of interest to the adversary goal, i.e., accessing data in cloud storage, Input Capture
12. **Command and Control:** communicating with compromised systems to control them, i.e., mimicking regular web traffic to communicate with a victim network, Data Obfuscation
13. **Exfiltration:** stealing data, i.e., transferring data to the cloud account, Exfiltration Over network
14. **Impact:** manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware, Data Manipulation, Defacement

In order to perform a Successful DFIR, it is essential to understand the concept of **MITRE ATT&CK Framework** as it will help to provide visualisation during the hypothesis phase.

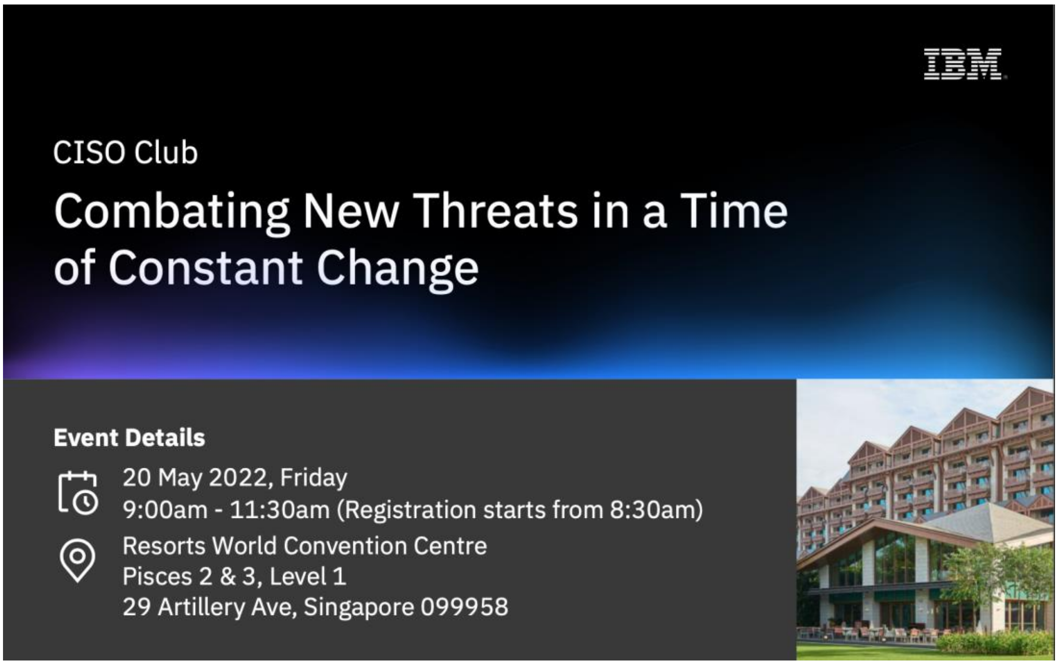
Conclusion

No matter how secure is the environment, compromise incident sometime can be inevitable. Thus, organisations should rethink their defensive strategy to not just focus on the prevention domain but also they need to know how to react and respond whenever there is a security incident.

For further enquiries, please contact Ms Joanna Zhang at joannazh@numencyber.com

back to top

Article from our CPP Partner, IBM



IBM

CISO Club

Combating New Threats in a Time of Constant Change

Event Details

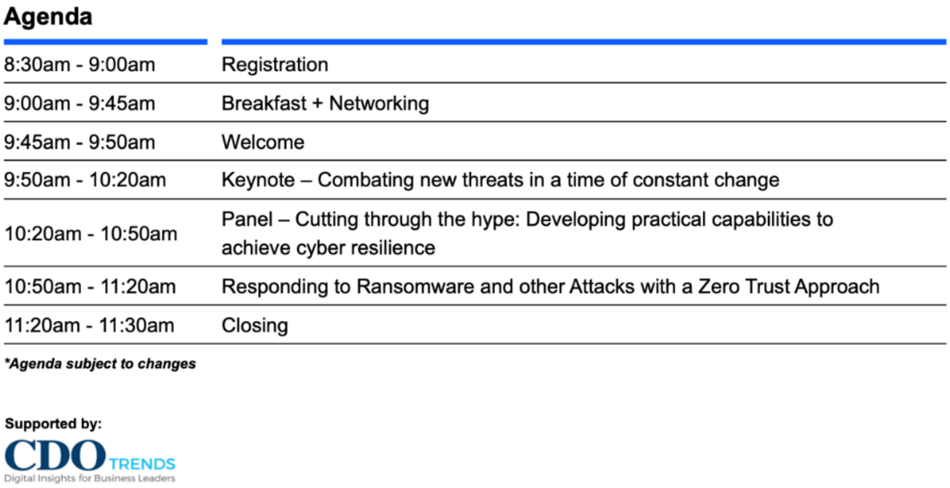
20 May 2022, Friday
9:00am - 11:30am (Registration starts from 8:30am)

