AiSP

NEWSLETTER

October 2021

NEWS & UPDATE

New Corporate Partners

AiSP would like to welcome **Insightz Technology** and **Mastercard** as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

INSIGHTZ TECHNOLOGY

New Listing Partners

AiSP partnered with **ALC Group** and **EC Council** to introduce new training and certifications for members to contribute to the Cybersecurity Ecosystem in 2021.

For listing enquiries please contact secretariat@aisp.sg

alc

EC-Council | WISSEN

Personal Data Protection Seminar 2021

Personal Data Protection Seminar 2021 was held virtually on 14 September. The event had a panel of distinguished speakers and AiSP Secretary Mr Tam Huynh was in the panel who shared insights on Data Breaches - Not if, But When.

The 1-week long event had a series of interesting workshops and seminars on the theme "Driving a Data Driven Culture".

PERSONAL DATA PROTECTION SEMINAR 2021
Driving a Data Driven Culture
pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE
In support of
IMDA INFOCOMM MEDIA DEVELOPMENT AUTHORITY
SG:DIGITAL
PDP Secretariat

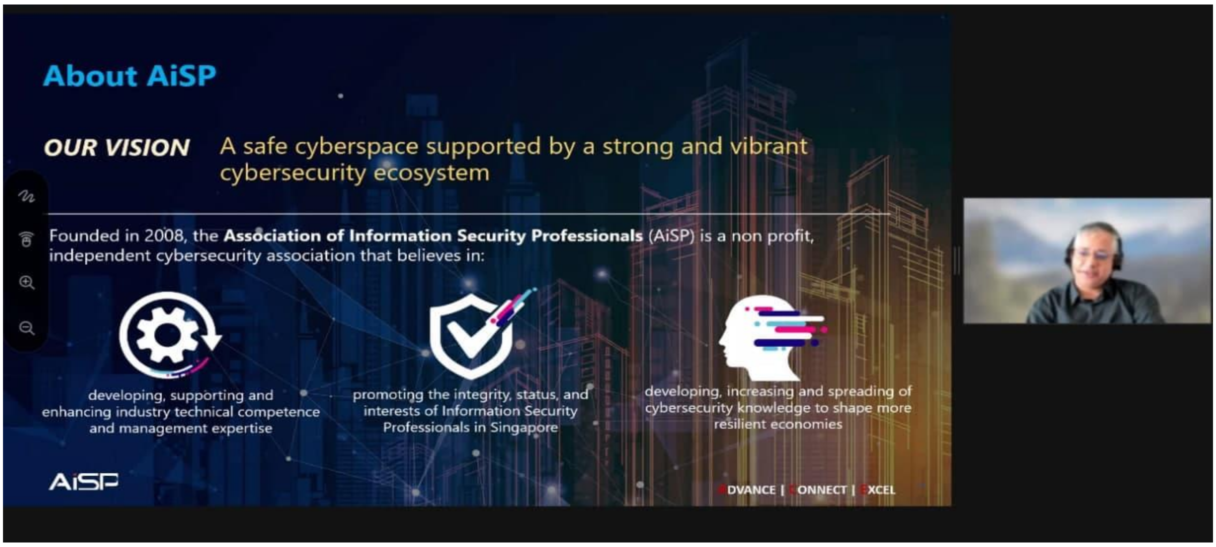
Knowledge Series Events

Operation & Infrastructure Security on 15 September

It is our pleasure to have Mr Chris Thomas and Mr Dominic Cheah from Extrahop and Tanium to join the webinar for our September Knowledge Series on 15 September. AiSP Vice President, Mr Andre Shori gave an opening address to kick off the session.

Chris shared on Defining an XDR Strategy for companies and the importance for employing the strategy in organizations. As the Technical Solutions Engineering Director for Tanium, Dominic offered insights on how to Accelerate Your Operations and Regain Visibility and Control. It was an insightful time for all our participants.

Return to the top

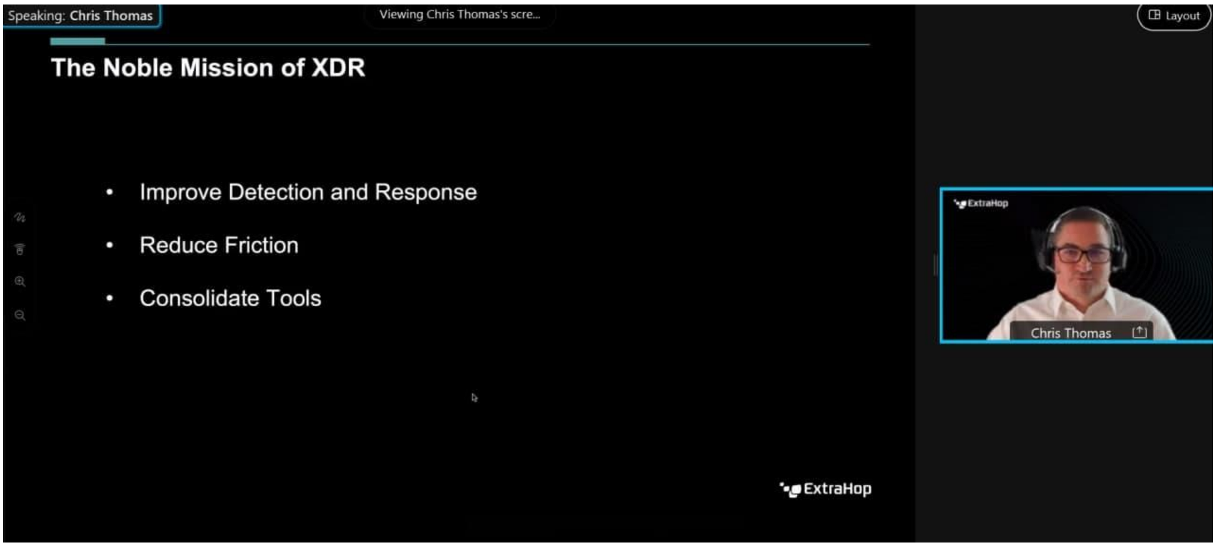


About AiSP

OUR VISION A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem

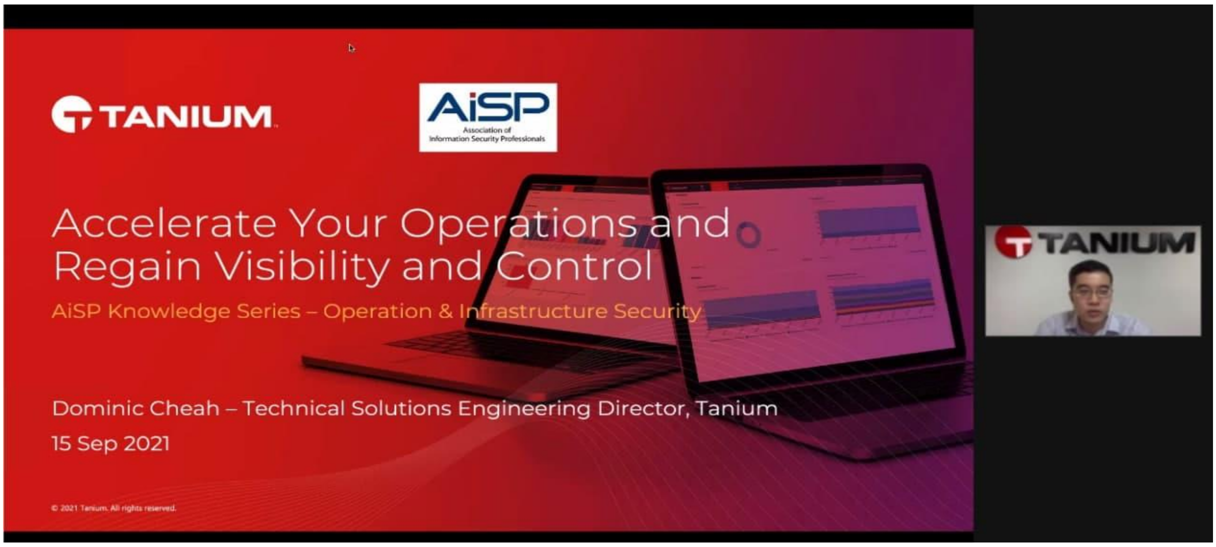
Founded in 2008, the **Association of Information Security Professionals** (AiSP) is a non profit, independent cybersecurity association that believes in:

- developing, supporting and enhancing industry technical competence and management expertise
- promoting the integrity, status, and interests of Information Security Professionals in Singapore
- developing, increasing and spreading of cybersecurity knowledge to shape more resilient economies



The Noble Mission of XDR

- Improve Detection and Response
- Reduce Friction
- Consolidate Tools



Accelerate Your Operations and Regain Visibility and Control

AiSP Knowledge Series – Operation & Infrastructure Security

Dominic Cheah – Technical Solutions Engineering Director, Tanium

15 Sep 2021

© 2021 Tanium. All rights reserved.

