AiSP NEWSLETTER

December 2021

NEWS & UPDATE

New Corporate Partners

AiSP would like to welcome ABPGroup, INTfinity, Numen Cyber Technology, Mandiant, IronNet Cybersecurity, Xcelink Group and Rajah & Tann as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Academic Partner

AiSP would like to welcome National University of Singapore (NUS) as our new academic partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

Continued Collaboration

AiSP would like to thank the following partners for their continued support in developing the cybersecurity landscape:

APP: Singapore Polytechnic (SP)

CPP: CISCO and BitCyber

We look forward to the exciting collaborations with these partners.

SINGAPORE POLYTECHNIC SP   BitCyber Securing Your Business   CISCO

Overview of Cybersecurity Local & Worldwide by Huawei

AiSP would like to thank our CPP Huawei Cloud for inviting our AiSP EXCO Member, Faith Chng to speak on 18 November's webinar: Safeguard Your Business Against Cyber Attacks. It was an informative and enjoyable session for the participants!

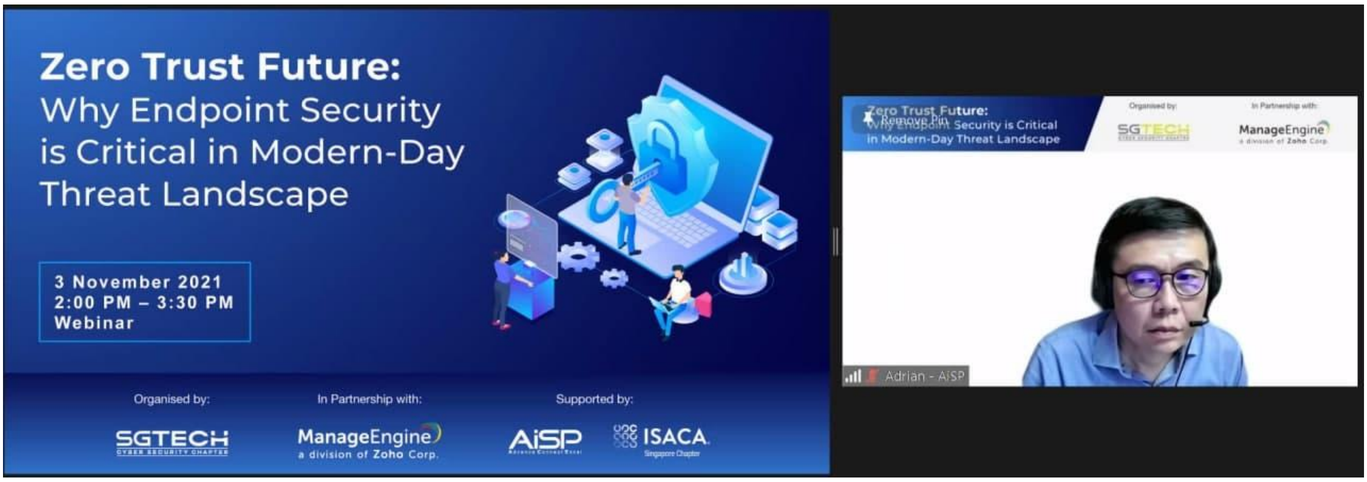
Overview of Cybersecurity Local & Worldwide
Faith Chng
18 Nov 2021

Overview of Cybersecurity Local & Worldwide
Faith Chng
18 Nov 2021

back to top

Zero Trust Future: Why Endpoint Security is critical in Modern-Day Threat Landscape by SGTech

We would like to thank all participants who have attended the webinar organized by SGTech on Zero Trust Future: Why Endpoint Security is critical in Modern-Day Threat Landscape on 3 November. AiSP EXCO Member, Mr Adrian Oey was one of the panel speakers who shared his insights on Zero Trust model and its importance in today's cybersecurity landscape.



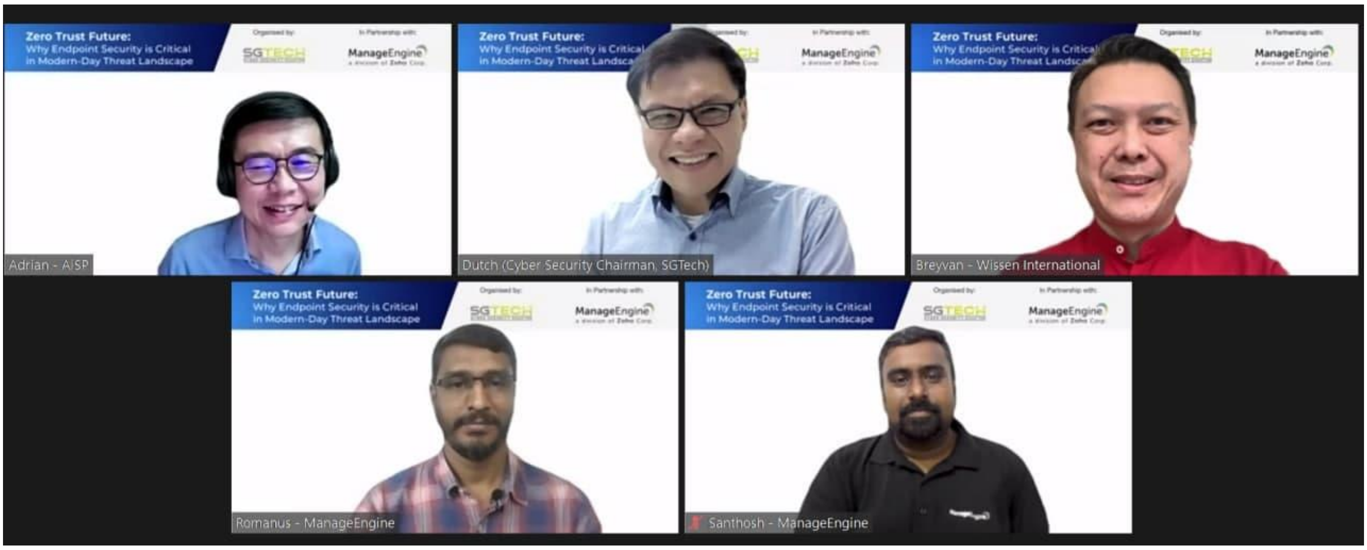
Zero Trust Future:
Why Endpoint Security is Critical in Modern-Day Threat Landscape

3 November 2021
2:00 PM – 3:30 PM
Webinar

Organised by: SGTECH CYBER SECURITY CHAPTER

In Partnership with: ManageEngine a division of Zoho Corp.

Supported by: AiSP ISACA Singapore Chapter

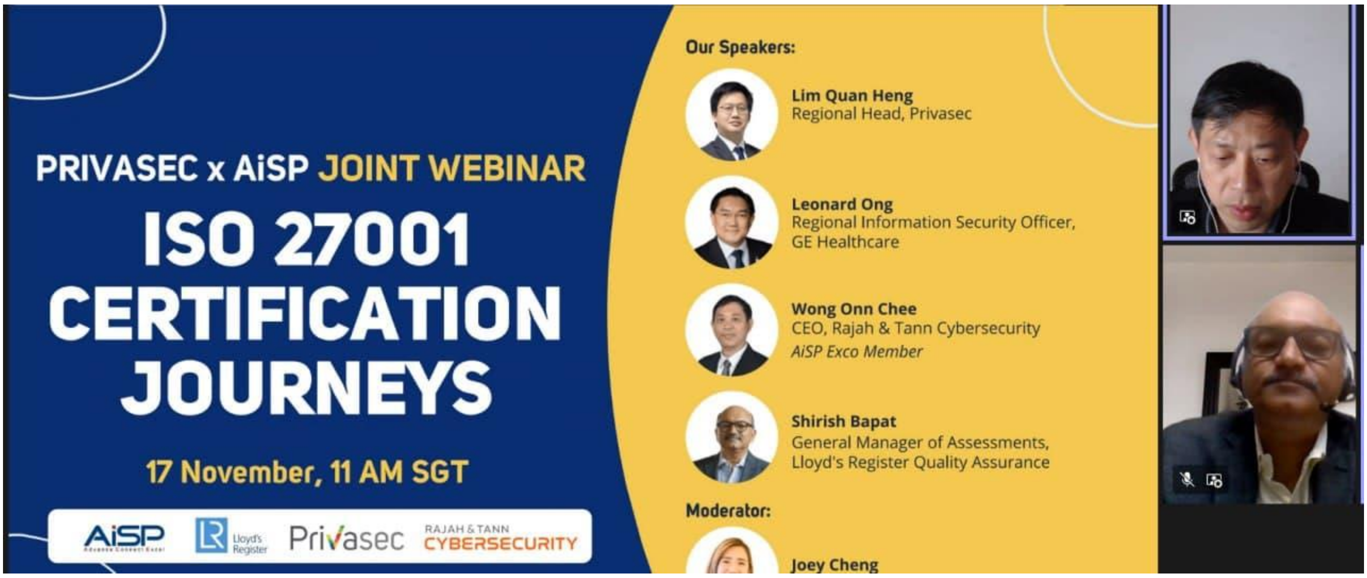


Adrian - AiSP
Dutch (Cyber Security Chairman, SGTech)
Breyvan - Wissen International
Romanus - ManageEngine
Santhosh - ManageEngine

back to top

Privasec x AiSP Joint Webinar - ISO27001 Certification Journeys

An insightful morning has been for our participants who attended the Privasec x AiSP Joint Webinar - ISO27001 Certification Journeys on 17 November morning. AiSP EXCO Member, Onn Chee W. was one of the panel speakers who shared during the webinar. We would like to thank our CPP Privasec for co-organizing the webinar with AiSP.



PRIVASEC x AiSP JOINT WEBINAR

ISO 27001 CERTIFICATION JOURNEYS

17 November, 11 AM SGT

Our Speakers:

Lim Quan Heng
Regional Head, Privasec

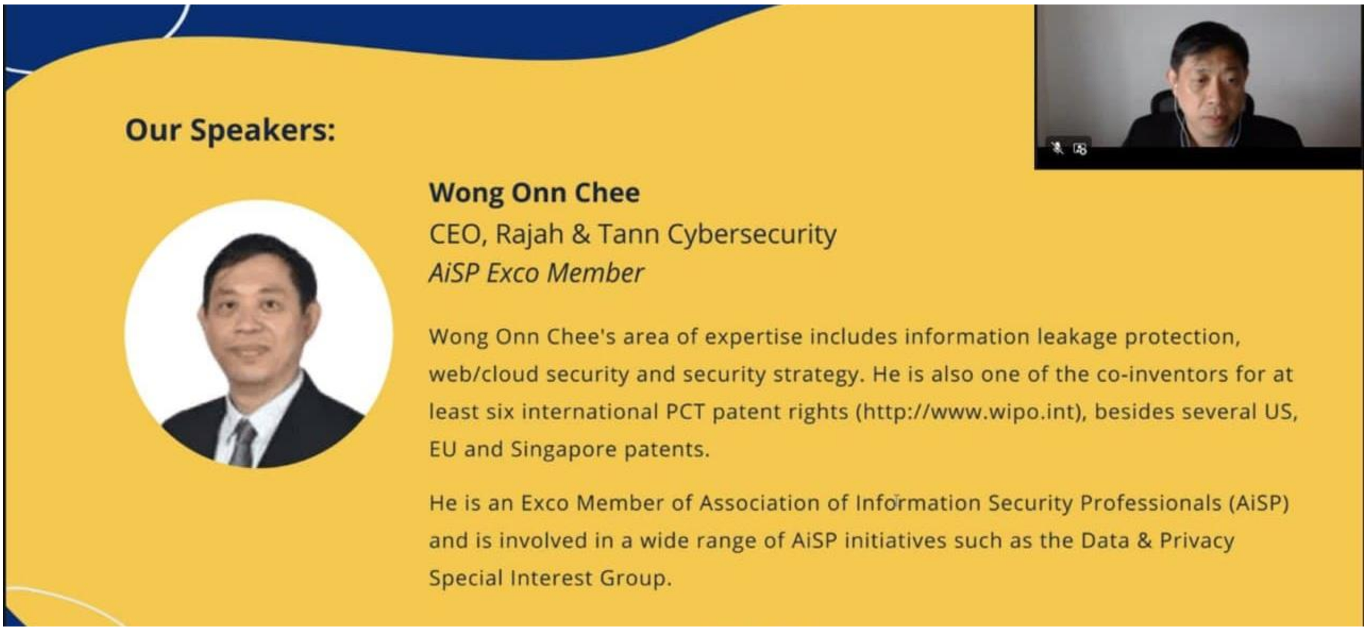
Leonard Ong
Regional Information Security Officer, GE Healthcare

Wong Onn Chee
CEO, Rajah & Tann Cybersecurity
AiSP Exco Member

Shirish Bapat
General Manager of Assessments, Lloyd's Register Quality Assurance

Moderator:

Joey Cheng



Our Speakers:

Wong Onn Chee
CEO, Rajah & Tann Cybersecurity
AiSP Exco Member

Wong Onn Chee's area of expertise includes information leakage protection, web/cloud security and security strategy. He is also one of the co-inventors for at least six international PCT patent rights (http://www.wipo.int), besides several US, EU and Singapore patents.