Resorts World Convention Centre
Pisces 2 & 3, Level 1
29 Artillery Ave, Singapore 099958

The world continues to grapple with a lasting pandemic, shifts to work-from-home and back-to-office, and geopolitical changes spawning a constant drone of mistrust. The result is chaos, and it is in chaos that cyber criminals thrive.

When CDOTrends spoke to IBM, it was evident that a zero trust approach was not just to prevent breaches, but to ensure that the organisation could continue to function amidst an attack.

With the volatile landscape and the evolution of both threat types and threat vectors, join our CISO Club, supported by CDOTrends, for stimulating discussions on the threat intelligence insights you need to stay ahead of attackers and fortify your critical assets more than ever.



Agenda

8:30am - 9:00am	Registration
9:00am - 9:45am	Breakfast + Networking
9:45am - 9:50am	Welcome
9:50am - 10:20am	Keynote – Combating new threats in a time of constant change
10:20am - 10:50am	Panel – Cutting through the hype: Developing practical capabilities to achieve cyber resilience
10:50am - 11:20am	Responding to Ransomware and other Attacks with a Zero Trust Approach
11:20am - 11:30am	Closing

Agenda subject to changes

Supported by:

CDO TRENDS
Digital Insights for Business Leaders

back to top

Scan the QR code to Register Now!

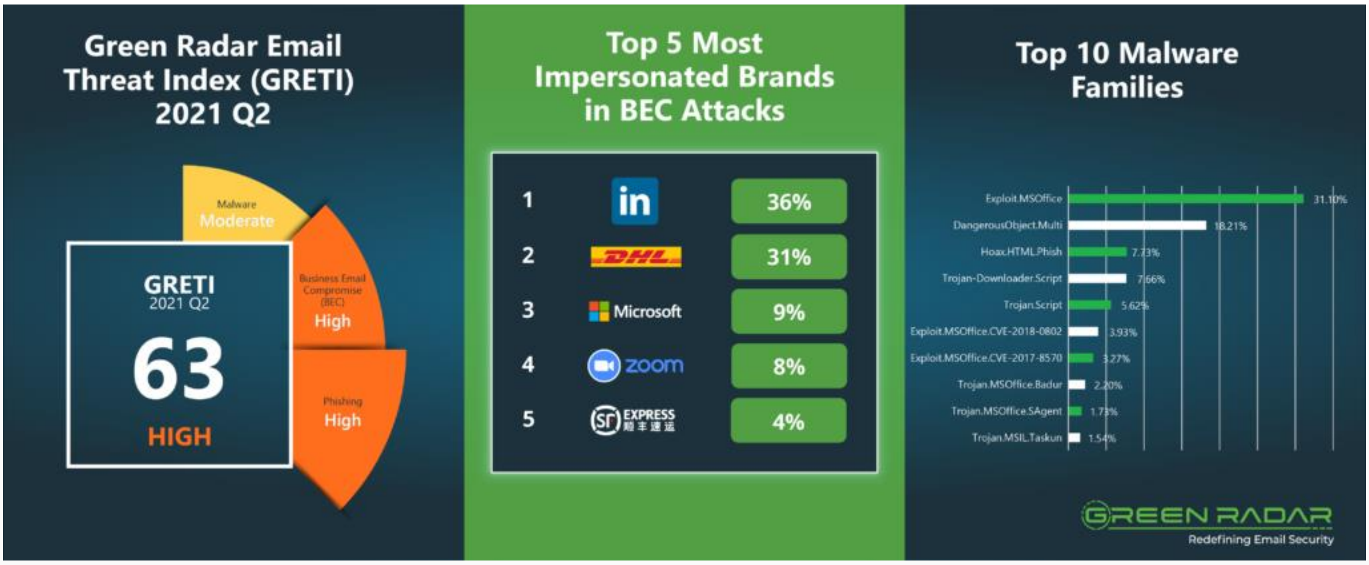
Article from our SME Cybersecurity Conference Sponsor, Green Radar