Return to the top

Internet of Things

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 – Internet of Things

Knowledge Series - Internet of Things

27 Oct | 7-9 PM | WebEx

Andrew Ong
Chairman, CTI SIG
CSCIS & Member of AiSP

Jonathan Chin
Business Development
Manager, OT Cybersecurity
Fortinet

Organised by :

Supported by :

Via :

Based off 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.

<u>Securing the OT Environment amidst Digital Transformation</u>
By Jonathan Chin, Business Development Manager, OT Cybersecurity Fortinet

With the rise of Digital Transformation and the benefits it provides, traditional OT Air Gapped Systems, are pushed into connectivity on an IT/OT converged platform.
Cloud/Hybrid Cloud, 5G and IOT/IIOT systems are topics that come into play.
This session will explore how you can protect and manage your OT systems' cybersecurity posture within this ever-changing landscape, without compromising plant availability and reliability.

Return to the top

Rise in IoT and Cybersecurity Threats
By Andrew Ong, Chairman, CTI SIG CSCIS & member of AiSP

In the recent years, there is a rapid increase in adoption of IoT solutions in digital transformation, smart workplaces, smart homes and smart cities initiatives. IoT is rapidly changing the consumers and business lifestyle trends. Join me in a session to explore and discuss IoT opportunities and challenges.

Date: 27 October 2021 (Wed)
Time: 7 PM to 9 PM
Venue: WebEx
Registration: https://aisp.webex.com/aisp/j.php?RGID=r97fdfc7b2b058718dcca3914c1e82208

Follow AiSP Today to CONNECT with us!		
Facebook	Instagram	LinkedIn

Association of Information Security Professionals (AiSP)
116 Changi Road, #04-03 WIS@Changi, Singapore 419718
Website: www.aisp.sg

Our office is closed. We are currently telecommuting.
Please email us at secretariat@aisp.sg or message us via Telegram during office hours.

Please click here to unsubscribe if you do not wish to receive any emails from AiSP.

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. IOT, 27 Oct
2. Emerging Trends – Blockchain & AI for Cyber Security, 17 Nov*
3. CTI, 1 Dec, Hybrid*
4. Data Security, 27 Jan*
5. Red Team VS Blue Team, 17 Feb*
6. 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

Return to the top

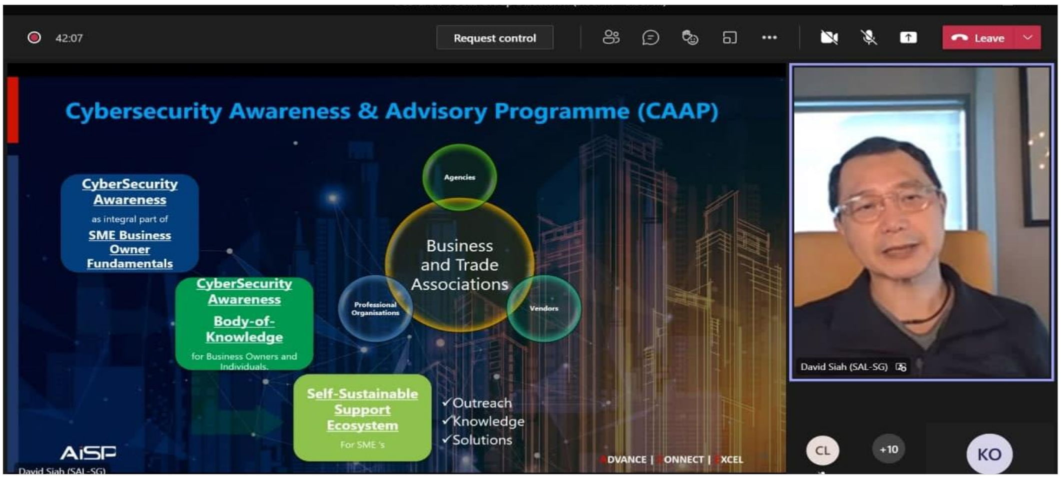
secretariat@aisp.sg for assistance. Please refer to our scheduled 2021 webinars in our event calendar.

Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP x SCS CAAP Focus Group Discussion – Singapore SMEs' Digital Adoption and Concerns on 9 September

We would like to thank all participants who joined our AiSP Committee Member, Mr David Siah on his sharing of SME's digital adoption and concerns on 9 September.

In partnership with Singapore Computer Society Cybersecurity Chapter, the session discussed on raising SMEs' awareness of cyber risks and adoption of cyber practices. He also shared on the CAAP framework and how it will help SMEs on their journey to be better protect their businesses in the cyber space.



Cybersecurity Awareness & Advisory Programme (CAAP)

CyberSecurity Awareness as integral part of SME Business Owner Fundamentals

CyberSecurity Awareness Body-of-Knowledge for Business Owners and Individuals.

Self-Sustainable Support Ecosystem For SME 's

Agencies
Business and Trade Associations
Professional Organisations
Vendors

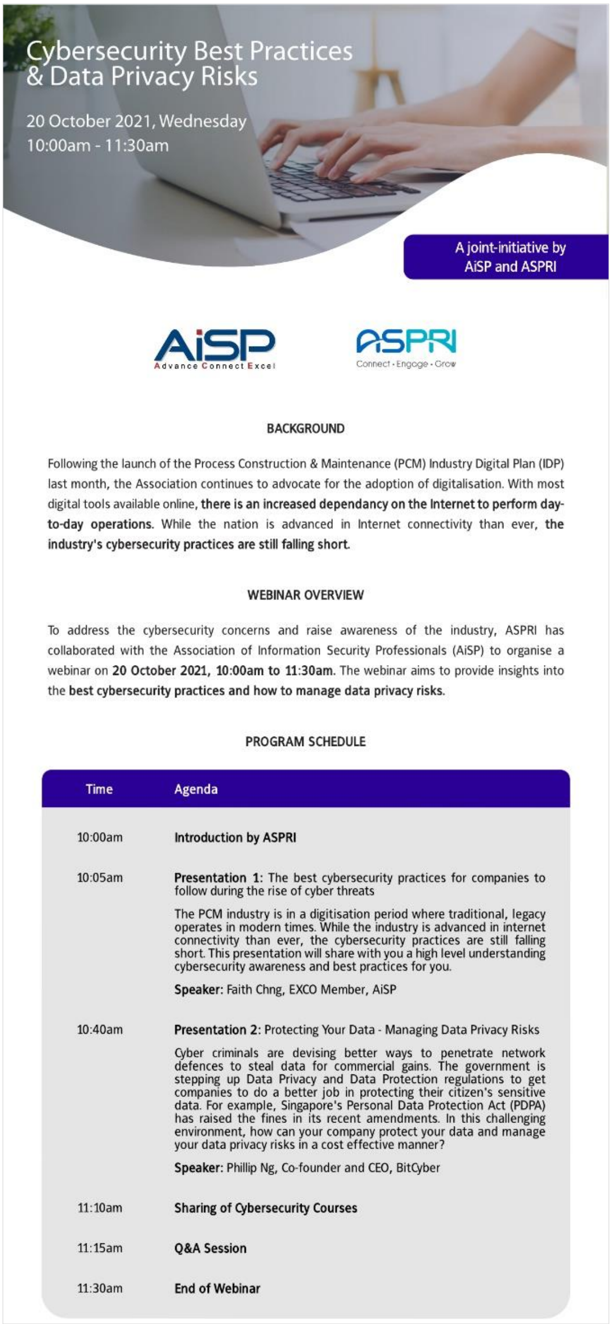
✓Outreach
✓Knowledge
✓Solutions

AiSP
DVANCE | ONNECT | XCEL

Return to the top

AiSP x ASPRI Cybersecurity Best Practices & Data Privacy Risks

AiSP hope to elevate Cybersecurity 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. Join our upcoming event below to expand your knowledge on cybersecurity issues.