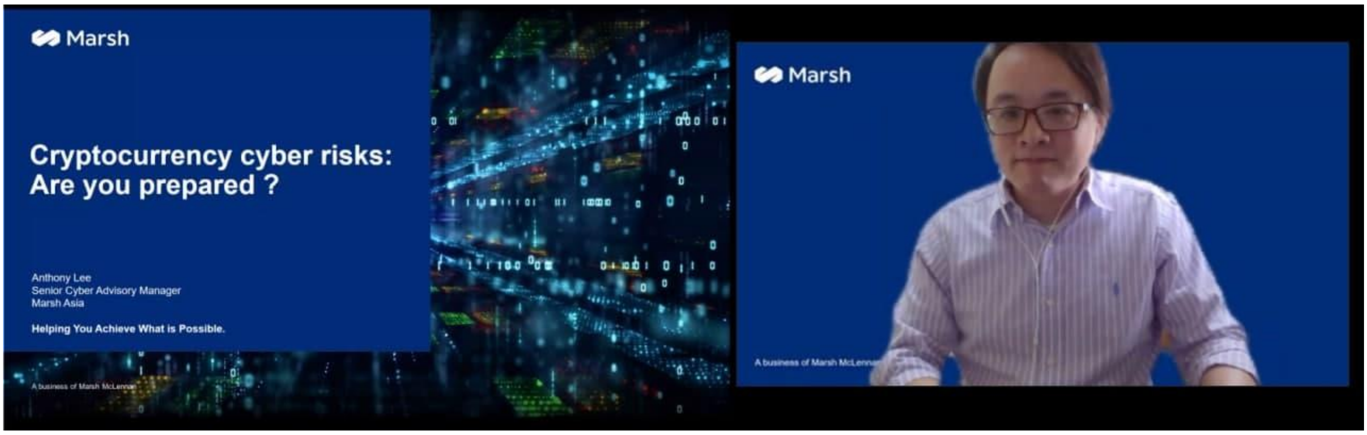
He is an Exco Member of Association of Information Security Professionals (AiSP) and is involved in a wide range of AiSP initiatives such as the Data & Privacy Special Interest Group.

back to top

Knowledge Series Events

Emerging Trends – Blockchain & AI for Cyber Security on 17 Nov

Thank you all who have joined us for our BOK sharing on Blockchain Technology by our speakers, Mr Anthony Lee and Mr Jeremie Deschamps from our CPP Marsh and Dr Xue Tengfei from our CPP Huawei.



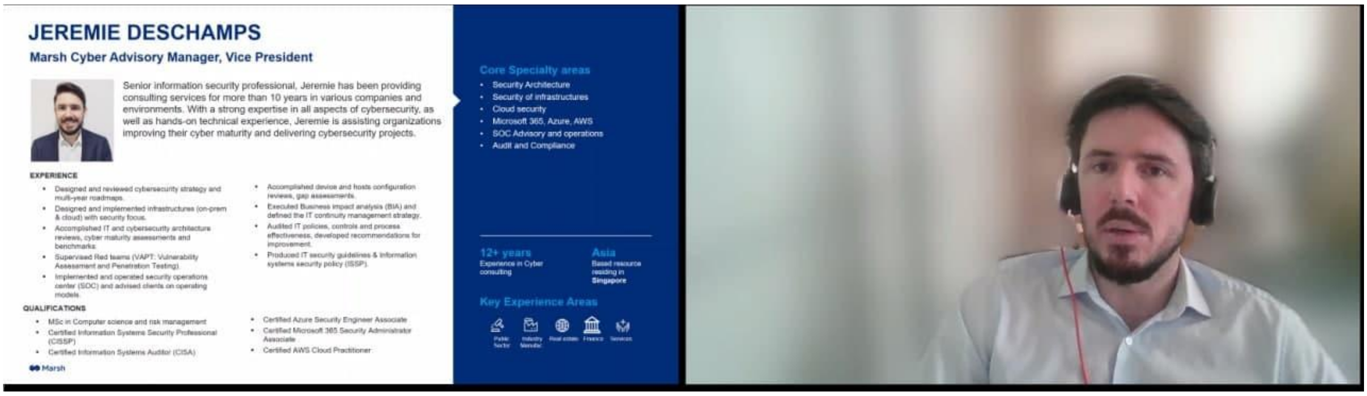
Marsh

Cryptocurrency cyber risks:
Are you prepared ?

Anthony Lee
Senior Cyber Advisory Manager
Marsh Asia

Helping You Achieve What is Possible.

A business of Marsh McLennan



JEREMIE DESCHAMPS

Marsh Cyber Advisory Manager, Vice President

Senior information security professional, Jeremie has been providing consulting services for more than 10 years in various companies and environments. With a strong expertise in all aspects of cybersecurity, as well as hands-on technical experience, Jeremie is assisting organizations improving their cyber maturity and delivering cybersecurity projects.

EXPERIENCE

- Designed and reviewed cybersecurity strategy and multi-year roadmaps.
- Designed and implemented infrastructures (on-prem & cloud) with security focus.
- Accomplished IT and cybersecurity architecture reviews, cyber maturity assessments and benchmarks.
- Supervised Red teams (VAPT: Vulnerability Assessment and Penetration Testing).
- Implemented and operated security operations center (SOC) and advised clients on operating models.
- Accomplished device and hosts configuration reviews, gap assessments.
- Executed Business impact analysis (BIA) and defined the IT continuity management strategy.
- Audited IT policies, controls and process effectiveness, developed recommendations for improvement.
- Produced IT security guidelines & information systems security policy (ISSP).

QUALIFICATIONS

- MSc in Computer science and risk management
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Azure Security Engineer Associate
- Certified Microsoft 365 Security Administrator Associate
- Certified AWS Cloud Practitioner

Marsh

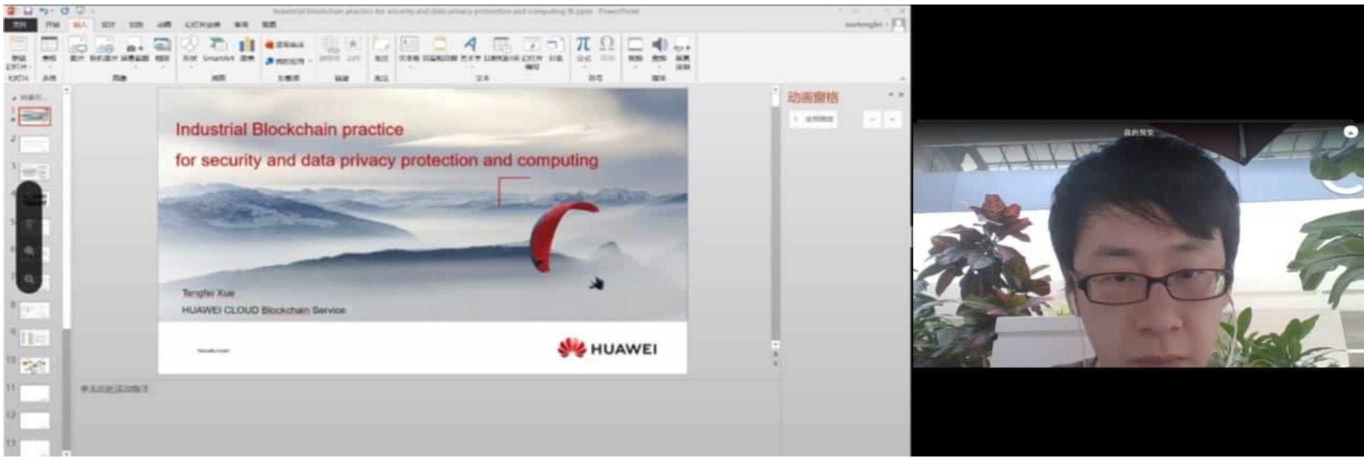
Core Specialty areas

- Security Architecture
- Security of infrastructures
- Cloud security
- Microsoft 365, Azure, AWS
- SOC Advisory and operations
- Audit and Compliance

12+ years
Experience in Cyber consulting

Asia
Based resource residing in **Singapore**

Key Experience Areas



Industrial Blockchain practice

for security and data privacy protection and computing

Tengfei Xue

HUAWEI CLOUD Blockchain Service

back to top

Data Security on 27 January 2022

Based on AiSP Information Security Body of Knowledge (IS BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable AiSP members with a bettering understanding of how IS BOK can be implemented at workplaces.

AiSP Knowledge Series – Data Security

KNOWLEDGE SERIES - DATA SECURITY
3PM-5PM | Zoom
JAN
27
AARON ANG
APAC Project Manager & Trainer
ThriveDX SaaS
CHOW LAI LENG
Head of Enterprise - SEA
Kaspersky
Organised by:
AiSP
Advance Connect Excel
Supported by:
kaspersky
ThriveDX
Formerly Cybint Solutions

As part of AiSP Knowledge Series, we have ThriveDX SaaS and Kaspersky with us to share about data security. The global COVID-19 pandemic has accelerated the pace of digital transformation. Businesses are creating, processing, and storing more data than ever before. Cybercriminals are also ramping up their campaigns targeting businesses. Building cybersecurity foundation is now a priority instead of an option. Join us as we learn about mitigating risk factor as well as integrating cybersecurity in your digital transformation journey.

Data Security – Patching the Human Firmware
By: Aaron Ang, APAC Project Manager & Trainer, ThriveDX SaaS

The global COVID-19 pandemic has accelerated the pace of digital transformation and have forced many of us to change the way we live, work and play. Businesses are also creating, processing and storing more data than ever before. In addition, today's sophisticated computing environments spanning public and private clouds, on-premise infrastructure,

back to top

remote endpoints, Operational Technology (OT) systems and Internet of Things (IoT) devices have made securing data an increasingly complex challenge. With the myriad of data protection technologies and solutions in our cybersecurity ecosystem today, the human factor remains the weakest link in the data protection strategies of many organizations.

Come join us at this session to learn how organizations can mitigate the human risk factor and secure their data by patching the human "firmware".

Building a cybersecure and sustainable future for SMBs in Singapore
By: Chow Lai Leng, Head of Enterprise – SEA, Kaspersky

Businesses have rapidly modernized to meet the needs of our digital age. The last two years also proved that technology is an essential tool to survive and even break through from this pandemic and beyond. Fast-tracked digitalization, however, comes with its fair share of cyber risks. As businesses shift major processes and billions of data online, cybercriminals are also ramping up their campaigns targeting businesses in every size and sector. As such, building cybersecurity foundation is now a priority instead of an option.

Join us in this session to know how to integrate cybersecurity in your digital transformation journey and to understand how you could better secure your business as you prepare for a post-pandemic recovery.

Date: 27th January 2022 (Thurs)
Time: 3PM to 5PM
Venue: Zoom
Registration: https://zoom.us/webinar/register/WN_LoYd6XryS0WNvxTG3jGcuQ

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 2021 are as follows (*may be subjected to changes*),

1. Data Security, 27 Jan
2. Red Team VS Blue Team, 17 Feb
3. Cryptography, 17 Mar

*Subjected to Singapore Government's directives for physical events during COVID-19 pandemic.

Please let us know if your organisation is keen to be our sponsoring speakers in 2022!

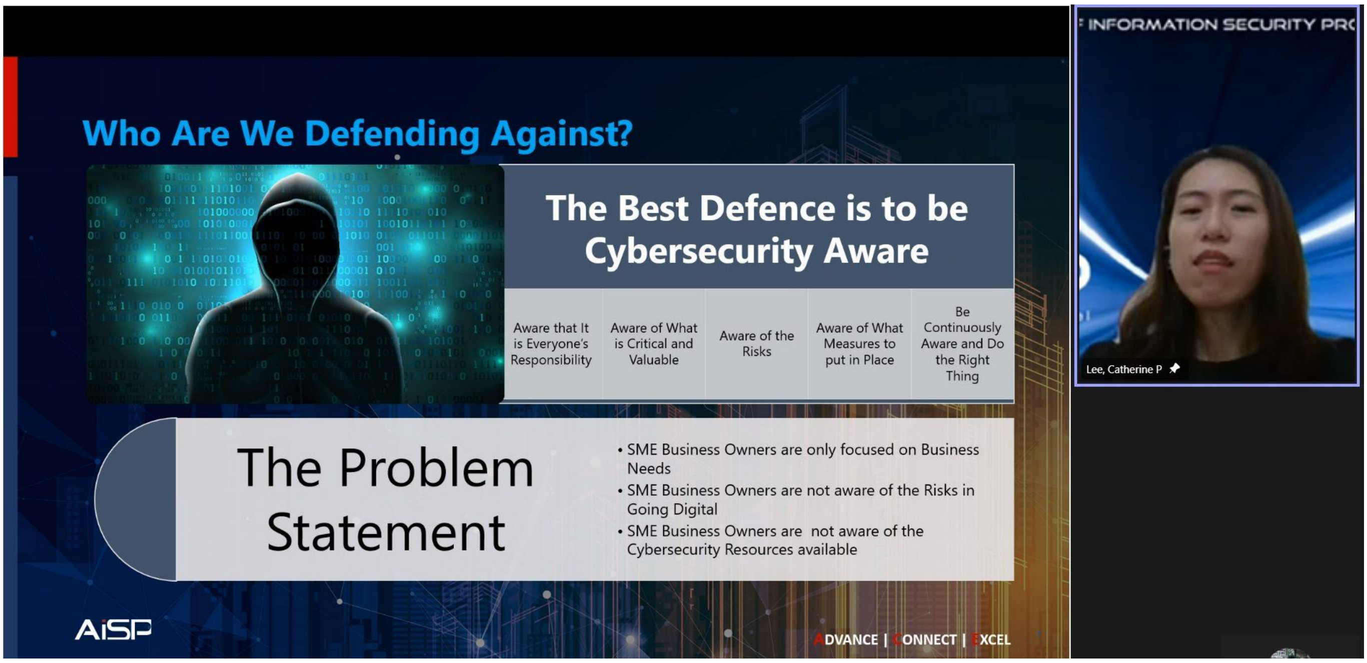
AiSP members who registered for the event, can playback the recorded event via their member profile in Glue Up. If you did not sign up for the event, please email secretariat@aisp.sg for assistance. Please refer to our scheduled 2021 webinars in our event calendar.

back to top

Cybersecurity Awareness & Advisory Programme (CAAP)

Cybersecurity Awareness and Cybersecurity Courses on 10 Nov

On 10 November, for CAAP Focus Group Discussion, we have AiSP EXCO Member, Ms Catherine Lee, to facilitate this session. We are also joined with like-minded participants to discuss about various cyber topics.