Business Email Compromise attacks highlighted as an emerging threat in the inaugural Green Radar Email Threat Index – 26 August 2020

Green Radar ("Green Radar" or "Company") launched the inaugural Green Radar Email Threat Index ("GRETI" or the "Index"） for the second quarter of 2021. The GRETI revealed the level of risks that organizations are exposed to remain at a high level, with an Index score of 63. The Index indicated that the most prominent email threats, including phishing and malware attacks, are shown as high and moderate levels respectively, with Business Email Compromise (BEC) attacks becoming an emerging threat with the potential to cause a high level of impact to businesses.

The Index was constructed using data originating from Green Radar's proprietary artificial intelligence (AI) and machine learning engine aidar™. It intercepts about 70% of the millions of daily incoming emails. Among those, 18.6% are flagged as highly sophisticated email attacks by aidar™ with the assistance from a team of experts at the Green Radar Security Operations Centers in Hong Kong and Singapore (SOCs). The GRETI aims to raise awareness of email threats posed to organizations and assist cybersecurity practitioners with the latest threat trends and insights to develop appropriate protective measures.

back to top



Phishing and Malware popular with fraudsters

The GRETI report highlighted phishing as the most frequently reported attack vector. Phishing activity remained high throughout the second quarter, and it was especially pronounced in June as fraudsters took advantage of Taobao's 618 shopping festival to plant fake goods delivery emails.

Although the level of attacks due to malware has moderated during the second quarter of the year, the report noted that fraudsters deployed new tactics and techniques to embed malware inside email attachments to evade and bypass technical controls. The most common malware recorded is the *Exploit.MSOffice* family that exploit vulnerabilities in Microsoft Office software. Infected devices can allow cybercriminals to control the user's device, destroy data, capture keystrokes and give them access to the broader corporate network.

Business Email Compromise costly for their victims

The consequence to organizations that fall victim to Business Email Compromise (BEC) attacks can be catastrophic even though the attack volume is small. With financial institutions often the target of attacks, fraudsters deploy this method to create highly realistic and tailored emails, impersonating big-name brands to add credibility in their attempt to cause harm and financial loss for their victims. The top three most impersonated brands identified in the report are LinkedIn, DHL and Microsoft.

Information has shown that a financial services firm in Hong Kong has lost HK$41 million from a BEC scam in 2020[1]. According to the statistics of Federal Bureau of Investigation (FBI), BEC attacks cost global businesses a staggering US$1.8 billion in 2020.[2]

For full report of the "Green Radar Email Threat Index", downloaded from: https://www.greenradar.com/email-threat-index/

back to top

Article from The Cybersecurity Awards 2021 Winner – Mr Yu Pengfei

I am extremely honoured to be the recipient of The Cybersecurity Awards 2021 (Student Category). It is heartening to have my work in the community recognized and celebrated. However, these achievements would not be possible if not for the support from the N0H4TS team and the wider Division Zero (Div0) cybersecurity community. I first embarked on my volunteering journey with the cybersecurity community back in 2018 as a year one student at university. Alas, time flies so quickly and the small N0H4TS student club founded by my friends and I has now grown into an extensive student-oriented community as a quarter under Div0.

Together, we launched significant initiatives and programs such as the first local cybersecurity student conference; STANDCON, the annual league-based Capture-The-Flag competition; The Cyber League, the progress and specialization tracker for our participants known as the Mastery Framework.

These breakthroughs wouldn't have been possible without the hardworking team at Div0-N0H4TS and the collaborations between everyone in the cybersecurity community. My warmest appreciation to the team and our partners for your continued support.

back to top

I was also inspired and had immense support from my mentors both in academia and the community. The achievements of N0H4TS were made possible because of the guidance from Dr. Goh Weihan from the Singapore Institute of Technology and Mr. Emil Tan, co-founder of Div0. I benefitted greatly from their wisdom and advice.

Just like how my mentors were role models to me, I hope I can be a role model to my fellow peers and juniors for them to follow my lead to volunteer and contribute to the cybersecurity ecosystem in the future.