Cybersecurity Best Practices & Data Privacy Risks

20 October 2021, 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 month, 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 **20 October 2021, 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**

Sign up now at
https://us06web.zoom.us/j/82464662993?pwd=UmRML0VaSDFEZzBPaVZmcFpjWmRFdz09

Return to the top

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.

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

Return to the top

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.

Contact AiSP Secretariat at secretariat@aisp.sg to secure your tickets. Visit https://www.aisp.sg/cyberfest/smeconf2021.html for more details.

Organised by **Supported by**

Sponsors

Supporting Partners

Return to the top

Student Volunteer Recognition Programme (SVRP)

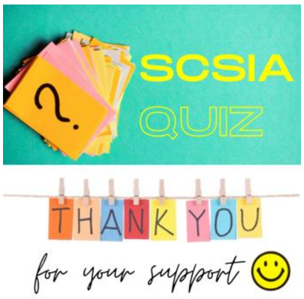
SVRP Nomination has officially concluded, and results will be released in Mid-October. Our student volunteer drive is ongoing till Dec 2022 for those who are interested to volunteer but not sure where to start. Please **click here** to apply today. The third SVRP Awards Ceremony will be held on 19 January 2022 at Lifelong Learning Institute Event Hall.

The Awards Ceremony is sponsored by:

ENSIGN INFOSECURITY | CONQUER THE UNKNOWN

Singapore Cyber Security Inter Association (SCSIA)

Cyber Day Quiz (Ended)



As part of **AiSP's CyberFest 2021** and in conjunction with **Singapore Cyber Day 2021 in** November 2021, the **Singapore Cyber Security Inter Association (SCSIA)** organized an online quiz competition for primary, secondary and tertiary students (aged 25 years and below) in Singapore with the support from the Cyber Security Agency of Singapore. This competition aims to pique interest in students and equip with knowledge on Cyber Security.

SCSIA Quiz has officially ended on 30 September. We would like to thank all participants for your continuous support for the past 28 weeks and logging on to our Facebook and LinkedIn page every Thursday for the quiz questions. We are in the process of selecting the finalists. E-Certificate of Participation will be emailed to all participants. Winners will be notified via email and **prizes will be given to the top scorers.**

Return to the top

Singapore Cyber Day 2021

The second inaugural Singapore Cyber Day will be 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 cybersecurity profession and how everyone can take part in Singapore's cybersecurity ecosystem and contribute towards our cyber resilience.

SCSIA volunteers are involved in a series of school talks for primary and secondary school students. There are two parts to the virtual talks:

1. Part 1: Virtual Event with the launch of videos and quiz and sharing by speakers from the professional bodies and associations.

2. Part 2: Videos and quiz for the students to take part in during the school holidays. The Singapore Cyber Security Inter Association (SCSIA) has organized an online quiz competition for primary, secondary and tertiary students (aged 25 years and below) in Singapore with the support from the Cyber Security Agency of Singapore. This competition aims to pique interest in students and equip them with knowledge on Cyber Security. This initiative was announced on 2 November 2020 and officially launched on 25 March 2021.

Organised by **Supporting Agency** **Supported by**

Supporting Associations

Return to the top

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
October 2021 Edition
Interview of Ms Soffenny Yap

Ladies Talk Cyber Series

For the Sixth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Soffenny Yap, Security Services Sales Leader at IBM where she spearheaded Cybersecurity services offerings in Singapore. She shared on her experiences with IBM and how we can encourage more women to enter the field.

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

Soffenny is a Security Services Sales Leader at IBM where she spearheaded Cybersecurity services offerings in Singapore. Soffenny has over 6 years of experience in Cybersecurity industry. She is an independent and self-motivated sales professional who carries a high expectation of herself and always striving to succeed. Her network and close relationship with partners and customers have help to provide vital client leads to her team and increase in business for the organization that she has worked for.

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

Return to the top

International Cyber Women Day 2021

As part of International Cyber Women Day 2021, AiSP will be featuring some of our Female Leaders on AiSP LinkedIn Page. Visit https://www.linkedin.com/company/aisp-sg/ to hear our female leaders experience Cybersecurity.

AiSP will also be organising a few ladies in cyber events in September to commemorate International Cyber Women Day 2021. We looked forward to having you in our AiSP Ladies in Cyber events. To find out how you can sponsor, volunteer, or play a part in our programmes, please contact us at secretariat@aisp.sg today.

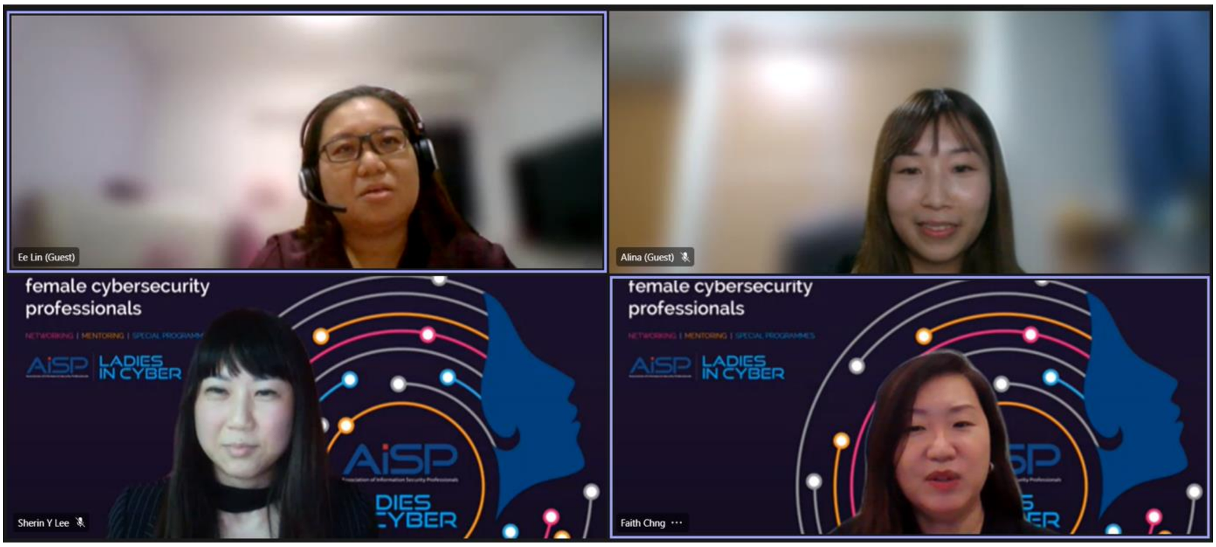
(Photo taken in 2019 during the AiSP Ladies Night)

AiSP Ladies in Cyber Spill the Tea on 1 September 2021

As part of International Cyber Women Day 2021, AiSP invited 3 Prominent Female Leaders in a Spill The Tea session on 1 Sept 21 (Wed) for a night of sharing and discussion on their role in Cybersecurity moderated by Faith. Our speakers shared personal experience in

Return to the top

their day to day job and how they are coping between their career and personal life, as well as their motivation on what motivates them to stay on and what are some of their biggest setback that they faced in their journey and what they hoped to achieve in the future. If you have missed the session, you can watch it on YouTube: https://youtu.be/eWpEaiw3Qys.



AiSP Ladies in Cyber Learning Journey & Fireside Chat In 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: January 2022 (Date to be confirm again)
Time: 7.30pm to 8.45pm (Please join in 5 mins before the session)

Return to the 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

Sign up at https://tinyurl.com/lic24092021

AiSP Ladies in Cyber Inaugural Symposium on 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 in 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.

Return to the top

Organised by

AiSP
Advance Connect Excel

Supporting Agency

CSA
SINGAPORE

Supported by

CYBER YOUTH
—SINGAPORE—

ENSIGN
INFOSECURITY
CONQUER
THE UNKNOWN

Sponsors

Acronis

Checkmarx

CISCO

DBS

FORTINET

GOVTECH
SINGAPORE

Singtel | Trustwave

ST Engineering

TANIUM

TREND
MICRO

Women on 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:

Return to the top

- 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. Please contact us if you are keen to be part of our SIGs as we are actively recruiting members!