Who Are We Defending Against?

The Best Defence is to be Cybersecurity Aware

Aware that It is Everyone's Responsibility	Aware of What is Critical and Valuable	Aware of the Risks	Aware of What Measures to put in Place	Be Continuously Aware and Do the Right Thing

The Problem Statement

- SME Business Owners are only focused on Business Needs
- SME Business Owners are not aware of the Risks in Going Digital
- SME Business Owners are not aware of the Cybersecurity Resources available

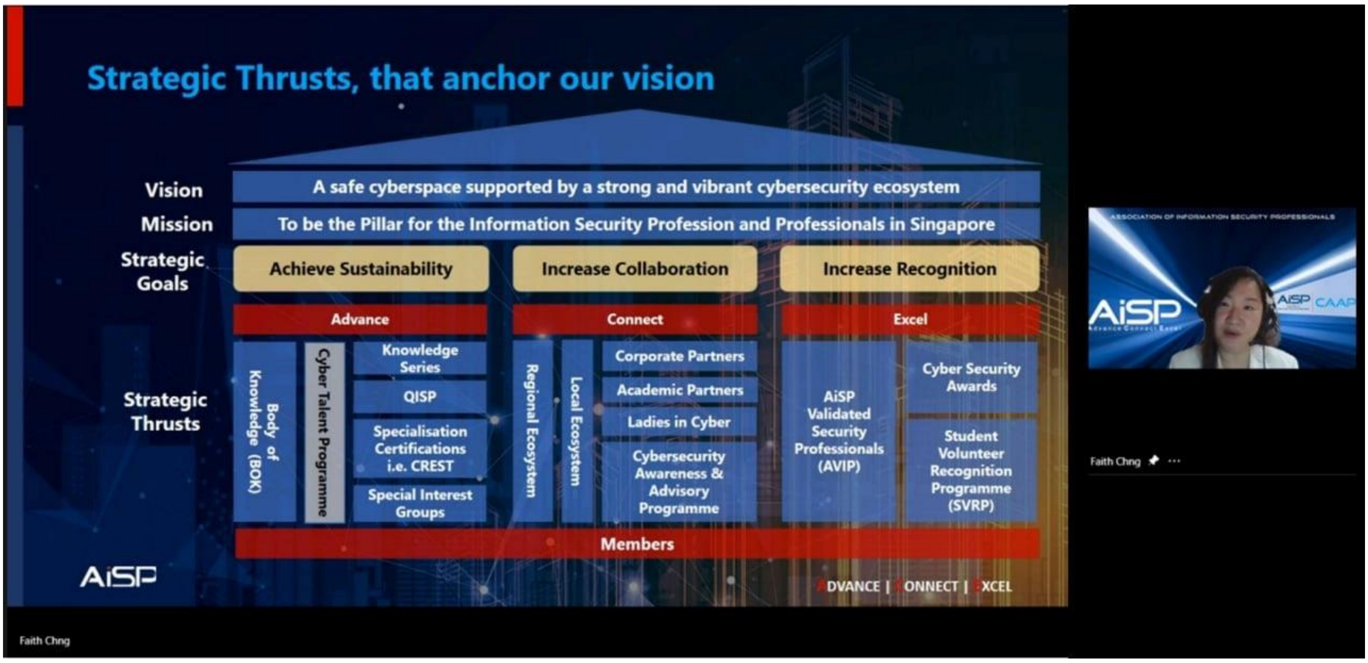
AiSP

ADVANCE | CONNECT | EXCEL

Singapore SMEs' Digital Adoption and Concerns on 24 Nov

On 24 November, AiSP x PA CAAP Focus Group Discussion Workshop was hosted by AiSP EXCO Member Faith Chng. We discussed several issues such as rising cyber threats, cybersecurity concerns as well as the importance of cybersecurity in businesses. We had a fruitful discussion with the participants, and we hope to have more people joining us in future sessions. We would like to give a big thank you to all that have attended this workshop and we hope everyone has gained some insights regarding these topics.

back to top



Strategic Thrusts, that anchor our vision

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

Mission: To be the Pillar for the Information Security Profession and Professionals in Singapore

Strategic Goals: Achieve Sustainability | Increase Collaboration | Increase Recognition

Strategic Thrusts:

Advance: Body of Knowledge (BOK); Cyber Talent Programme; Knowledge Series; QISP; Specialisation Certifications i.e. CREST; Special Interest Groups

Connect: Regional Ecosystem; Local Ecosystem; Corporate Partners; Academic Partners; Ladies in Cyber; Cybersecurity Awareness & Advisory Programme

Excel: AiSP Validated Security Professionals (AVIP); Cyber Security Awards; Student Volunteer Recognition Programme (SVRP)

Members

AiSP
ADVANCE | CONNECT | EXCEL
Faith Chng
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP
AiSP CAAP
Faith Chng

AiSP x Mastercard: Cybersecurity for SMEs on 24 Nov

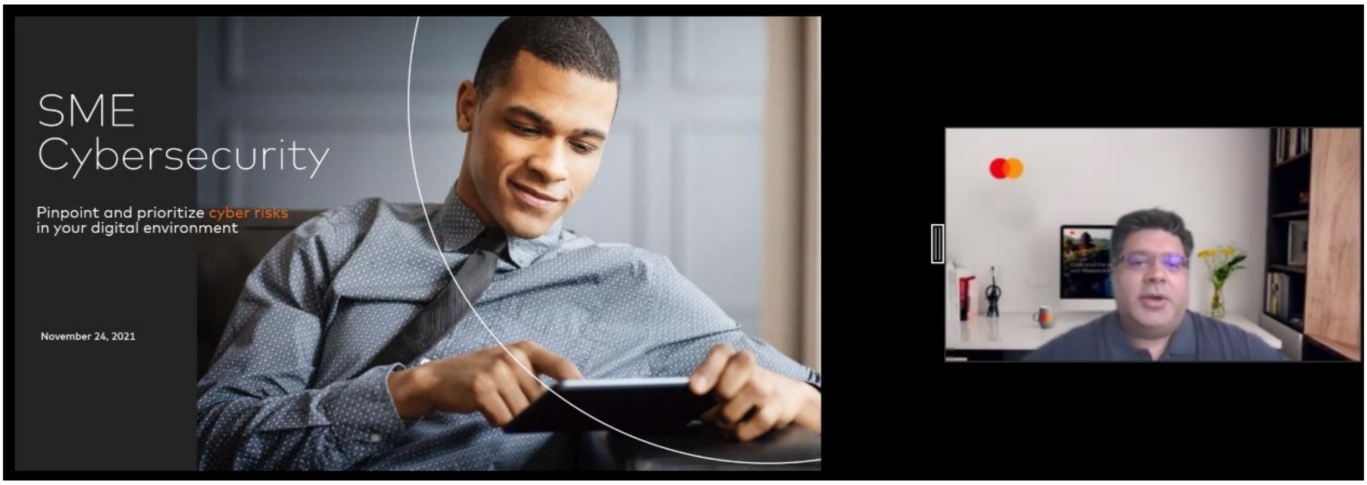
AiSP hosted a seminar for cybersecurity for SMEs on 24 November. We invited Tony Low, AiSP CAAP Lead, Veronica Low from Cyber Security Agency of Singapore - CSA as well as Urooj Burney from our Corporate Partner Mastercard.

Our speakers shared insights regarding topics such as responsibilities on data & privacy, cybersecurity for small businesses, as well as how small businesses can strengthen their cybersecurity. We ended the session with a fireside chat, moderated by Michael Lew from Rajah & Tann Technologies.

It was a fruitful session, and we are happy to have everyone join in this webinar. We hope to see you in our future events.

back to top

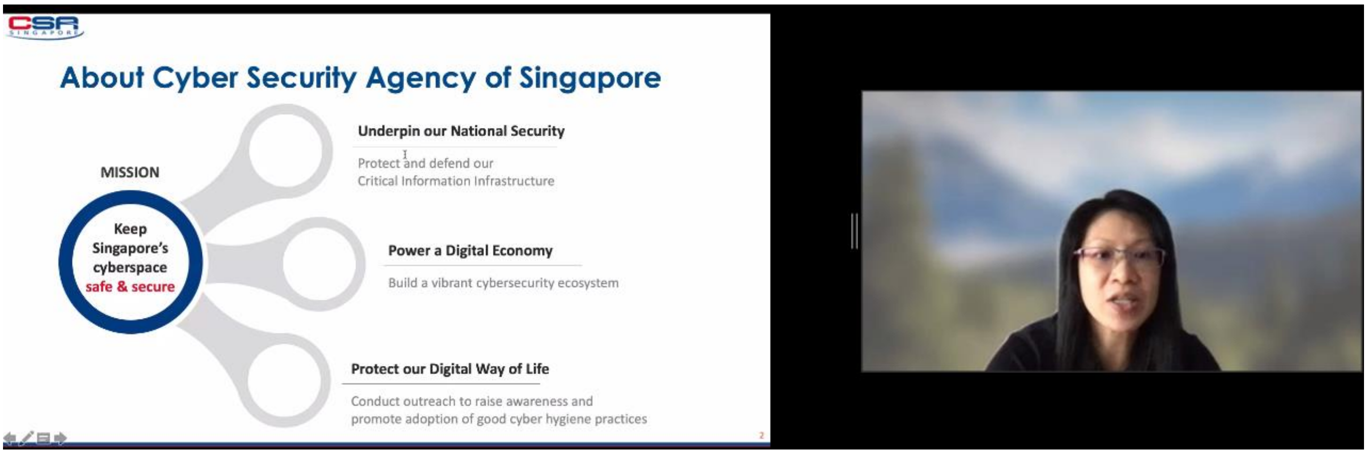
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP
Advance Connect Excel
CAAP
CYBERSECURITY AWARENESS & ADVISORY PROGRAMME



SME Cybersecurity

Pinpoint and prioritize cyber risks in your digital environment

November 24, 2021



About Cyber Security Agency of Singapore

MISSION

Keep Singapore's cyberspace safe & secure

Underpin our National Security

Protect and defend our Critical Information Infrastructure

Power a Digital Economy

Build a vibrant cybersecurity ecosystem

Protect our Digital Way of Life

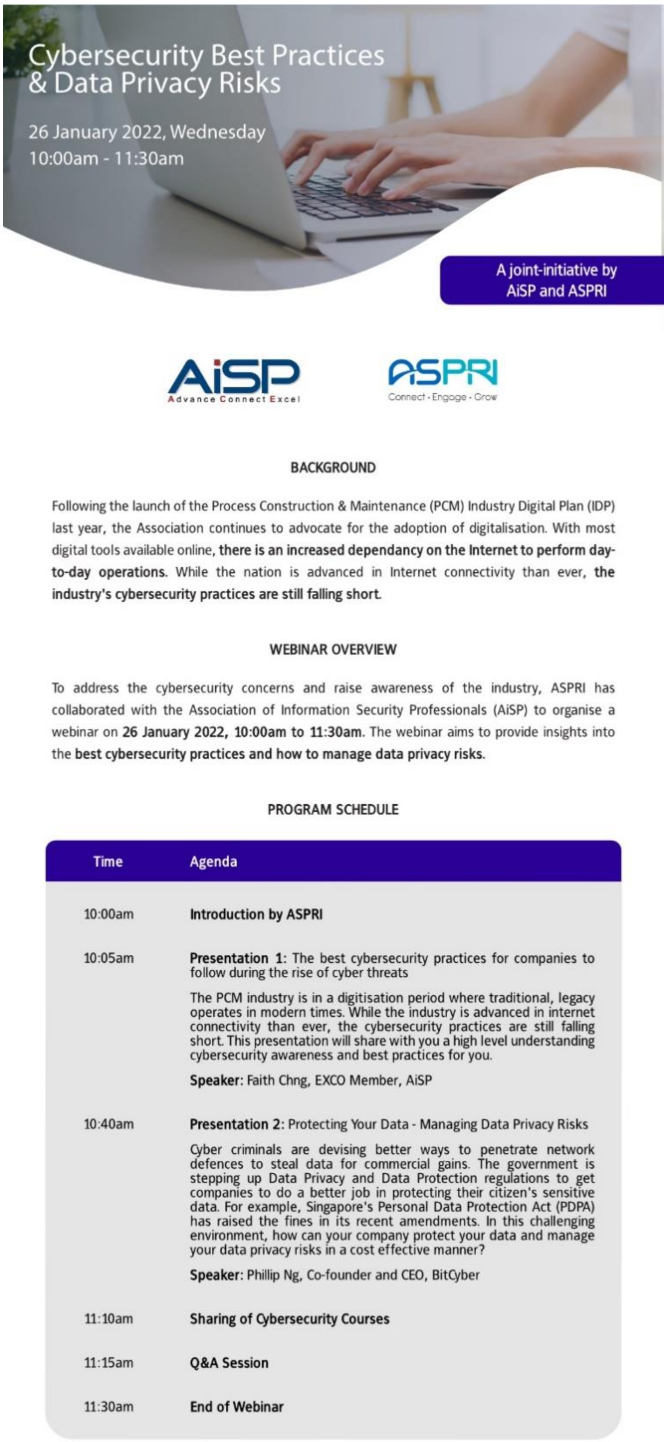
Conduct outreach to raise awareness and promote adoption of good cyber hygiene practices

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 ASPRI – Cybersecurity Best Practices & Data Privacy Risks