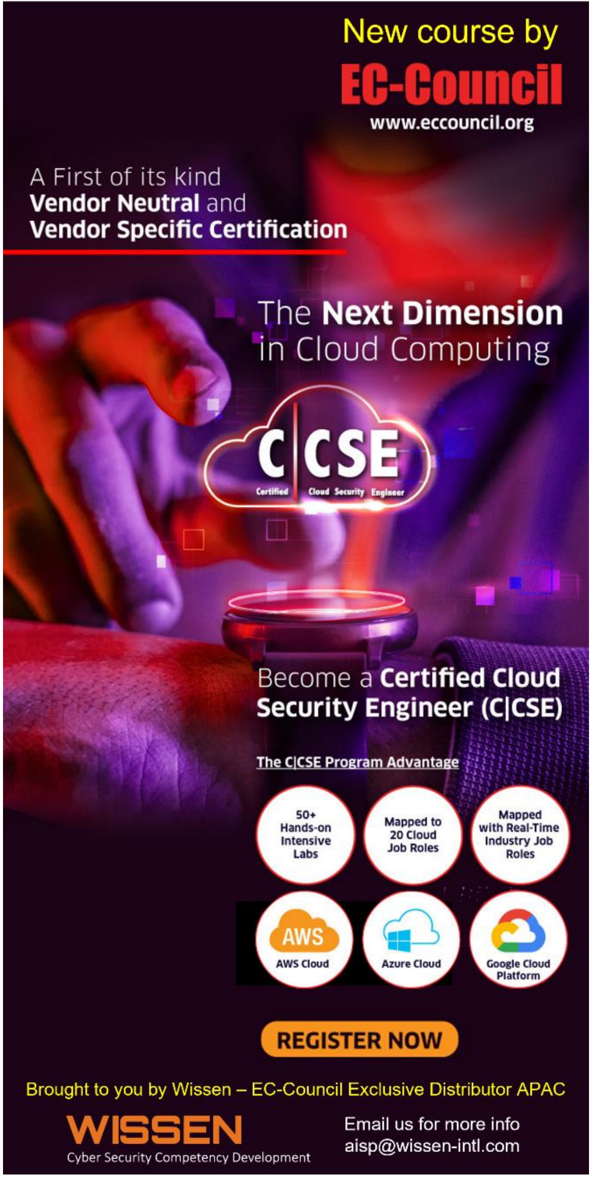
Lastly, this award not only reaffirms my contributions to the cybersecurity community in Singapore, but also the efforts of my fellow volunteers at N0H4TS. This award marks the end of my four-years journey as a university student. Moving forward as a young professional in the Government Technology Agency, I hope to continue to contribute back to the community by acting as the bridge between the industry and the community. So don't worry, you will still see me around at meet ups!

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

back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International


New course by
EC-Council
www.eccouncil.org
A First of its kind
Vendor Neutral and
Vendor Specific Certification
The Next Dimension
in Cloud Computing
C|CSE
Certified Cloud Security Engineer
Become a Certified Cloud
Security Engineer (C|CSE)
The C|CSE Program Advantage
50+ Hands-on Intensive Labs
Mapped to 20 Cloud Job Roles
Mapped with Real-Time Industry Job Roles
AWS
AWS Cloud
Azure Cloud
Google Cloud Platform
REGISTER NOW
Brought to you by Wissen – EC-Council Exclusive Distributor APAC
WISSEN
Cyber Security Competency Development
Email us for more info
aisp@wissen-intl.com

Introducing new course by EC-Council
Certified Cloud Security Engineer (CCSE)

Organizations need cloud security engineers to help them build a secure cloud infrastructure, monitor vulnerabilities, and implement incidence response plans to mitigate cloud-based threats. CCSE, with its unique blend of vendor-neutral and vendor-specific concepts, trains candidates in the fundamentals while equipping them with job-ready practical skills.

Email us to find out more aisp@wissen-intl.com

back to top

Listing of Courses by ALC Council

Stand out from the crowd
with the world's most exclusive cyber security certification
SABSA®
alc

"The global standard for Cyber Security Architecture"

SABSA Foundation 23-27 May 2022

Live Virtual training 9:00 am – 5:00 pm SGT

Special 15% discount for AiSP members

Getting your architecture right is the critical success factor for robust and effective cyber security in business and government.

SABSA represents the world standard for cyber security architecture. When you get your SABSA accreditation you become a member of an exclusive group positioned strategically between two domains – that of top management and that of the technical subject matter expert.