Special Interest Group (SIG) Events

Date	Event
9 November 2021	Combined SIG Event

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.

Return to the top

Regionalisation

Singapore – Romania: Webinar on Cybersecurity

SINGAPORE-ROMANIA: WEBINAR ON CYBERSECURITY

26 Oct 2021 | Webex

3PM - 4.30PM (SGT) | 10AM - 11.30AM (EET)

Organised by

Via

Supporting Partners

Supported by

AiSP Advance Connect Excel
ATIC
SGTECH
webex by cisco
EMBASSY OF ROMANIA in the Republic of Singapore
Enterprise Singapore
Alibaba Cloud
BitCyber Securing Your Business
Bitdefender
CYBER SWARM
Cyscale
kaspersky
SAFETECH INNOVATIONS

In collaboration with Association for information Technology and Communications of Romania (ATIC) and SGTech, we have invited companies from Singapore and Romania to share more about cybersecurity. Join us to find out more through insights from our panel of speakers.

Opening Addresses by Key Personnel
By Mr. Florin-Marius TACU, H. E. The Ambassador of Romania in Singapore
By Prof. Dr. Vasile Baltac, President of ATIC
By Mr Johnny Kho, President, AiSP
By Mr Eugene Lam, Executive Committee Member, Cyber Security Chapter, SGTech

Return to the top

Opening Address By Key Personnel

Florin-Marius TACU
H. E. The Ambassador of Romania in Singapore

Vasile Baltac
President, ATIC

Johnny Kho
President, AiSP

Eugene Lam
Executive Committee Member, Cybersecurity Chapter, SGTech

Singapore & Romania ICT Landscape

Eugene Lam
Executive Committee Member, Cybersecurity Chapter, SGTech

Florin VREJOIU
Programme Manager, ATIC

Singapore ICT Landscape
By Mr Eugene Lam, Executive Committee Member, Cyber Security Chapter, SGTech

SGTech will present the Singapore ICT landscape including sharing on how overseas companies can leverage on Industry Associations to accelerate their go-to-market into Singapore and the Asia Pacific Region.

Romania - the site of the "European Cybersecurity Industrial, Technology and Research Competence Centre" (ECCC)
By Mr Florin VREJOIU, Programme Manager, ATIC

Romania - Unique combinatorial skills supported by broad country advantages
ATIC - The best entry point for ICT partnerships with specialists from Romania.
ATIC is a right member of the following international organisms:

- WITSA - World Information Technology and Services Alliance
- CEPIS - Council of European Informatics Societies
- IT_STAR - Regional ITC Association in Central, Eastern & Southern Europe

Panel of Presentations & Debates

Return to the top

Panel of Presentations & Debates

Ovidiu-Adrian CICAL
CEO, Cyscale

Costin G. Raiu
Director, Global Research and Analysis Team, Kaspersky

Mihai RANETI
CEO, Swarm European Services

Alex "Jay" Balan
Security Research Director, Bitdefender

Victor GANSAC
CEO, Safetech Innovation

Mike Low
Senior Compliance Manager, Alibaba Cloud

1. **Your organization as a knowledge graph - how graph technology is changing cloud security**
   By Mr Ovidiu-Adrian CICAL, CEO, Cyscale

   At Cyscale we merged the knowledge graph model with our cloud security expertise and developed this innovative new technology called Security Knowledge Graph™.
   It uses a data model that maps networks of cloud entities in an exhaustive graph which supports automated reasoning across multi-cloud infrastructures.
   Our Security Knowledge Graph™ will surface crucial issues of all your interlinked cloud assets, helping you improve your security and data governance procedures.

2. **2021 cyber threats overview: Romania and Singapore**
   By Mr Costin G. Raiu, Director, Global Research and Analysis Team, Kaspersky

   During this presentation, we will discuss the latest security trends affecting businesses worldwide with a focus on Romania and Singapore. We will talk about the role of threat intelligence in protecting against advanced attacks and provide advice on how to defend against sophisticated threat actors.

3. **New cyber security solution based on neuromorphic computing**
   By Mr Mihai RANETI, CEO, Swarm European Services

   H.E.C.K. - Hardware Encryption and Communication Kit
   H.E.C.K secures the communication and it has optional edge computing capabilities. It comes in various form factors and thus can be deployed in different types of environments – being able to fulfil any kind of customer requirements.

4. **Threats landscape for enterprise security**
   By Mr. Alex "Jay" Balan, Security Research Director, Bitdefender

Return to the top

Quick outline of all highly successful attack vectors against enterprises along with some predictions for the near future.

5. **a trustful partner for cyber security and critical infrastructure resilience**
By Mr Victor GANSAC, CEO, Safetech Innovation

Safetech Innovations has In-Depth Expertise In Cyber Security and an important experience in implementing innovative solutions to various categories of beneficiaries in Romania and abroad.
We will present our knowledge, capabilities and skills which contribute to the recognition of the company as one of the most certified and efficient in the field of cybersecurity at national, European and international level.
We will be presenting also the main cybersecurity services and solutions (proprietary or well-known international ones) as well as the way we bridge the gap between companies, technology and the public sector by partnering with world class innovators, renowned R&D Institutes and international organizations to increase the security and resilience of information networks and critical infrastructures. A special place will be allocated to the main projects in our R&D portfolio which include STI-CERT (SAFETECH COMPUTER EMERGENCY RESPONSE TEAM) - a private CERT/CSIRT, owned and operated by our company, that provides continuous cyber security threats and incidents monitoring services for private and public sector clients, iSAM, the Information Security Automation Manager, our first Information Security solution developed in-house, to assist companies with their GRC efforts, and SafePIC, a product that sets a standard in the field of cyber security, interoperability and cyber protection for critical infrastructure.

6. **Privacy Compliance in Alibaba Cloud**
By Mr Mike Leow, Senior Compliance Manager, Alibaba Cloud

Many countries and regions, including ASEAN, have turned on their respective Privacy and Data Protection laws and regulations. With certifications on DPTM and APEC CBPR, Alibaba Cloud is committed to providing reliable, secure, and compliant cloud computing products and services. Learn in this upcoming webinar, from our Senior Compliance Manager, on how we adhere to industry standards and best practices that meet the requirements of both international and domestic markets, and how we deal with heightened expectations from our customers and regulators.

Date: 26 October 2021 (Tue)
Time: 3.00PM – 4.30PM (SGT) / 10.00AM – 11.30AM (EET)
Venue: Webex
Registration: https://aisp.webex.com/aisp/j.php?RGID=r180f2334bb18367e7e761a337bc535cf

Follow AiSP Today to CONNECT with us!		
Facebook	Instagram	LinkedIn

Return to the top

The Cybersecurity Awards

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 2021 in Q1 of 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 Advance Connect Excel
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 CONQUER THE UNKNOWN
ST Engineering
TREND MICRO
Gold Sponsors
CyberProof A UST Global Company
Centre for Strategic Infocomm Technologies
DBS
kaspersky
Singtel
wizlynx group
Silver Sponsors
PCS SECURITY
RSA
SIT Singapore Institute of Technology
THALES
Wsg Workforce Singapore

Return to the 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
15 Sep – 30 Nov	SMEICC Conference Series 2021	Partner

Upcoming Events

Date	Event	Organiser
05 Oct	Advisory's Discover+: Cloud Computing	AiSP
05 – 06 Oct	IndoSec Summit 2021	Partner
05 – 07 Oct	GOVWARE	Partner
08 Oct	ITE College West - Security Summit 2021	Partner
12 Oct	CISCO ASEAN	Partner
20 Oct	AiSP x ASPRI CAAP Webinar	AiSP & Partner
22-Oct	Sharing on Cybersecurity as Career – Organised by NTUC	Partner
26 Oct	AiSP x Mastercard CAAP Workshop	AiSP & Partner
26 Oct	Singapore – Romania: Webinar on Cybersecurity	AiSP & Partner
26 – 27 Oct	ADS & ARTC during Singapore International Energy Week 2021	Partner
27 Oct	Knowledge Series – Internet of Things	AiSP
02 – 03 Nov	CISO ASEAN	Partner
02 – 03 Nov	Cyber Security for Financial Services Asia Part II	Partner
08 – 12 Nov	Singapore FinTech Festival 2021	AiSP & Partner
08 Nov	Singapore Cyber Day	AiSP
09 Nov	SIG Day	AiSP
10 Nov	CAAP Focus Group Discussion & Sharing of AiSP Courses	AiSP & Partner
17 Nov	Knowledge Series – Emerging Trends – Blockchain & AI for Cybersecurity	AiSP
23 Nov	Cyber Leaders Series	AiSP
23 Nov	CREST Webinar	AiSP