Cybersecurity Best Practices & Data Privacy Risks

26 January 2022, Wednesday
10:00am - 11:30am

A joint-initiative by AiSP and ASPRI

AiSP Advance Connect Excel

ASPRI Connect · Engage · Grow

BACKGROUND

Following the launch of the Process Construction & Maintenance (PCM) Industry Digital Plan (IDP) last year, the Association continues to advocate for the adoption of digitalisation. With most digital tools available online, **there is an increased dependancy on the Internet to perform day-to-day operations.** While the nation is advanced in Internet connectivity than ever, **the industry's cybersecurity practices are still falling short.**

WEBINAR OVERVIEW

To address the cybersecurity concerns and raise awareness of the industry, ASPRI has collaborated with the Association of Information Security Professionals (AiSP) to organise a webinar on **26 January 2022, 10:00am to 11:30am.** The webinar aims to provide insights into the **best cybersecurity practices and how to manage data privacy risks.**

PROGRAM SCHEDULE

Time	Agenda
10:00am	**Introduction by ASPRI**
10:05am	**Presentation 1:** The best cybersecurity practices for companies to follow during the rise of cyber threats The PCM industry is in a digitisation period where traditional, legacy operates in modern times. While the industry is advanced in internet connectivity than ever, the cybersecurity practices are still falling short. This presentation will share with you a high level understanding cybersecurity awareness and best practices for you. **Speaker:** Faith Chng, EXCO Member, AiSP
10:40am	**Presentation 2:** Protecting Your Data - Managing Data Privacy Risks Cyber criminals are devising better ways to penetrate network defences to steal data for commercial gains. The government is stepping up Data Privacy and Data Protection regulations to get companies to do a better job in protecting their citizen's sensitive data. For example, Singapore's Personal Data Protection Act (PDPA) has raised the fines in its recent amendments. In this challenging environment, how can your company protect your data and manage your data privacy risks in a cost effective manner? **Speaker:** Phillip Ng, Co-founder and CEO, BitCyber
11:10am	**Sharing of Cybersecurity Courses**
11:15am	**Q&A Session**
11:30am	**End of Webinar**

back to top

Speakers' Profiles

Ms Faith Chng
EXCO Member
AiSP

Faith is a mathematics NUS graduate with about 20 years of experience in IT and telecommunications industry handling sales, marketing and product. She has been handling cybersecurity product since 2012 with primary role in vendor management, product marketing and product management.

She has worked with managed security services provider and productised end to end services for enterprises. End to end cybersecurity services includes training, network and risk compliance assessments, managed security services, incident responses, holistic architecture design, consolidated IT Security solution, etc.

Mr Phillip Ng
Co-founder and CEO
BitCyber

Philip co-founded BitCyber with a vision to simplify cybersecurity in this age of digital transformation. An IT veteran who has built a successful career in cybersecurity and hybrid cloud technologies, Philip has held GM roles at public listed companies Achieva & Frontline, and senior sales leadership roles at MNCs Symantec, NetApp, British Telecom, Sun Microsystems, HP, and Unisys. He has also been an Angel investor since the Dot.Com period and is always on the lookout for promising young entrepreneurs.

Being a father of 3, Philip is naturally very concerned about the online dangers that children face in today's highly connected world of social media. Philip is making it his mission to make cyber defence accessible to every person and to promote cyber awareness to make the world a safer place.

Click here to register

AiSP SME Cybersecurity Conference

Business owners of small and medium enterprises (SMEs) and Enterprise are only focused on business needs and are not aware of the digital risks and cybersecurity resources available for them. The purpose of the AiSP SME Conference is to help Enterprises, SMEs and individuals to be more cyber aware and the different solutions out in the market that can help them in it.

back to top

Organised by the Association of Information Security Professionals (AiSP), the AiSP SME Conference is a unique event that brings together organisations to discuss the importance of being cyber aware and stay protected. The event will provide our speakers with the opportunity to share their experience, skills and knowledge to show how cybersecurity can help companies to stay protected. AiSP aims to elevate cybersecurity awareness among companies and establish a self-sustaining ecosystem with active participation from government agencies, business associations, cybersecurity communities, and solutions provider.

As part of AiSP Cybersecurity Awareness and Advisory Programme (CAAP), this event is for Singapore Enterprise and SMEs to know more about cybersecurity as a business requirement and how they can implement solutions and measures for cyber-resilience. CAAP hopes to elevate cybersecurity awareness as integral part of business owner's fundamentals and establish a self-sustainable support ecosystem programme with active participation from agencies, business associations, security communities and solutions provider.

Under CAAP, AiSP aims to launch the Cybersecurity Awareness e-learning which is based on the Cybersecurity Awareness and Advisory Programme (CAAP) Body of Knowledge to enhance digital and cyber awareness levels targeted at SME's and Individuals. AiSP also aims to launch the SME Cyber Safe portal to provide an online sitemap for Businesses & individuals in terms of Cyber Awareness Maturity Journey.

The conference will be held physically subjected to the COVID restrictions and government guidelines with the following details:

Date: 7January 2022 (Friday)
Time: 10:00 am – 4:00 pm
Venue: Lifelong Learning Institute

Join us to hear what our speakers have to say and provide on the solutions to help in your business and tour the Solution Booths and Cybersecurity Courses to find out more on Cybersecurity.

Secure your seat here: https://www.eventbrite.sg/e/168509655917
Visit https://www.aisp.sg/cyberfest/smeconf2021.html for more details.

back to top

Organised by

Supported by

Sponsors

Supporting Partners

Student Volunteer Recognition Programme (SVRP)

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. The third SVRP Awards Ceremony will be held on 19 January 2022 at Lifelong Learning Institute Event Hall.

The Awards Ceremony is sponsored by:

back to top

Singapore Cyber Security Inter Association (SCSIA)

Singapore Cyber Day 2021

8th November 2021 Career Advice Cyber Citizenship Singapore Cyber Day 2021	10th November 2021 COPYRIGHT Career Advice Cyber Ethics Singapore Cyber Day 2021	12th November 2021
15th November 2021 Career Advice Cyber Relationship Singapore Cyber Day 2021	17th November 2021 Career Advice Cyber Citizenship Singapore Cyber Day 2021	19th November 2021
22nd November 2021 ISACA ONE IN TECH Career Advice Cyber Use Singapore Cyber Day 2021	24th November 2021 Cyber Career Cyber Relationships Career Advice Cyber Relationship Singapore Cyber Day 2021	26th November 2021

The second inaugural Singapore Cyber Day was held on 8 November 2021. The Singapore Cyber Day aims to reach out to students in Singapore who are keen to find out more about cyber security and how they can be part of our community.

The Singapore Cyber Security Inter Association (SCSIA) consists of professional and industry associations: AiSP, Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Charter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)2 Singapore Chapter, SCS, SGTech and The Law Society of Singapore will be organising the second Singapore Cyber Day.

SCSIA aims to inspire future generation of youths on opportunities in Cybersecurity. They are reaching out to primary and secondary schools and pre-universities to talk about the

back to top

cybersecurity profession and how everyone can take part in Singapore's cybersecurity ecosystem and contribute towards our cyber resilience.

Video Link available here: https://www.youtube.com/watch?v=R9k67bOod54

Singapore Cyber Day Quiz 2021

Singapore Cyber Day Quiz will be held throughout the month of December for the students to take part in during the December school holidays. The online quiz competition is opened to primary, secondary and tertiary students (aged 25 years and below) in Singapore with the support from Cyber Security Agency of Singapore & Fortinet. This competition aims to pique interest in students and equip them with knowledge on Cyber Security. The quiz links will be available from the launch date onwards.

Week 1 Quiz – Launch on 1st Dec https://forms.office.com/r/uEVAxA3kzW	Week 2 Quiz – Launch on 8th Dec https://forms.office.com/r/fxCcfmAFZK
Week 3 Quiz – Launch on 15th Dec https://forms.office.com/r/YmB0fzLnb1	Week 4 Quiz – Launch on 22nd Dec https://forms.office.com/r/BRYNskzN53

Ladies in Cybersecurity

https://www.aisp.sg/ladies_about.html
NETWORKING | MENTORING | SPECIAL PROGRAMMES
LADIES IN CYBER
AiSP
Association of Information Security Professionals
'Ladies Talk Cyber' Series
December 2021 Edition
Interview of Ms Catherine Lee

Ladies Talk Cyber Series

For the Eighth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Catherine Lee, APAC Regional Senior IT Risk Management & Cybersecurity Specialist with expertise in Cybersecurity Governance, Risk and Compliance. She shared on her experiences as a cybersecurity specialist in various industries.

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

Catherine Lee is an APAC Regional Senior IT Risk Management & Cybersecurity Specialist with expertise in Cybersecurity Governance, Risk and Compliance. She has profound experience in leading cybersecurity maturity risk assessment and third party security risk assessment as well as driving cybersecurity transformation roadmap implementation for a wide range of industries including Pharmaceutical, FinTech, Oil & Gas, etc. to ensure necessary security due diligence is in place while enabling innovation.

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

back to top

AiSP Ladies in Cyber Learning Journey & Fireside Chat
21 January 2022 at CISCO Office (Hybrid Format)

Cybersecurity industry has always had an undeserved reputation of being a man's world. And there are quite a few reasons for the disproportionate number but arguably the main reason for it, is the lack of understanding of what women can do in an industry that's perceived to be tough and unforgiving. Yet, recent studies show that women are more likely to hold high-level roles in cybersecurity industry. It has also been proven that organizations advocating gender diversity tends to be more profitable.

AiSP has continuously initiate activities to inspire more women to join the force by engaging and educating students early, holding role-model pairings and hosting dialogues with notable women leaders and cybersecurity practitioners who can provide guidance and inspiration to the younger generation.

This September, **AiSP Ladies in Cyber** is organizing a hybrid fireside chat together with our Corporate Partner Cisco Systems. Join **SMS Sim Ann, Wendy, Catherine and Sherin** - our female leaders from Cybersecurity industry as they share their experience, advice and provide guidance on career in IT industry for females. Please email to secretariat@aisp.sg to find out more details on the event.

Date: 21 January 2022
Time: 7.30pm to 8.45pm (Please join in 5 mins before the session)
Sign up at https://tinyurl.com/lic24092021

back to top

JOINTLY ORGANISED BY:

SUPPORTED BY:

AS PART OF

SG CYBER WOMEN X SERIES

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

Ms Wendy Ng
Head of Cyber Security Sales, Singapore Cisco Systems

Ms Catherine Lee
Senior Specialist, Regional IT Risk Management & Security

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

AiSP Ladies in Cyber Inaugural Symposium on 18 March 2022

AiSP will be organising the inaugural Ladies in Cyber Symposium for the female Youths that highlights 4 different topics on cybersecurity, including the importance of cybersecurity, and how women can play a role in it. We are expecting 150 Youths and professionals (Subject to COVID-19 restrictions) at the event. The theme for this year Symposium is “**How can Women in Tech define the future of Cyber & Tech”.**

AiSP’s Vice-President and Founder for AiSP Ladies in Cyber Initiative, Ms Sherin Y Lee shared, “What we’re trying to do here is not to highlight women because they are women. Rather, we’re trying to amplify the message that women can and have been doing great work in cybersecurity – and by providing tangible examples. From any roles such as building companies, products & services, to technology security design and operations, all the way to incident response and recovery for organisations. The other message we’re trying to get out there is that cybersecurity is more than programming. There are diverse roles available – come join us to learn more about what you can do by interfacing with industry professionals from diverse roles in this sector.”

The event will be held on 18 March 2022 at Life-Long Learning Institute with Minister Josephine Teo as the Guest of Honour as part of International Women Day 2022. She will be having a dialogue session with the attendees during the event.

Visit https://www.aisp.sg/cyberfest/ladies_symposium.html for more details on the event. Contact AiSP Secretariat at secretariat@aisp.sg for more information of the event and if you sponsor and be part of it.

back to top

Supported by

CYBER YOUTH SINGAPORE

ENSIGN INFOSECURITY CONQUER THE UNKNOWN

Sponsors

Acronis

Checkmarx

CISCO

DBS

FORTINET

GOVTECH SINGAPORE

HUAWEI CLOUD Grow with Intelligence

IBM

Singtel Trustwave

ST Engineering

TANIUM

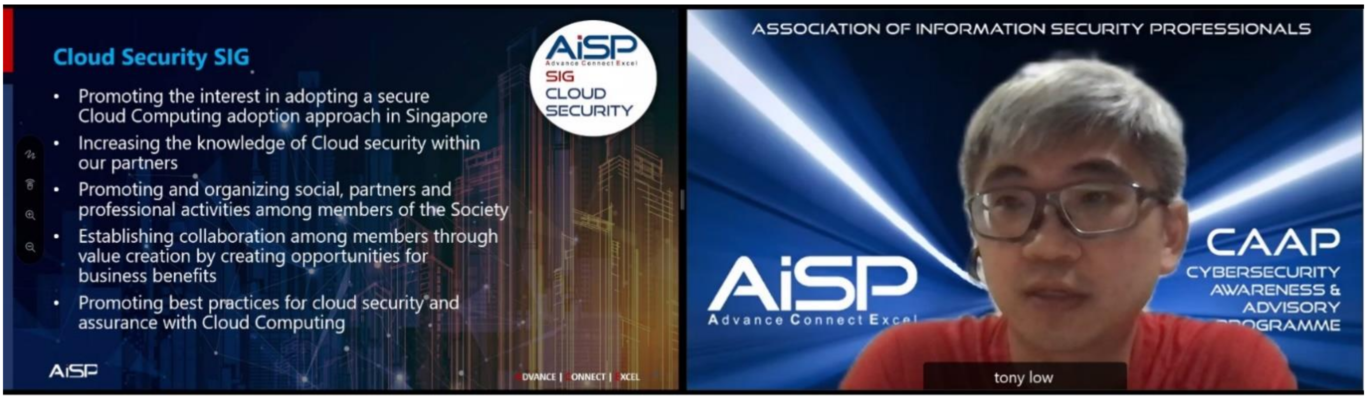
TREND MICRO

Women on Cyber

Special Interest Groups

Special Interest Group Day on 9 November

On 9 November, we invited the respective SIG Leads as well as Thomas Pan from CSCIS / Centre for Strategic Cyberspace + International Studies and Niel Pandya from Micro Focus. The speakers shared more about their SIG, namely Cloud Security, CTI, D&P and IoT. Thomas shared about the importance of IoT and Security while Niel shared regarding protection against ransomware. We hope everyone has a better understanding of each SIG, and how they can contribute.