SABSA mandates the most highly-qualified instructors

Fully-accredited SABSA training is conducted only by instructors who hold the SABSA Master certification - the most demanding certification in the industry. Accredited SABSA trainers have to pass three exams – SABSA Foundation and two Advanced courses - with a minimum mark of 75%. They then have to attain the SABSA Master certification by preparing a university-style thesis

back to top

demonstrating experience and understanding, subject to review by two assessors. That is what you get from ALC.

SABSA Certification >>

ALC is the only accredited SABSA provider in Singapore

ALC Training Pte Ltd is the only accredited provider of SABSA cyber security architecture training in Singapore.

Start your SABSA journey with the globally recognised **SABSA Foundation Certificate**. Next course to be held in the Singapore time zone on 23-27 May 2022.

Full course details and registration >>

ALC Training Pte Ltd is proud to be an AiSP Partner.

Take a look at our full Singapore training program.

You can claim your AiSP 15% member discount against any course. All you have to do is copy-paste ALCAiSP15 on the Promotion Code field on the registration form.

Any questions, don't hesitate to contact us at customerservice@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®) Course

STEPPING UP ON INFORMATION SECURITY
AiSP
Advance Connect Excel
QUALIFIED INFORMATION SECURITY PROFESSIONAL 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
- Security Controls
- Security Principles and Lifecycle
- Business Continuity Planning
- Develop and Implement Security Goals, Objective and Strategy and Programs

back to top

- Maintain and Review Security Operations

COURSE DETAILS

2022 Course dates can be found on https://www.aisp.sg/qisp_training.html
Time: 9am-6pm
Fees: $2,500 (before GST)*
**10% off for AiSP Members @ $2,250 (before GST)*
*Utap funding is available for NTUC Member

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

STEPPING UP ON INFORMATION SECURITY
AiSP
Advance Connect Excel
CYBERSECURITY ESSENTIALS COURSE

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

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

Course Objectives

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

- Introduction to Security
- Risk Management
- Cybersecurity IT Platform
- Securing the Server
- Securing the Network
- Cloud Computing
- Cybersecurity Operations

back to top

COURSE DETAILS

Training dates for year 2022 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

TARGET AUDIENCE

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

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

Program Partner

Delivery Partners

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: 2021 to 2022) from 1 Sept 2021 to 31 Dec 2022. 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.

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. Interested applicants should be qualified AiSP Ordinary Members (Path 1) for at least a year to apply for AVIP.

Your AiSP Membership Account
AiSP has ceased its digital platform, Glue Up and are currently exploring other options to provide our members a better and user-friendly experience.

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!

back to top

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

ABPGROUP

Acronis

BCG

BitCyber
Securing Your Business

BD

BeyondTrust

BLACKPANDA

Checkmarx

CISCO

CSIT
Centre for Strategic Infocomm Technologies

CSA
SINGAPORE

CYCOGNITO

CYFIRMA
DECODING THREATS

DBS

elastic

ENSIGN
INFOSECURITY

ExtraHop

FIREEYE™

FORTINET®

GOVTECH
SINGAPORE

HUAWEI CLOUD
Grow with Intelligence

IBM®

無限

INSIGHTZ
TECHNOLOGY

IronNet

ITSEC
ASIA

kaspersky

MANDIANT®

Marsh

back to top

MICRO FOCUS

MINDEF SINGAPORE

mimecast

NETWITNESS An RSA Business

NUMEN

PriVasec

RAJAH & TANN CYBERSECURITY

Recorded Future

Responsible Cyber

SAVIYNT

SecurID An RSA Business

SECURECRAFT

Singtel

ST Engineering

TANIUM

ThriveDX Formerly Cybint

TREND MICRO

xcellink.pte.ltd. completing your technology chain

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

ITE Institute of Technical Education

NYP NANYANG THE INNOVATIVE POLYTECHNIC

NGEE ANN POLYTECHNIC

NUS National University of Singapore

REPUBLIC POLYTECHNIC DISCOVER. TRANSFORM. ACHIEVE

SiT SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SMU SINGAPORE MANAGEMENT UNIVERSITY

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek POLYTECHNIC

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.

Advance Connect Excel

🌐 www.AiSP.sg
✉ secretariat@aisp.sg
☎ +65 8878 5686
📍 116 Changi Road, #04-03 WIS@Changi, S419718
Please email us for any enquiries.

back to top