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

Return to the top

CONTRIBUTED CONTENTS

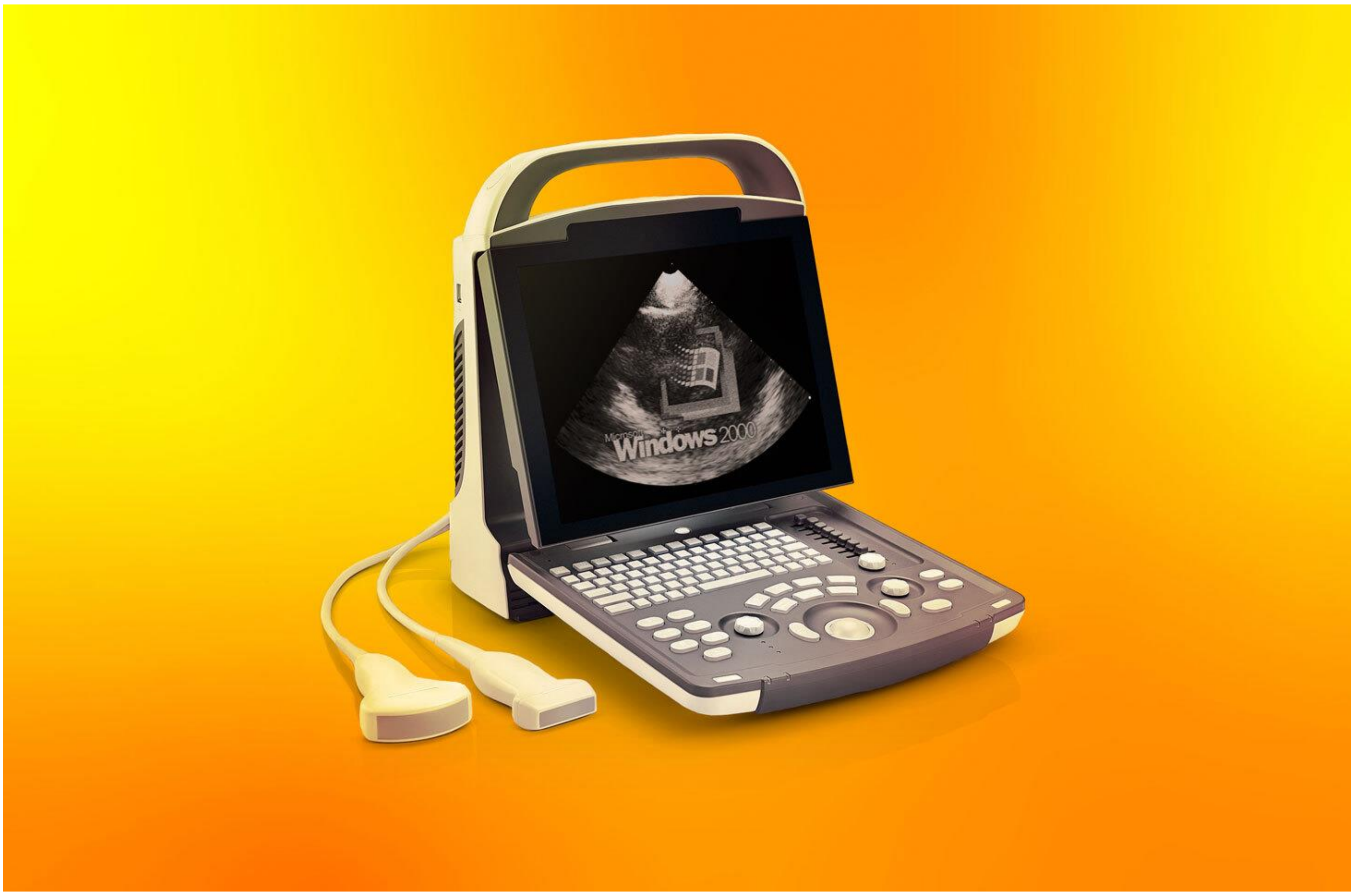
Article from IoT SIG

Protect networked IoT devices or protect the network from IoT devices?

IoT devices tend to greatly increase a company's attack surface, but you can minimize the risk.

Nikolay Pankov

June 4, 2021



In Into the Mind of an IoT Hacker at RSA Conference 2021, security specialists Itzik Feiglevitch and Justin Sowder brought up the issue of vulnerability of various IoT devices and the special

Return to the top

treatment they require from corporate cybersecurity. They offered a few stunning examples showcasing the state of IoT security in today's businesses.

Few cybersecurity specialists keep track of their corporate IoT hardware. More often than not, smart elevators, all sorts of sensors, IPTV, printers, surveillance cameras, and the like are just a motley collection of disparate devices, each with its own OS and proprietary protocols, and many lacking any sort of proper control interface … you get the picture. Your company may have thousands of them.

Why IoT devices introduce extra cybersecurity risks

IoT devices are not always regarded as belonging to the relevant infrastructure; although a network printer normally counts as a network device, the same isn't true of "smart building" components or even IP telephony systems. To be clear, such devices tend to be connected to the same network as corporate workstations are.

Staff coming and going may complicate the situation even further. The greater the turnover in cybersecurity and IT, the better the chance a new person won't know a thing about the IoT zoo connected to the network.

Perhaps worst of all, some of those devices are accessible from the outside. The reasons may be legitimate — vendor control over some aspect of a device; telework availability; maintenance — but having devices on the corporate network on the one hand, while being permanently hooked to the Internet on the other, is risky.

It may sound paradoxical, but the very robustness of modern electronics is another risk factor: Some IoT devices have very long life spans and are running in vastly more complex security environments than they were designed for.

For example, some devices run obsolete, vulnerable operating systems that are no longer updated — and even if they can be, updating may require physical access (which can range from difficult to nearly impossible). Some feature unchangeable passwords, debugging backdoors erroneously left in the final firmware release, and many other surprises to spice up the life of an IT security pro.

Why attackers take an interest in IoT devices

Cybercriminals find IoT devices interesting for several reasons, both for host company attacks and for attacks on other companies. The main uses for compromised smart devices are:

- Setting up a botnet for DDoS attacks;
- Mining cryptocurrency;
- Stealing confidential information;
- Sabotage;
- As a springboard for further attacks and lateral movement in the network.

Return to the top

Case studies

Researchers have described some cases that are fairly ridiculous. These relate to both standard devices connected to the Internet and quite narrowly specialized ones. Two prominent examples highlight ultrasound machines and devices using Zigbee protocols.

Ultrasound machine

Modern organizations working in the healthcare sector make use of numerous IoT medical devices. To test the security of such devices, researchers bought and tried to hack a used ultrasound machine. They needed only about five minutes to compromise it; the device was running on a version of Windows 2000 that had never been updated. Moreover, they were able not only to obtain control of the device, but also to gain access to the patient data the previous owner hadn't deleted.

Physicians often use medical devices for years, or even decades, without updating or upgrading them. That's understandable — if it ain't broke, etc. — but these devices don't merely operate for a long time in the first organization that acquires them; they are often resold and continue to operate.

Zigbee protocols

Companies use Zigbee networking protocols, which were developed in 2003 for energy-efficient wireless communication between devices, to build mesh networks, and often to connect various components within a smart building. The result: a gateway somewhere in the office that controls dozens of different devices, such as, for example, a smart lighting system.

Some researchers say a cybercriminal could easily emulate a Zigbee device on a regular laptop, connect to a gateway, and install malware there. The cybercriminal would just have to be within the coverage area of the Zigbee network — for example, in the office lobby. Once they controlled the gateway, however, they could sabotage work in any number of ways — for example, by turning off all of the smart lights in the building.