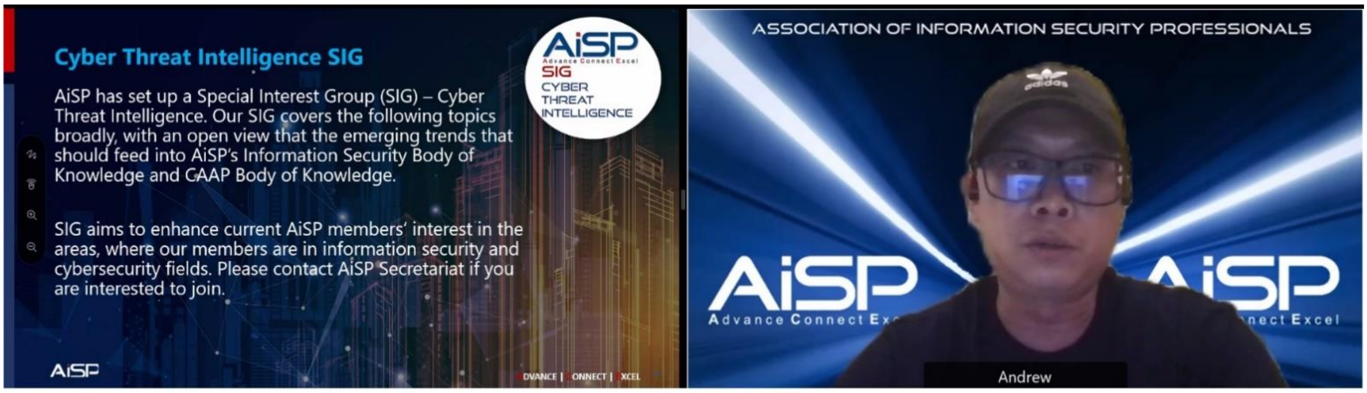


Cloud Security SIG

- Promoting the interest in adopting a secure Cloud Computing adoption approach in Singapore
- Increasing the knowledge of Cloud security within our partners
- Promoting and organizing social, partners and professional activities among members of the Society
- Establishing collaboration among members through value creation by creating opportunities for business benefits
- Promoting best practices for cloud security and assurance with Cloud Computing

AiSP SIG CLOUD SECURITY
AiSP
DVANCE | ONNECT | XCEL
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP Advance Connect Excel
CAAP CYBERSECURITY AWARENESS & ADVISORY PROGRAMME
tony low

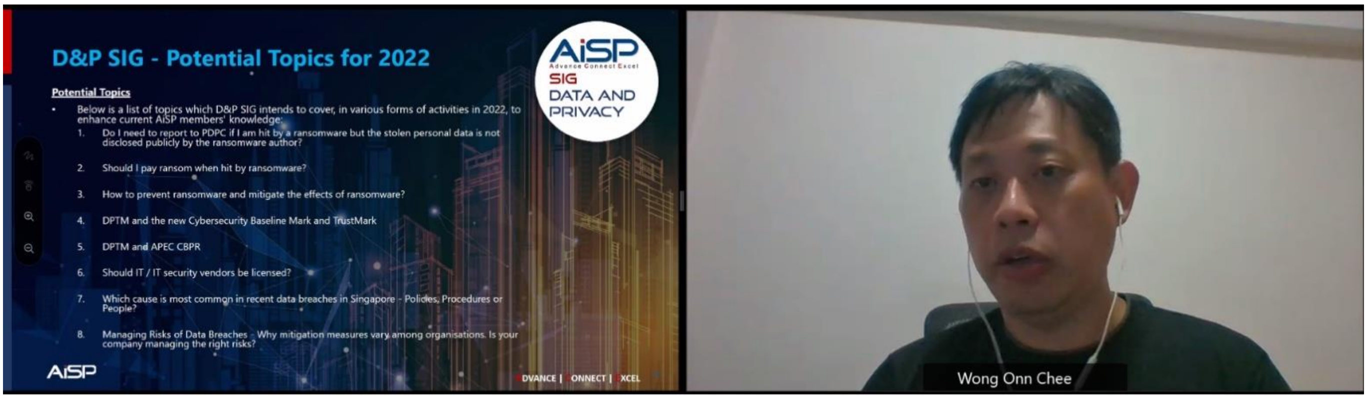
back to top



Cyber Threat Intelligence SIG

AiSP has set up a Special Interest Group (SIG) – Cyber Threat Intelligence. Our SIG covers the following topics broadly, with an open view that the emerging trends that should feed into AiSP's Information Security Body of Knowledge and CAAP Body of Knowledge.

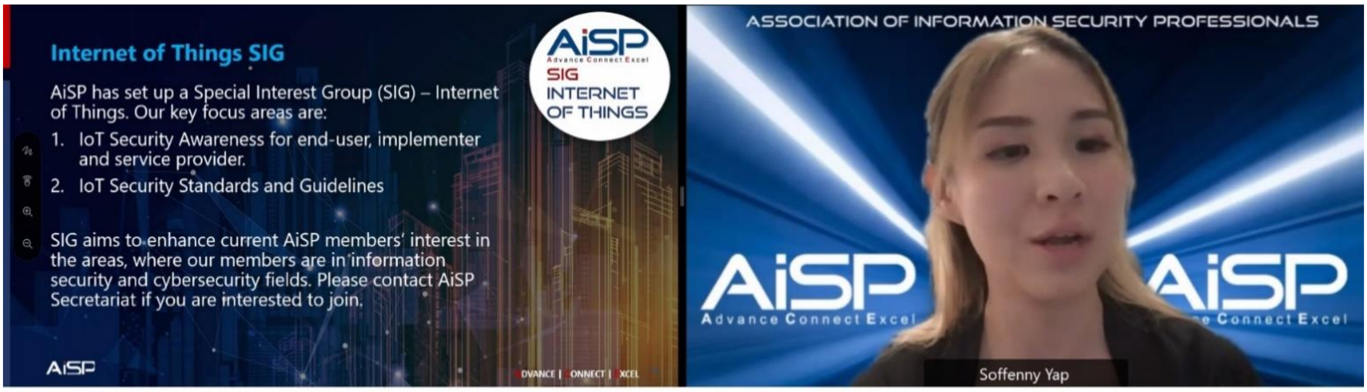
SIG aims to enhance current AiSP members' interest in the areas, where our members are in information security and cybersecurity fields. Please contact AiSP Secretariat if you are interested to join.



D&P SIG - Potential Topics for 2022

Potential Topics

- Below is a list of topics which D&P SIG intends to cover, in various forms of activities in 2022, to enhance current AiSP members' knowledge:
  1. Do I need to report to PDPC if I am hit by a ransomware but the stolen personal data is not disclosed publicly by the ransomware author?
  2. Should I pay ransom when hit by ransomware?
  3. How to prevent ransomware and mitigate the effects of ransomware?
  4. DPTM and the new Cybersecurity Baseline Mark and TrustMark
  5. DPTM and APEC CBPR
  6. Should IT / IT security vendors be licensed?
  7. Which cause is most common in recent data breaches in Singapore - Policies, Procedures or People?
  8. Managing Risks of Data Breaches - Why mitigation measures vary among organisations. Is your company managing the right risks?



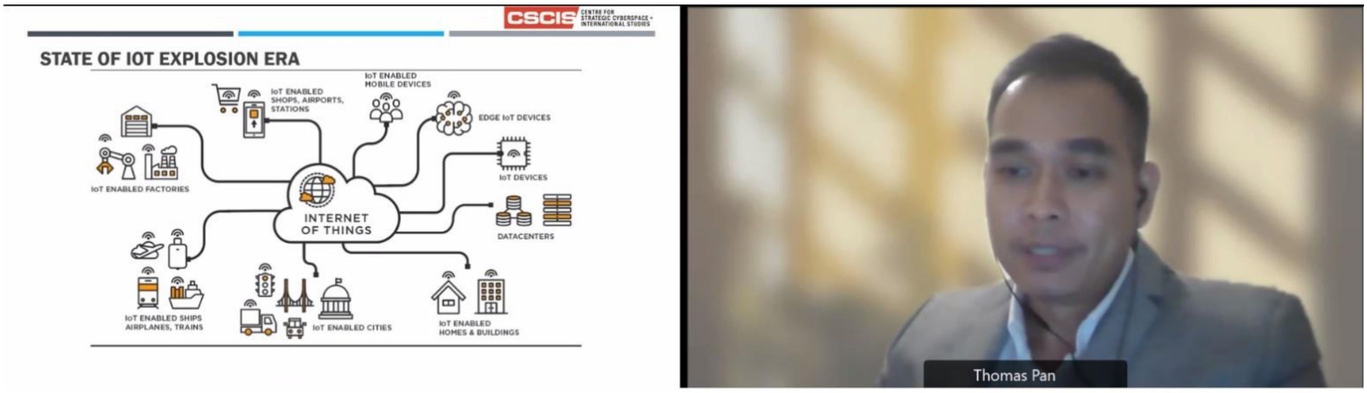
Internet of Things SIG

AiSP has set up a Special Interest Group (SIG) – Internet of Things. Our key focus areas are:

1. IoT Security Awareness for end-user, implementer and service provider.
2. IoT Security Standards and Guidelines

SIG aims to enhance current AiSP members' interest in the areas, where our members are in information security and cybersecurity fields. Please contact AiSP Secretariat if you are interested to join.

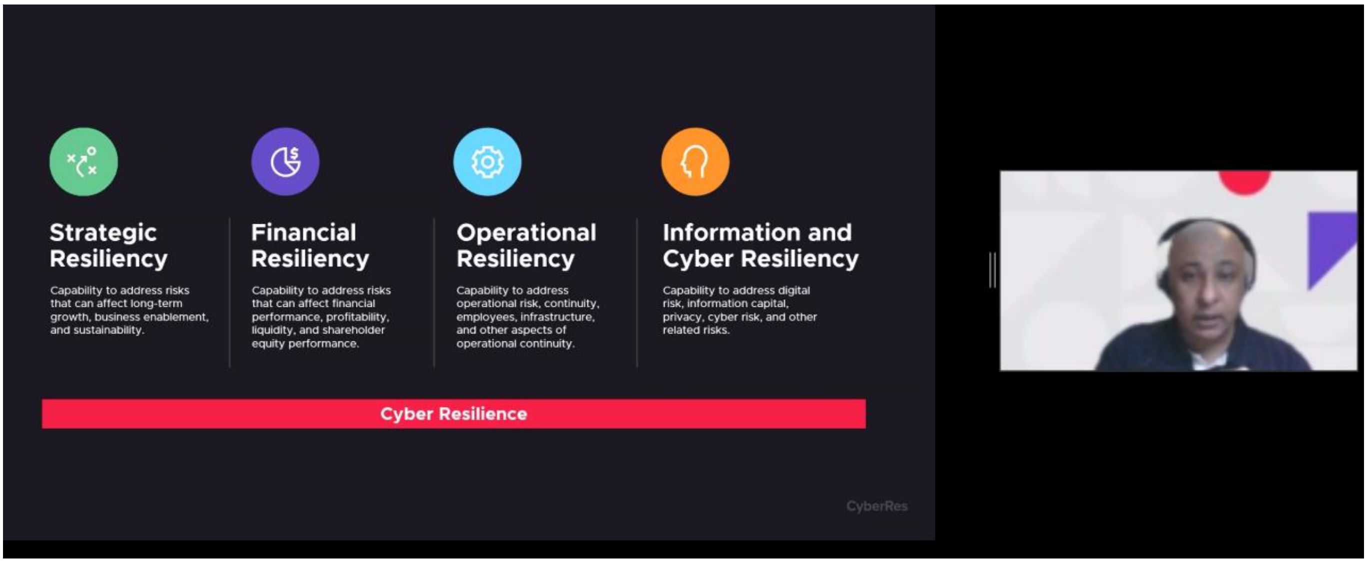
AiSP
Advance Connect Excel
SIG
INTERNET OF THINGS
AiSP
DVANCE | ONNECT | XCEL
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP
Advance Connect Excel
Soffenny Yap



STATE OF IOT EXPLOSION ERA

CSCIS
CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES
INTERNET OF THINGS
IoT ENABLED FACTORIES
IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS
Thomas Pan

back to top



Strategic Resiliency

Capability to address risks that can affect long-term growth, business enablement, and sustainability.

Financial Resiliency

Capability to address risks that can affect financial performance, profitability, liquidity, and shareholder equity performance.

Operational Resiliency

Capability to address operational risk, continuity, employees, infrastructure, and other aspects of operational continuity.

Information and Cyber Resiliency

Capability to address digital risk, information capital, privacy, cyber risk, and other related risks.