How to secure a corporate network

Security officers are not always sure whether they should protect IoT devices *on* the corporate network or protect the corporate network *from* IoT devices. Actually, both problems need to be solved. The important thing here is to ensure that every item and action on the network is visible. Establish corporate security requires first identifying all devices connected to the network, correctly classifying them, and, ideally, analyzing associated risks.

The next step is, of course, network segmentation based on the results of the analysis. If a device is necessary and irreplaceable but has vulnerabilities that updates cannot fix, then you'll need to configure the network to deny vulnerable devices Internet access and also to remove their access from other network segments. Ideally, use a Zero Trust concept for segmentation.

Monitoring network traffic for anomalies in relevant segments is also critical to your ability to trace compromised IoT devices being used for DDoS attacks or mining.

Return to the top

Finally, for the early detection of advanced attacks that employ IoT devices as anchors in the network and attack other systems, use an EDR-class solution.

For any enquiries, please contact Kaspersky Head of Public Affairs, APAC, Ms. Genie Gan, at genie.gan@kaspersky.com

About the Author

Nikolay Pankov | Senior Editor, Kaspersky

Nikolay Pankov is a cybersecurity enthusiast and vintage computer collector. As a Kaspersky blog editor, he specializes in reaching business audiences.

Return to the top

Article from our CPP Partner, Marsh

Cyber Risks: between mitigation and transfer, what is the best choice?

Cyber security has raised increasing interest from business stakeholders worldwide. Every day, we read about new cyber-attacks in the news, and we see companies becoming victims despite their cybersecurity resources and budgets. Today, cyber risk costs businesses almost $450 billion per year. The expanding digitization and continuously increasing cyber threats constantly challenge the companies' cybersecurity strategies and controls. Therefore, how does a business build cyber resilience when it does look like it is already a lost game?

Technological adoption immediately increases the business attack surface, which defines the entry points for cybercriminals into your company's environment. This, combined with weaknesses across people, processes, and technological controls, lead to successful cyber-attacks.

Currently, within the overall business world, there are a few misconceptions that require immediate attention:

1. Cloud is either secure or is not secure: Cloud deployment is based on a shared responsibility model. This model defines both; the cloud provider and the customer's roles and responsibilities using cloud services. The customer remains the solely responsible actor for ensuring proper security controls "in" the cloud, protecting its assets. The cloud provider provides the security "of" the cloud. While most cloud providers offer documentation about those roles and responsibilities, cloud misconfigurations remain the most common reasons for data breaches.

2. Industrial Control Systems are air-gapped, and their security does not require Information Security team support: Industrial control attacks have been increasing during the last years due to the massive financial gain following the disruption of industrial processes. When a factory is disrupted for a short amount of time, the business might suffer extreme financial losses. Thus, cybercriminals target those systems through various attack vectors, including third parties, and publicly exposed devices by mistake. A recent successful attack exploited a remote access control that allowed a vendor to pursue the maintenance of Supervisory control and data acquisition (SCADA) systems.

3. Good technology or brand does not have technical vulnerabilities: CVEs, short for Common Vulnerabilities and Exposures are available on various websites where anyone can access to a list of publicly disclosed computer security flaws. Those flaws include different very well-known brands, hardware, software, and firmware. No technology is bullet-proof.

Return to the top

4. Cyber insurance is not required if the business has good cybersecurity controls: 100% security is neither the right goal, neither achievable for your business. A good cyber strategy incorporates a risk management process that balances mitigation and transfer, providing the most optimal risk financing strategy. Cyber insurance is designed to mitigate losses from various cyber incidents, including data breaches, business interruption, and network damage. It supports your incident response process, beyond the technical aspects. It also looks at your business interruption profit loss, for example.

After demystifying those misconceptions, let us look at the important steps for cyber risk management. It is essential to understand the business activities and strategic initiatives before building a cyber strategy. The cyber strategy should ideally consider the whole business attack surface, and not limit itself to critical assets. Today, businesses operate in an interconnected ecosystem, that includes even third parties connecting to their environment.

A successful cyber strategy identifies cyber risks and defines the mitigation and transfer based on the business's risk appetite:

1. Identify your cyber risks: Identifying cyber risks is a complex and far from trivial task. In fact, cyber risk requires a business focus, rather than a technical focus on threats. Often, threats are identified as cyber risks in the cybersecurity industry, however they are not. For example, ransomware is a threat. This threat might affect an asset, leading to a successful cyber-attack. The cyberattack might lead to a business interruption, causing financial losses and profit decrease. The latter is a cyber risk.

2. Quantify your cyber risks: Qualitative frameworks describing cyber risks remain very subjective, and do not allow informed decisions for mitigation strategies. They also do not facilitate investment requests and budget allocations. Financial quantification on the other hand is an immediate business value-add framework defining possible costs associated to a cyber risk if the risk materialises. The above case would consider the losses related to profit loss, communication costs, recovery costs, forensic investigation costs, public relation costs, etc. The losses associated with a cyber-attack are not limited to technical costs and business relevant costs.

3. Address each cyber risk; balancing mitigation and transfer: Knowing that 100% security does not exist, and that a cyber-attack is an inevitable financial cost for the business, build a strategy that considers a balance between additional security controls, and cyber insurance coverage for better cash and liquidity management, following a cyber-attack.

4. Repeat.

Cyber risk management is a relatively new risk domain. It has to further mature to achieve the same level as other traditional business risks, i.e., property, operational, financial, etc. However, today, businesses are unable to operate without technology. Thus, cyber risk is

Return to the top

a business risk requiring clear investment and focus from each business stakeholder, including the board of directors.

Reach out to Marsh Cyber Risk Consulting team for support or inquiries regarding cyber risk management and cyber insurance.

Return to the top

Article from our CPP Partner, MicroFocus

Bullet Proof your Software Development and Application Security Testing

A recent study has shown that during building applications in the software development lifecycle, there has been an increased focus on efficiency. Typically, what causes inefficiency in the software development lifecycle are two components – the data and the testing.

Let's take a look at the testing element first, in today's world with all us connecting remotely we are part of this new 'Hyper Connectivity' phenomenon – and applications need to be able to scale. Quality and functional testing has been there for some time, but a new form of testing has emerged over the last few years – Application Security Testing, testing for code vulnerabilities and web application vulnerabilities.

How effectively you develop your code and test your code is largely going to depend on the data you have and the quality of data. I recall almost 20 years ago, as a developer, I simulated the data to represent business process and failed miserably – the quality of my data was poor and miles from how the real business data looked.

The data aspect for me has always been interesting – as a database administrator it was always my job to provision databases to the development and testing teams. In those days, the easiest means to provision a database for development and testing was to copy the production database – this remains the best option for many enterprises today. I have to say, those that use this method – do reset the passwords for all users …. but only some.

The challenge has always been two-fold, how do I consistently change the data across the database and secondly how can I reduce the amount of data held within the database.

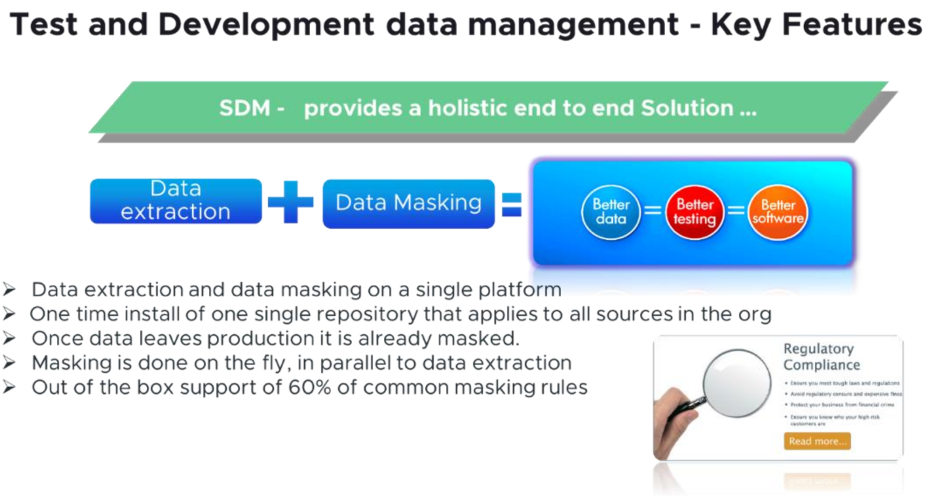
- Creating the correct data and volumes of data for development and testing purposes is highly inefficient and seldom reflects true business process.
- Reproducing production data for development and testing requirements still the preferred approach.
    - How can I generate data that accurately represents business transactions without compromising the security of the data?
    - How can I create subsets of data and anonymize the data and ensure it is fit for purpose for development and testing?
    - How can I automate spinning up development and testing environments securely?

A common approach for protecting data in non-production environments is the use of Data Masking. There are two flavors for Data Masking – Static Data Masking and Dynamic Data Masking.

Return to the top

Static Data Masking – this is the permanent and persistent change of data across the database. A few tools allow you to reverse the process, but it is very rare. This also includes data sub-setting – a feature that help me reduce the amount of data stored in the databases. Sub-setting the data can be based on volume and also number of days/months/years etc. A production database can be copied to a development database holding only 6 months of data, with the data anonymized. This certainly allows developers to be able to develop code against data that accurately represents business data.

Micro Focus Structured Data Manager provides an end-to-end holistic solution for a number of use cases, one of which includes test and development data management.



Test and Development data management - Key Features

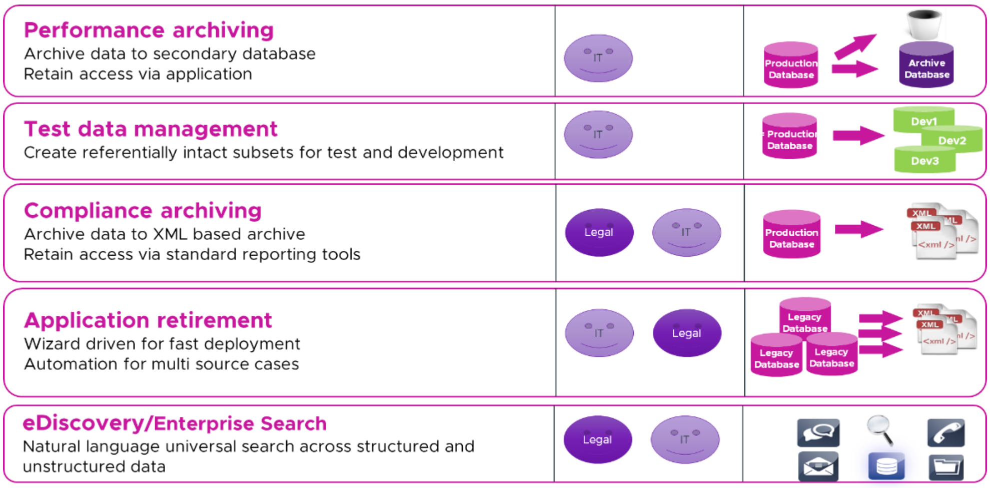
- Data extraction and data masking on a single platform
- One time install of one single repository that applies to all sources in the org
- Once data leaves production it is already masked.
- Masking is done on the fly, in parallel to data extraction
- Out of the box support of 60% of common masking rules

Regulatory Compliance

- Ensure you meet tough laws and regulations
- Avoid regulatory censure and expensive fines
- Protect your business from financial crime
- Ensure you know who your high risk customers are

Such solutions support several different popular database sources and targets that include alternate databases, XML & CSV files, and big data platforms.

There are other popular use cases for which Structured Data Manager can be used for:



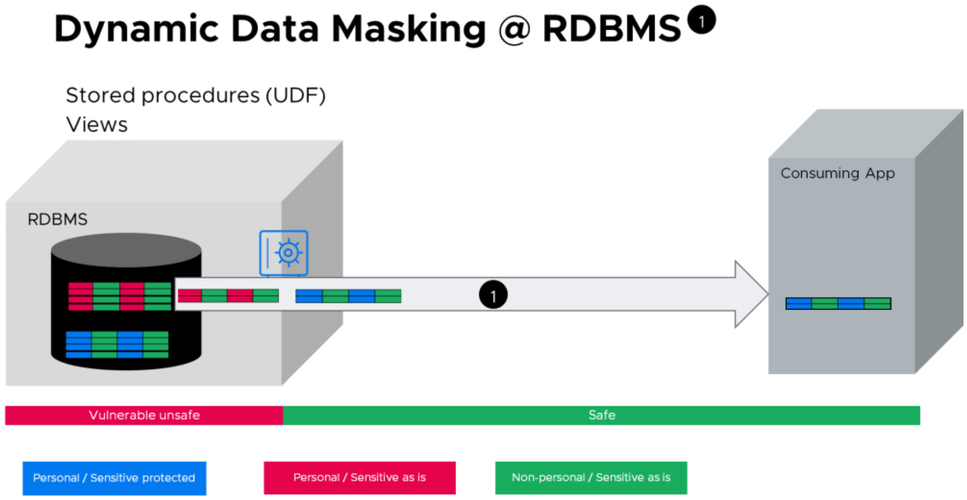
Performance archiving Archive data to secondary database Retain access via application	IT	Production Database → Archive Database
Test data management Create referentially intact subsets for test and development	IT	Production Database → Dev1, Dev2, Dev3
Compliance archiving Archive data to XML based archive Retain access via standard reporting tools	Legal IT	Production Database → XML
Application retirement Wizard driven for fast deployment Automation for multi source cases	IT Legal	Legacy Database, Legacy Database, Legacy Database → XML
eDiscovery/Enterprise Search Natural language universal search across structured and unstructured data	Legal IT	

We mentioned there are two main approaches to masking and we have looked at Static – let's look at Dynamic Data Masking now.

Return to the top

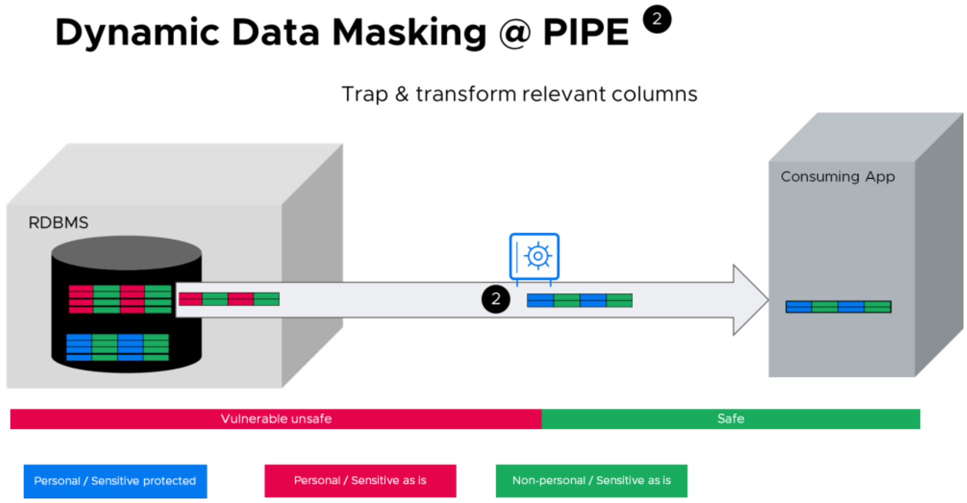
Dynamic Data Masking allows organizations to mask/anonymize data in a non-permanent manner, allowing full or partial masking of fields. This approach is often applied to production systems.

There are several approaches to Dynamic Data Masking –
The first is using the capabilities of the database stored procedures and views to mask the data. This means the data stored is unmasked and masking is performed at the database layer via the database stored procedures and views.


Dynamic Data Masking @ RDBMS 1
Stored procedures (UDF)
Views
RDBMS
1
Consuming App
Vulnerable unsafe
Safe
Personal / Sensitive protected
Personal / Sensitive as is
Non-personal / Sensitive as is

In this example, anyone who by-passes the views and procedures or even has access directly to the database storage layer will be able to see data unmasked.