Cyber Resilience

CyberRes

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
- Cyber Threat Intelligence
- Data and Privacy
- 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

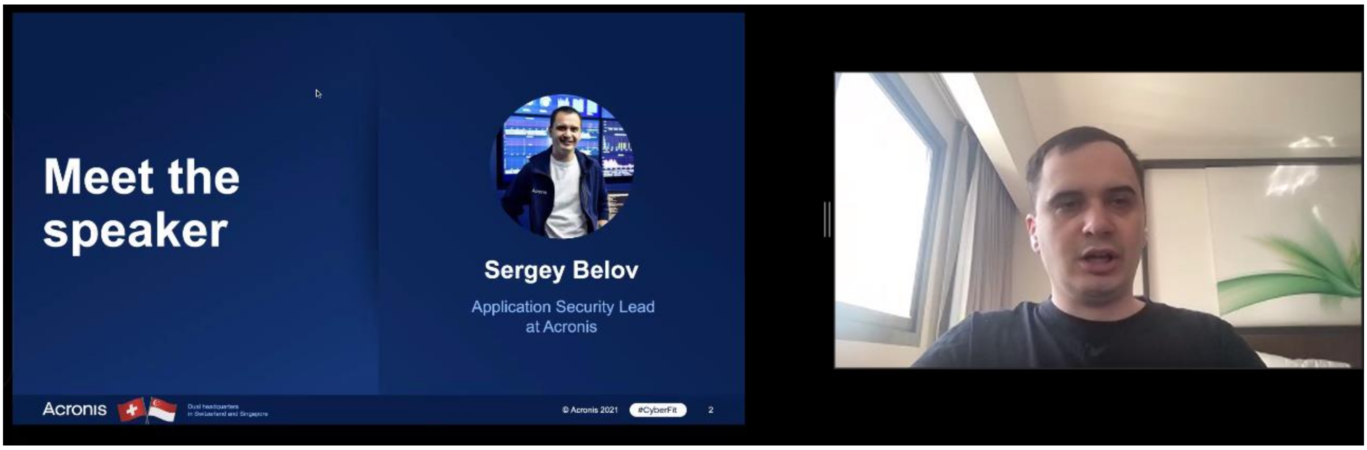
CREST Singapore

The CREST Singapore Chapter was formed by CREST International in partnership with CSA and AiSP to introduce CREST penetration testing certifications and accreditations to Singapore in 2016. Our CREST practical exam had resume on 26 August 2021. Please click here for the exam schedule for 2021.

back to top

Crest Webinar on 23 November

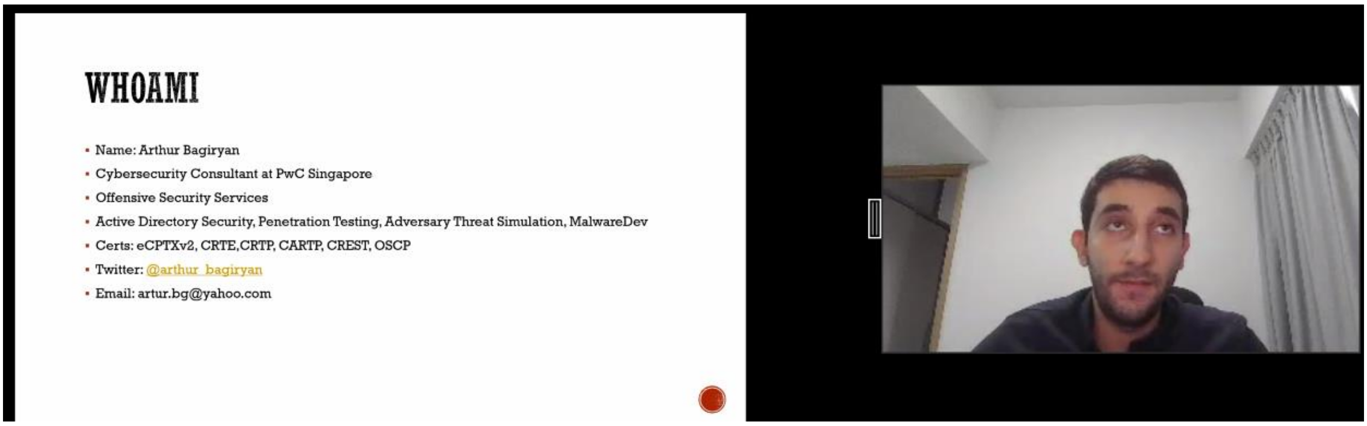
On 23 November, we had Arthur Bagiryan, member of AiSP and Sergey Belov from our Corporate Partner, Acronis joined us for Crest Webinar. We discussed about securing Azure AD and top mistakes of huge web-portals. We ended off the webinar with a Q&A session. We hope everyone who have attended are able to gain some insights into these topics.



Meet the speaker

Sergey Belov

Application Security Lead at Acronis



WHOAMI

- Name: Arthur Bagiryan
- Cybersecurity Consultant at PwC Singapore
- Offensive Security Services
- Active Directory Security, Penetration Testing, Adversary Threat Simulation, MalwareDev
- Certs: eCPTXv2, CRTE,CRTP, CARTP, CREST, OSCP
- Twitter: @arthur_bagiryan
- Email: artur.bg@yahoo.com

Regionalisation

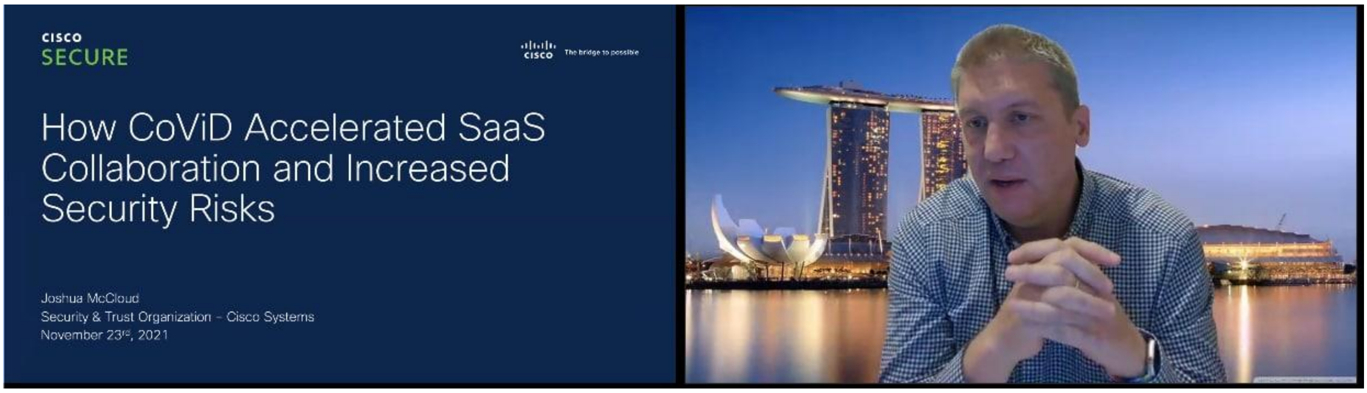
Cyber Leader Series on 23 Nov

Today's Cyber Leader Series was organised by AiSP and CyberTogether from Israel. In this session, we have Guy Segal and David Warshavski from Sygnia, and Shiran Kleiderman from Celsius. We are also joined by Joshua McCloud from our Corporate Partner Cisco Systems - Singapore, as well as Andre Shori from Schneider Electric. We ended the session with a round table discussion, moderated by Ron Moritz, Chairman of Cyber Together.

Our speakers shared insights regarding various topics including ransomware defence strategies, crypto ecosystem, SaaS collaboration and a day in the life of a CISO. We hope

back to top

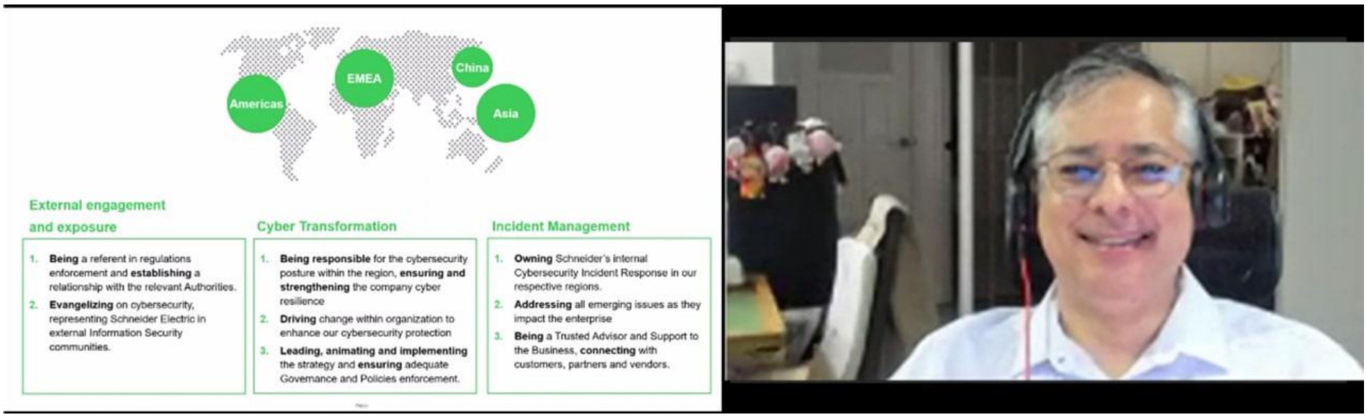
everyone enjoyed the session. We look forward to further collaborations and to see you again.



CISCO SECURE

How CoViD Accelerated SaaS Collaboration and Increased Security Risks

Joshua McCloud
Security & Trust Organization – Cisco Systems
November 23rd, 2021



External engagement and exposure

1. **Being** a referent in regulations enforcement and **establishing** a relationship with the relevant Authorities.
2. **Evangelizing** on cybersecurity, representing Schneider Electric in external Information Security communities.

Cyber Transformation

1. **Being responsible** for the cybersecurity posture within the region, **ensuring and strengthening** the company cyber resilience
2. **Driving** change within organization to enhance our cybersecurity protection
3. **Leading, animating and implementing** the strategy and **ensuring** adequate Governance and Policies enforcement.

Incident Management

1. **Owning** Schneider's internal Cybersecurity Incident Response in our respective regions.
2. **Addressing** all emerging issues as they impact the enterprise
3. **Being** a Trusted Advisor and Support to the Business, **connecting** with customers, partners and vendors.

Shiran Kleiderman
CYB OGETHER
Cyber Security Association
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP Advance Connect Excel
AiSP Advance Connect Excel

back to top

The Cybersecurity Awards

THE CYBERSECURITY Awards 2021

TCA 2021 nomination period has ended on **16 June 2021**. Thank you to all who have submitted the nominations.

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)

The Cybersecurity Awards 2021 winners will be announced at The Award Ceremony on 14 January 2022.

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

TCA2021 Sponsors & Partners

THE CYBERSECURITY Awards 2021
Organised by
AiSP
Supported by
CSA SINGAPORE
Supporting Associations
CSCIS
CSA cloud security alliance
HTCIA
ISACA Singapore Chapter
(ISC)² Official Chapter Singapore
Singapore 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
CSIT Centre for Strategic Infocomm Technologies
DBS
kaspersky
Singtel
wizlynx group
Silver Sponsors
PCS SECURITY
RSA
SIT Singapore Institute of Technology
THALES
wsg Workforce Singapore

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
1 Dec	Knowledge Series - CTI	AiSP
1 Dec	SINCON 2021 CXO Workshop	Partner
3 Dec	CyberCrimeCon2021	Partner
9 Dec	Micro Focus x SCW - Secure Code Tournement	Partner
7 Jan	**SME Cybersecurity Conference**	AiSP & Partner
14 Jan	**TCA Awards Ceremony 2021**	AiSP
19 Jan	**SVRP Awards Ceremony 2021**	AiSP
21 Jan	**LIC Learning Journey to CISCO**	AiSP & Partner
26 Jan	AiSP x ASPRI CAAP Workshop	AiSP & Partner
27 Jan	Knowledge Series – Data Security	AiSP & Partner
28 Jan	Cyber Day Quiz Prize Presentation	AiSP & Partner

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

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

Securing Cloud Strategies

Organisations in Singapore and around the world have adopted cloud computing as a key enabler of their digital transformation journey which was accelerated due to COVID-19 pandemic. Cloud computing offers various attractive benefits to organisations from IT maintenance cost reduction, system scalability and innovation enabling capabilities yet introduces cybersecurity and compliance challenges that to be addressed. With many high-profile breaches and leaks of sensitive data related to insecure cloud setup reported in recently months, companies are forced to re-evaluate their cloud readiness, architecture, and security.

The following five areas should be considered by organisations to better prevent future cloud data leaks

- Responsibility: In some cases, a “shared responsibility model” is not well defined between companies and partners in their cloud ecosystems, causing loopholes in business processes that eventually lead to security incidents in the cloud. In its simplest terms, the cloud shared responsibility model denotes that CSPs are responsible for the security of the cloud and customers are responsible for securing the data they put in the cloud. Depending

back to top

on the type of deployment—IaaS, PaaS, or SaaS—customer responsibilities will be determined. To build a shared responsibility model, organizations and vendors must clearly define each entity's responsibilities, work together to establish — and constantly update — business processes to minimize loopholes, and create mechanisms to help quickly identify and respond to cloud-related incidents in a collaborative way.

- Visibility: Having visibility over data and IT asset are the basic cyber hygiene and the only advantage of cyber security defenders against hackers. However, many companies have limited visibility into what applications are running in their cloud, what data they have there, and who has access to the data and applications.
  Organisations could consider existing technical solution such as a Cloud Access Security Broker (CASB) that can help increase your visibility into cloud activities. They can provide visibility into user actions and resource activities, and more importantly, what services are running and what data is at risk. Companies can track who did what, from where, and when it happened. Companies should consider gaining a greater understanding of their cloud environment using a cloud discovery tool; apply continuous monitoring and automation to discover the provisioning and de-provisioning of cloud resources; and locate where key assets are in the cloud and identify potential legal, compliance and privacy requirements.

- Governance: Business processes, policies and standards are yet to be designed to support the rapidly growing cloud landscape, taking into consideration the myriad industry, data privacy, and other requirements. The Personal Data Protection Act (PDPA), for example, introduces new and significant requirements such as breach notification. Various data privacy regulations also require data localization or restrict data transfer to certain jurisdictions.
  Security and its operating model should grow at the speed of business. The nature of the cloud dictates that each platform has to be treated differently to enable effective security and doing so effectively and at scale across multiple cloud providers. Cloud service provider-specific processes and policies should be built and the corresponding implementation and operations patterns should be defined. Companies should implement a strategic, enterprise-wide approach to overseeing, managing and securing vital data and how to do so in a multi-cloud environment.
- Secure Design: Security should be a conversation starting at the design phase. Building a cloud land zone which is defined as a configured environment with a standard set of secured cloud infrastructure, policies, best practices, guidelines, and centrally managed services plays big role. Having a defined secure landing zone could also help application teams get to cloud faster and security embedded.

  The following are key design elements to be considered for a secure landing zone
  - Multi-account approach to provide the highest level of resource and security isolation
  - Fine grain Role Based Access Control to support least privilege, separation of duties and data abstraction
  - Data protection utilizing encryption services provided by cloud vendors
  - Cyber-attack readiness taking advantages of cloud native services protecting common attacks on workloads
  - Centralized security monitoring for early detection and quick response

back to top

- Automation: Given the speed and elasticity of cloud operations, it is no longer possible to manually secure the cloud separately from DevOps. Companies should automate the deployment and operations aspects of the cloud, especially DevOps, by automating core security tasks, including secure orchestration and provisioning, vulnerability management, patch management, continuous integration and deployment, the security helpdesk, and security metrics generation and reporting.

With these steps, organizations can not only improve their cloud security, but help create a more resilient data system that can create competitive advantages in an increasingly digital world.

About the Author

Huynh Thien Tam
Secretary, AiSP

Tam is a cyber-security advisor with multiple years of experience on advising organisations across industries in Singapore and APAC region on cyber-security matters. Tam is currently a Managing Director of PwC's Cybersecurity practice in Singapore. Tam holds Offensive Security Certified Professional (OSCP), CREST Registered Penetration Tester and Certified Information Systems Security Professional (CISSP), GIAC Certified Forensic Examiner (GCFE) and GIAC Certified Forensic Analyst (GCFA). He gathered several hacking competition awards, reported zero-day vulnerabilities and spoke at various security events in the region.

Article from our CPP Partner, Mandiant

Mandiant Predictions for 2022

Steve Ledzian - VP, CTO – APJ, Mandiant

The rate of change across technology in general is blazingly fast, but the advancements in cyber security maybe even faster. Cyber security is an arms race between attackers and defenders, each seeing if they can outpace each other with the latest innovations. It's against this backdrop at the end of every year where cyber security vendors and experts try to cast their gaze into the future, beyond both what attackers and defenders are doing today, and try to predict what tomorrow will bring. 'Predictions' may pack more punch for the headlines, but in cyber security, the term 'forecasting' is perhaps more appropriate. That's because our expectations of the future are based on the trends we see now. And it's not just the attacker behaviors, we consider everything else, from technology and workplace trends to changing laws and regulations.

back to top

This year, Mandiant released its Predictions Report 2022 and called out 14 predictions to consider for year ahead. We'll take a focused look at a few of the predictions in this article. If you're interested in the full report, you can access it here and if you'd like to observe an on demand briefing of the report here.

Ransomware and Multifaceted Extortion - No End in Sight: Increased Frequency and Expanding Tactics

Every recent Mandiant predictions report has included a section on ransomware. This year is no exception; in fact, our outlook on the threat for 2022 is perhaps more grim. Ransomware actors are becoming increasingly aggressive, turning these once relatively simple attacks into more elaborate—and lucrative—multi-faceted extortion operations. What we're seeing are attackers who are already technically-savvy learning to become more business-savvy. With each attack, they've been learning where the pressure points are the businesses most sensitive to. They combine multiple points of leverage simultaneous in trying to force the victim into doing what no victim wants to do - pay the extortion/ransom. Going further than just encrypting files, attackers are now shaming victims by turning what used to be a quiet service disruption into a public breach. Attackers are trying to recruit insiders to gain initial entry into victim networks, threatening DDoS attacks, and promising to sell off the stolen data of victims who don't pay. Attacker creativity in finding new ways to add even more pressure to an already difficult situation for victims will continue in 2022.

More Public Breaches in the Asia-Pacific and Japan (APJ) Region

Historically, breaches in the APJ region have on only very rare occasions been made public, but that is likely to change in 2022 as multi-faceted extortion becomes more prevalent. In the past, making the public aware of a breach benefitted neither the attacker nor the victim organization. The attackers wanted to stay invisible for as long as possible, hoping to maintain their access to victim networks for extended periods of time. Victims wanted to avoid the reputational damage, financial impact and other consequences that come from a breach. Multi-faceted extortion has changed all that. Now attackers are simply threatening to expose breaches and publish sensitive data to increase the urgency to pay. APJ organizations must be ready to deal with these types of extortion operators, but unfortunately, many organizations in the region lack experience with these types of threats, or don't yet take them seriously. Therefore, we expect to see a lot more breaches of APJ organizations being made public by attackers in 2022.

Deepfakes : Not just for information Operations

When nation states engage in "fake news", it's often less about whether that message is true or false and more about inauthentically making that message appear as if it came from a source that it didn't actually come from. Typically, the goal is to stoke division and ultimately, destabilize. These black propaganda efforts date back to long before the Internet and were used in WWII, just over radio rather than the social media. What has stayed consistent though is that a key characteristic of this type of information is inauthenticity. When it comes to inauthenticity, it's hard to imagine a better tool than the deepfake. Convincing video or audio of a person doing or saying something they never did or say is the holy grail for the actors behind information operations.

Not to be left out, financially motivated cyber criminals have started taking advantage of this new technology. Organizations are catching on to the Business Email Compromise (BEC) scams which have allowed attackers to steal millions of dollars without using any malware at all. Organizations have stepped up procedures to validate requests that come in over email to change an account number before payment by confirming authenticity with a phone call. Enter cyber criminal deep fakes. In 2019, the Wall Street Journal detailed one such case where a CEO's voice was replicated to increase the appearance of a scam's authenticity. A second case happened in 2021 covered by Forbes which netted attackers a much larger theft.

Ultimately you can characterize hacking as taking a technology and using it in creative ways that it was never intended for or architected for. The hacking mindset will persist and in 2022, we'll see the playground for this creativity only get bigger.

For more information, reach us at APJ@mandiant.com or visit, www.mandiant.com.

back to top

Article from our CPP Partner, Cybint

From Starting to Thriving in Cyber

Aaron Ang
APAC Project Manager and Trainer,
ThriveDX SaaS (formerly Cybint)

It was the year 2013. I had just graduated from university and was standing in front of a class of forty students, most of whom were in the fourth grade. It was the start of my first career as a language teacher in an elementary school in the northern part of Singapore. Much has changed since then.

After about three years as a classroom teacher, I took on a role at the Information Technology Division (ITD) of the Ministry of Education (MOE) in Singapore, where I provided consultancy to the Ministry and our local schools on cybersecurity risk management, compliance and governance, as well as conducted cybersecurity workshops and awareness programmes for both adult staff and students. I spent five fulfilling years at MOE ITD and was subsequently given the opportunity to work at the Cyber Security Agency of Singapore (CSA), a government agency tasked to protect Singapore's cyberspace.

Today, I'm the APAC Project Manager and Trainer at ThriveDX SaaS (formerly Cybint), and part of my job involves teaching adults who are eager to take on a career in cybersecurity. Having personally experienced what a mid-career switch to cybersecurity is like, I find myself being able to relate to the struggles of many who have embarked on this journey. When asked why I took the plunge in the first place, I often share (half-jokingly) that interacting with computers is much less stressful than interacting with fourth graders. Yet one thing is for sure – I have enjoyed the journey thus far.

Increasing demand for cybersecurity professionals worldwide

Amidst the global COVID-19 pandemic, where the world has seen a severe lack of physical resources and human capital, a challenge of a different form is brewing in cyberspace. Multiple studies have reported that the global cybersecurity workforce needs to grow at an exponential rate just to meet the demands of the industry.

In the beautiful city of Singapore where I call home, the Cyber Security Agency of Singapore (CSA), a governmental agency given the task of protecting Singapore's cyberspace, estimated a talent shortage of 3,400 cybersecurity professionals in 2020.

Sometime in the year 2020, as part of my stint at the Cyber Security Agency of Singapore (CSA), I had the opportunity to embark on a deep-dive of Singapore's cybersecurity manpower landscape. It was the height of the pandemic and we were really trying to tackle cybersecurity's two greatest threats: solving the talent shortage and closing the skill gaps. I spent a year studying policies, programmes, reports and data, and spoke to executives and hiring managers of cybersecurity companies, both local and abroad.

Here's what I learnt:

Having a cybersecurity certification does not guarantee employment

Just do a quick search on adult learning and IT-related certifications in Singapore. You will realise that cybersecurity certifications are one of the most popular adult learning courses here. Yet, why are cybersecurity companies still facing a talent shortage and why aren't people getting employed?

One of the points that really stood out in my conversations with executives and hiring managers is that job-seekers with cybersecurity certifications do not necessarily have the practical, real-world technical skills that companies require. Most cybersecurity companies require potential candidates to pass a skills-based examination to demonstrate their technical capabilities as part of the recruitment process and unfortunately, studying for a paper-based certification is very different from responding to an attack in real-time.

Knowing how to communicate an attack is just as important as knowing how to stop an attack

back to top

Cybersecurity professionals do not work in an underground basement with a hoodie on and a box of pizza by the side. In large organizations especially, cybersecurity professionals are required to communicate with various stakeholders and “speak the lingo”. Getting a solution approved by your board and giving instructions to your vendor to implement the solution require very different sets of lexicon. Executives appreciate it when technical information is presented in a clear and concise manner that is easy to understand.

This is where previous work experience counts. Mid-career professionals, who bring with them a wealth of experience from their previous roles, are often better able to find their way around the corporate boardroom. Unlike technical skills which can be easily learnt, communication and people skills require experience and time to hone.

Being a part of a community makes the journey easier

“If you want to go fast, go alone. If you want to go far, go together” – African proverb

As part of my job at ThriveDX SaaS (formerly Cybint), I’ve had the chance to conduct workshops, awareness talks and webinars. I always enjoy watching the expressions on others’ faces when I share that my first job was a language teacher in a local primary school.

As I transited from a career in teaching to a career in cybersecurity, I had opportunities to learn from others within the cybersecurity community. Most were willing to share their knowledge, skills and stories. The community kept me going when things got tough.

Last year, I had the honour of carrying on this tradition by starting a Discord server for youths who are interested in cybersecurity and mentoring those who are interested in embarking on a career in cybersecurity. We now have more than 300 youths in the server, many of whom have picked up skills in the domains of red teaming, blue teaming and OSINT that can rival seasoned cybersecurity practitioners.

Traits of a good cybersecurity practitioner

Unlike some fields of Information Technology, following documentation and manuals to the letter simply doesn’t cut it in cybersecurity. Cybersecurity practitioners are often required to think out of the box and innovate on their feet. Malicious actors and cyber criminals do not play by the rules. Outsmarting them therefore requires a high level of situation awareness, as well as a keen sense of curiosity and “street intelligence”.

Looking back, it has been about 7 years since I took on my first cybersecurity project. Yet each day in the job is an opportunity for continuous and lifelong learning. The cybersecurity landscape is constantly evolving. New threats are always on the horizon. This is an industry where a willingness to continually adapt, evolve and upskill oneself is essential.

Ready to launch your career in cybersecurity?

So, think a career in cybersecurity is for you?

The Cybersecurity Bootcamp powered by ThriveDX SaaS (formerly Cybint) is an accelerated training program designed to successfully prepare people with little or no background in IT for entry-level jobs in cybersecurity, a highly in-demand and promising career path.

Developed around military training methodologies and hands-on learning, the program focuses on the key skills sought by employers. The Bootcamp prepares you not only with technical knowledge, but also with the essential practical and soft skills necessary for a successful career in cybersecurity.

Our Bootcamp includes:

- Accelerated Program

back to top

The Bootcamp was developed under the principle of "everything you need to know, and only what you need to know." Our accelerated learning methodology and streamlined curriculum focus on teaching you the specific skills you will need for the job market. The Bootcamp also includes ongoing access to our online learning platform after graduation, including content updates covering emerging cyber threats and tools.

- Hands-on Skills Training

To ensure you get to practice what you learn, we have developed over 60 unique labs and over 100 different exercises. Technical skills, frameworks, and tools are taught through hands-on exercises in a safe virtual environment.

- Career Services and Support

Essential soft-skills training, from teamwork to interview prep, is embedded throughout the program. Upon graduation, you will also connect to a global alumni network and community.

About the Author

Aaron Ang (linkedin.com/in/aaronangsg/) is the APAC Project Manager and cybersecurity trainer at ThriveDX SaaS (formerly Cybint). Prior to joining ThriveDX SaaS (formerly Cybint), Aaron was part of the Cyber Security Agency of Singapore (CSA), a government agency tasked to protect Singapore's cyberspace.

Aaron is an experienced cybersecurity practitioner who has had the opportunity to work with veterans in the industry, both in the public and private sector. He has provided training and consultancy services to organizations worldwide to help them patch the weakest link in cybersecurity - the human firmware.

He also volunteers as a career mentor for youths and students who are looking to embark on a career in cybersecurity.

About ThriveDX SaaS (formerly Cybint)

ThriveDX Formerly Cybint

ThriveDX SaaS (formerly Cybint) is a global cyber education company with a commitment to reskilling and upskilling in cybersecurity. We tackle the industry's two greatest threats: the workforce shortage and the skills gap. Our solutions were developed by a team of military cyber experts, industry professionals, and educators under the vision of creating a safer digital world through education, training, and collaboration.

Article from our Event Sponsor, Data Terminator

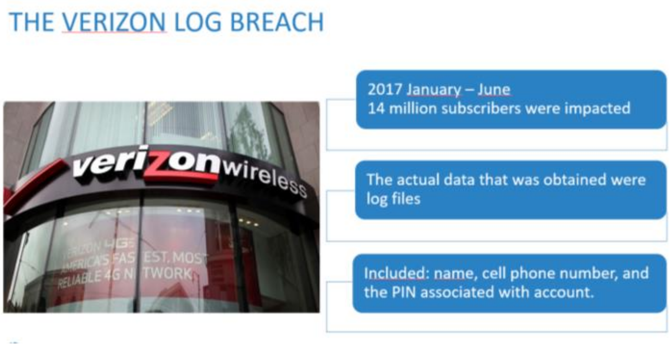
An Indispensable Tool for Cybersecurity

In today's fast changing world of cybersecurity technologies, log management is boring. Syslog started way back in 1980's as part of the Sendmail project. Log messages can be used for security analysis, system/operational management, debugging and compliance.

back to top

In those days, there were not so many systems/devices connected to an organization's network. The EPS (events per second or number of log messages per second) count for each network was low. At the same time, logs collected were primarily for system/operational management or troubleshooting purposes. Losing a few logs here and there was not a big deal. It was also unlikely that anyone would bother to "steal" log information since it was not perceived to be of value to external parties.

In today's highly interconnected world with an almost infinite number of connected devices, the requirements have totally changed. Log management systems are now required to handle enormous amounts of information with EPS of a typical network easily in the 10,000-100,000 range. At the same time, log information has become a target of cyber theft (see picture right). Finally, log messages form the primary and key type of data input for SIEM (security information and event management) systems, which sit at the heart of a modern SOC (security ops center).


THE VERIZON LOG BREACH

2017 January – June
14 million subscribers were impacted

The actual data that was obtained were log files

Included: name, cell phone number, and the PIN associated with account.

Such security systems are typically very costly and while very effective for security analysis, are not the ideal pl
to store logs for compliance and/or incident response purposes.

This is where **syslog-ng** comes in. The **syslog-ng** project was started in 1998 by Balázs Scheidler. It has since been developed into an enterprise grade, highly secure and scalable log management tool trusted by top enterprises and government organizations around the world.
Key features of **syslog-ng** that feed its popularity include:

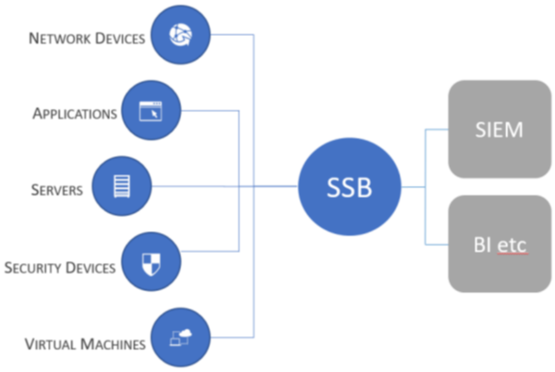
- Highly efficient code base able to scale up to 500,000 EPS per instance
- Encrypted transmission of log messages
- ALTP (advanced log transfer protocol) combined with flow control and reliable disk buffering minimizes any log loss during transmission
- Encrypted and tamper proof log store to protect from unauthorized viewing and alteration
- Cost effective licensing based on number of log sources, not volume of logs
- Ability to collect from all common log sources like Windows/Linux servers, applications, network/security devices using the RFC3164 and/or RFC5424 log message standards

Ability to feed to all commonly used SIEMs/analytics systems like Splunk, QRadar, Arcsight, Hadoop etc

The **syslog-ng** Store Box (SSB) is a hardware or virtual appliance version of **syslog-ng** with a web-based GUI. It allows lightning quick searching and viewing of logs with minimal operational and maintenance issues. This is currently very popular for the compliance use case (eg CII) as well as a unfiltered log store for incident response purposes.
A typical deployment architecture can be found in the diagram.

DT Asia is the authorized **syslog-ng** distributor for the region.

Contact us at enquiry@dtasiagroup.com for more information.

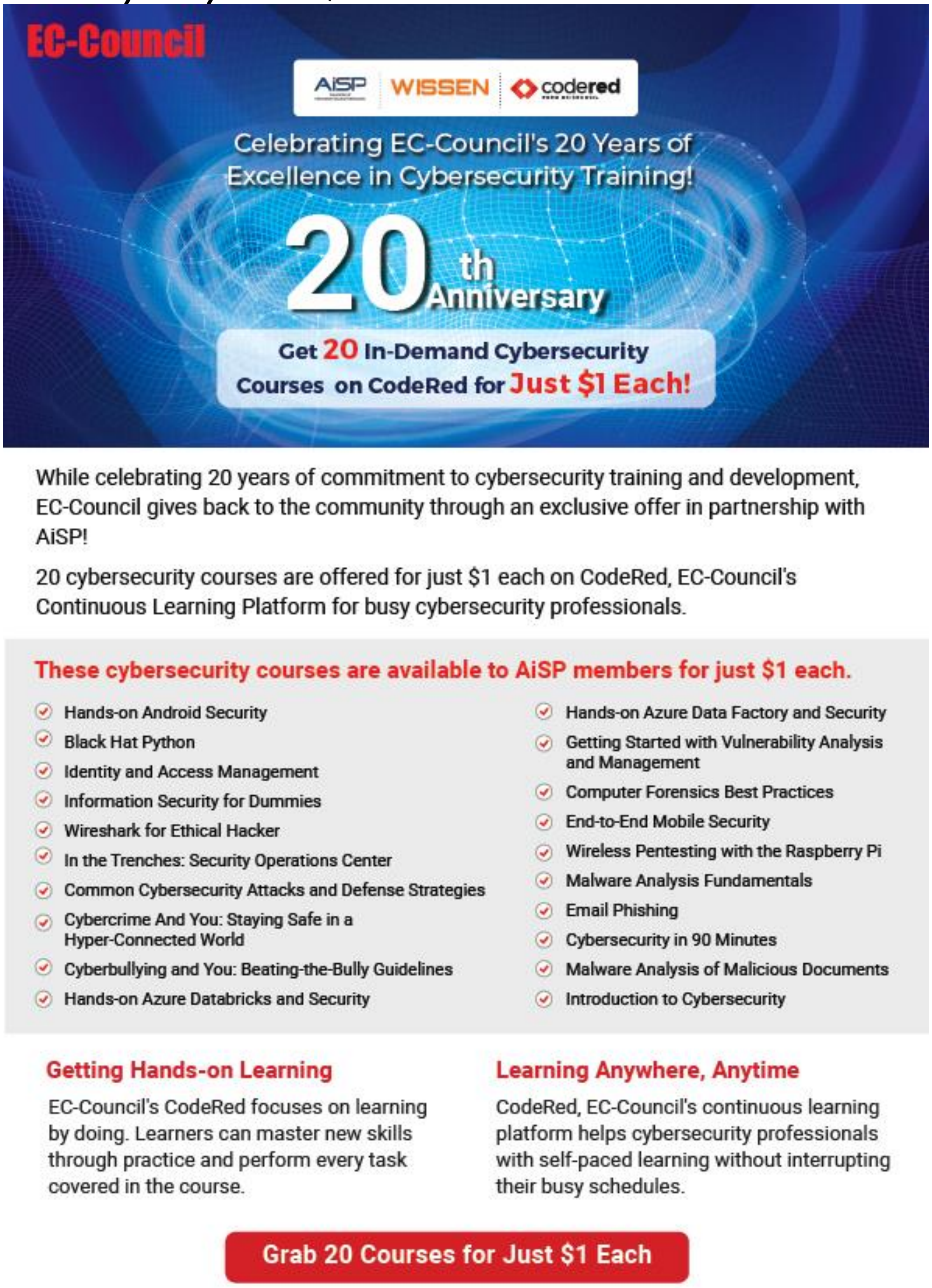


back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

Get 20 in-demand cybersecurity courses from CodeRed for just USD $1 each! Brought to you by Wissen, EC-Council Exclusive Distributor!



EC-Council

AiSP | WISSEN | codered

Celebrating EC-Council's 20 Years of Excellence in Cybersecurity Training!

20th Anniversary

Get 20 In-Demand Cybersecurity Courses on CodeRed for Just $1 Each!

While celebrating 20 years of commitment to cybersecurity training and development, EC-Council gives back to the community through an exclusive offer in partnership with AiSP!

20 cybersecurity courses are offered for just $1 each on CodeRed, EC-Council's Continuous Learning Platform for busy cybersecurity professionals.

These cybersecurity courses are available to AiSP members for just $1 each.

- ✓ Hands-on Android Security
- ✓ Black Hat Python
- ✓ Identity and Access Management
- ✓ Information Security for Dummies
- ✓ Wireshark for Ethical Hacker
- ✓ In the Trenches: Security Operations Center
- ✓ Common Cybersecurity Attacks and Defense Strategies
- ✓ Cybercrime And You: Staying Safe in a Hyper-Connected World
- ✓ Cyberbullying and You: Beating-the-Bully Guidelines
- ✓ Hands-on Azure Databricks and Security
- ✓ Hands-on Azure Data Factory and Security
- ✓ Getting Started with Vulnerability Analysis and Management
- ✓ Computer Forensics Best Practices
- ✓ End-to-End Mobile Security
- ✓ Wireless Pentesting with the Raspberry Pi
- ✓ Malware Analysis Fundamentals
- ✓ Email Phishing
- ✓ Cybersecurity in 90 Minutes
- ✓ Malware Analysis of Malicious Documents
- ✓ Introduction to Cybersecurity

Getting Hands-on Learning

EC-Council's CodeRed focuses on learning by doing. Learners can master new skills through practice and perform every task covered in the course.

Learning Anywhere, Anytime

CodeRed, EC-Council's continuous learning platform helps cybersecurity professionals with self-paced learning without interrupting their busy schedules.

Grab 20 Courses for Just $1 Each

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

Date 13-17 December 2021
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

Register your interest here: https://forms.office.com/r/Ab0MKfgQXg

*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

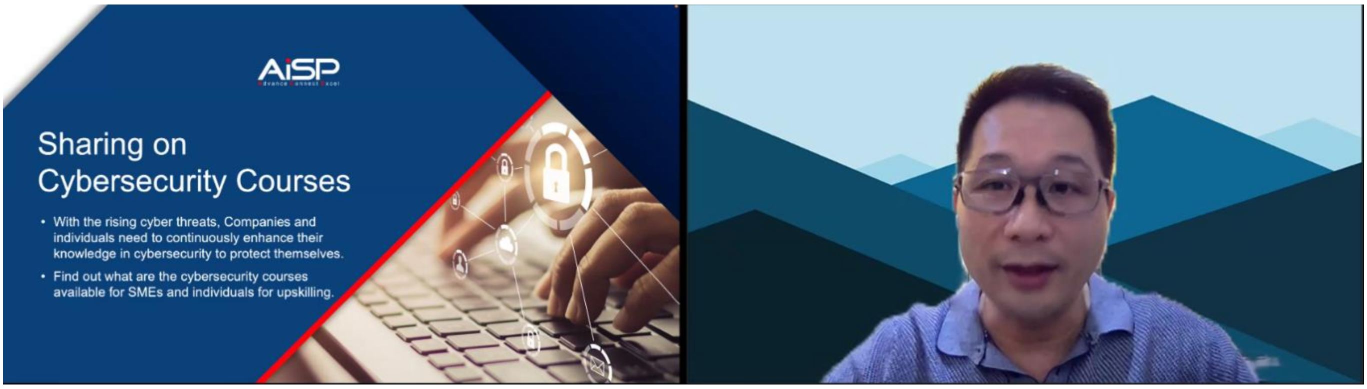
NETASSIST

back to top

Cybersecurity Essentials Course

Essential Course Briefing on 8 November

Our Training Partner, Mr Nicholas Yong from Transformist did a comprehensive sharing on our Essential Course for cybersecurity. He shared the modules that will be covered in the course and our AiSP Certification Road Map.



Sharing on Cybersecurity Courses

- With the rising cyber threats, Companies and individuals need to continuously enhance their knowledge in cybersecurity to protect themselves.
- Find out what are the cybersecurity courses available for SMEs and individuals for upskilling.

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.

back to top

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

Course Objectives

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

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

COURSE DETAILS

Date: TBC
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

Transformists NETWORK

Delivery Partners

Ai Network 360

OPUS ACADEMY

NETASSIST

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: 2020\1 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) to apply for AVIP.

Your AiSP Membership Account
AiSP has moved its digital membership to Glue Up, previously known as Event bank, an all-in-one cloud platform for event and membership management. You can access your digital membership via the **web portal** or the mobile application (**App Store**, **Google Play**), using the email address you have registered with AiSP.

The platform allows our members to sign up for events and voluntary activities and check membership validity.

Membership Renewal
Members will receive an auto-generated email from Glue Up and it will send the reminder 1 month before the expiry date of your membership. Members can renew and pay

back to top

directly with Glue Up or one of the options listed here. We will be adding GIRO (auto - deduction) this year. 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

MINDEF SINGAPORE

NUMEN

Privasec

RAJAH & TANN CYBERSECURITY

Responsible Cyber

SecurID An RSA Business

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

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.

AiSP
Advance Connect Excel

🌐 www.AiSP.sg
✉ secretariat@aisp.sg
☎ +65 8878 5686
📍 116 Changi Road, #04-03 WIS@Changi, S419718
Our office is closed. *We are currently telecommuting.*
Please email us during office hours.

back to top