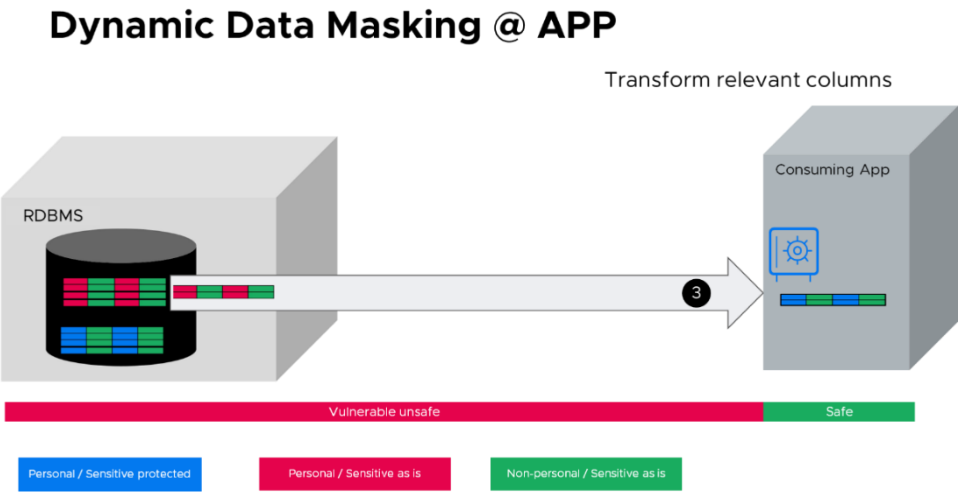
The next approach is by using a network proxy/gateway to perform the masking.


Dynamic Data Masking @ PIPE 2
Trap & transform relevant columns
RDBMS
2
Consuming App
Vulnerable unsafe
Safe
Personal / Sensitive protected
Personal / Sensitive as is
Non-personal / Sensitive as is

Here the data travel's part way across the network before the proxy/gateway determines the need to mask the data. This approach will require the proxy/gateway to be available in High Availability to ensure no leakage of data.

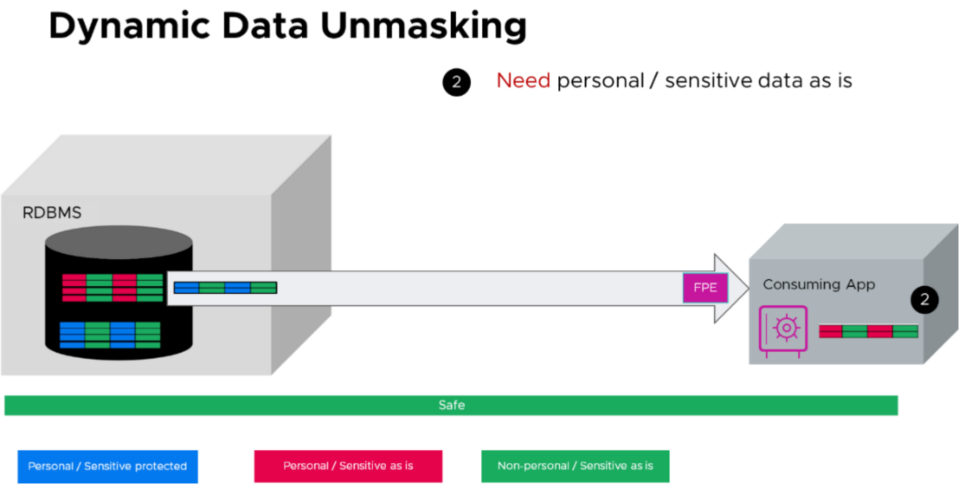
Return to the top

The next approach is leveraging the application to determine whether the data should be masked. With this approach the data travels unprotected for longer in the network layer.


Dynamic Data Masking @ APP
Transform relevant columns
RDBMS
Consuming App
3
Vulnerable unsafe
Safe
Personal / Sensitive protected
Personal / Sensitive as is
Non-personal / Sensitive as is

A point to note here is that the application could experience performance issues based on the volumes of data that need to be masked.

The final approach we will look at is Dynamic Data UNMASKING….that's right, UNMASKING! What if we were to mask the data by default, and store the data masked and allow it to be used downstream for other uses such as analytics.

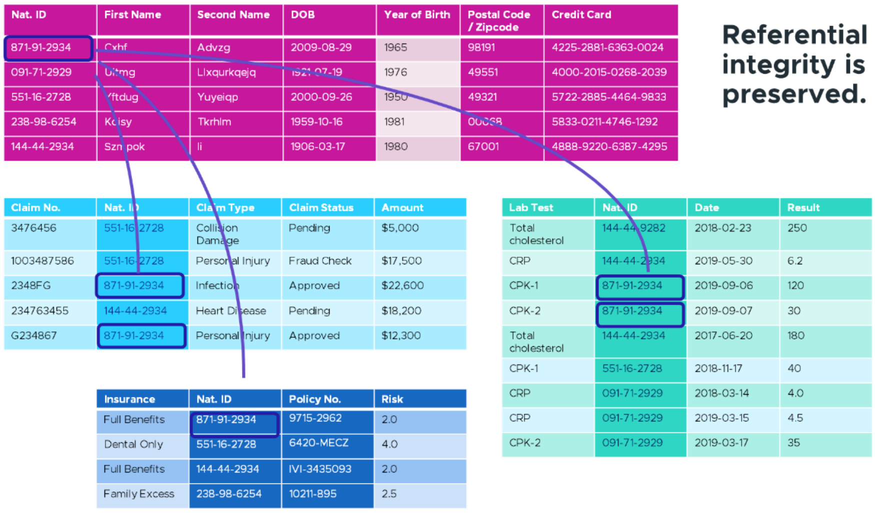

Dynamic Data Unmasking
2
Need personal / sensitive data as is
RDBMS
FPE
Consuming App
2
Safe
Personal / Sensitive protected
Personal / Sensitive as is
Non-personal / Sensitive as is

With this approach – as the data is written to the data store, we automatically mask the data. Data is protected by default and only unmasked at the application or presentation layer depending on the access policy. It's easier to unmask data than mask data at the application layer.

We should mention Format Preserving Encryption FPE….this approach allows the data type to be used by applications without decrypting or unmasking.

Format preserving encryption means the format of the field is maintained, this means that referential integrity within the database is also maintained too.

Return to the top



Nat. ID	First Name	Second Name	DOB	Year of Birth	Postal Code / Zipcode	Credit Card
871-91-2934	Cxhf	Advzg	2009-08-29	1965	98191	4225-2881-6363-0024
091-71-2929	Uitmg	Llxqurkqejq	1921-07-19	1976	49551	4000-2015-0268-2039
551-16-2728	Yftdug	Yuyeiqp	2000-09-26	1950	49321	5722-2885-4464-9833
238-98-6254	Kcisy	Tkrhlm	1959-10-16	1981	00068	5833-0211-4746-1292
144-44-2934	Sznpok	li	1906-03-17	1980	67001	4888-9220-6387-4295

Referential integrity is preserved.

Claim No.	Nat. ID	Claim Type	Claim Status	Amount
3476456	551-16-2728	Collision Damage	Pending	$5,000
1003487586	551-16-2728	Personal Injury	Fraud Check	$17,500
2348FG	871-91-2934	Infection	Approved	$22,600
234763455	144-44-2934	Heart Disease	Pending	$18,200
G234867	871-91-2934	Personal Injury	Approved	$12,300

Lab Test	Nat. ID	Date	Result
Total cholesterol	144-44-9282	2018-02-23	250
CRP	144-44-2934	2019-05-30	6.2
CPK-1	871-91-2934	2019-09-06	120
CPK-2	871-91-2934	2019-09-07	30
Total cholesterol	144-44-2934	2017-06-20	180
CPK-1	551-16-2728	2018-11-17	40
CRP	091-71-2929	2018-03-14	4.0
CRP	091-71-2929	2019-03-15	4.5
CPK-2	091-71-2929	2019-03-17	35

Insurance	Nat. ID	Policy No.	Risk
Full Benefits	871-91-2934	9715-2962	2.0
Dental Only	551-16-2728	6420-MECZ	4.0
Full Benefits	144-44-2934	IVI-3435093	2.0
Family Excess	238-98-6254	10211-895	2.5

We can use this data downstream for analytics without having to decrypt the data. The data remains protected as it travels within the network and enterprise. We only need to decrypt the data when it needs to be revealed to the users who need to see the real data.

Once we have the right data and with the right levels of security we can start to look at application security testing.

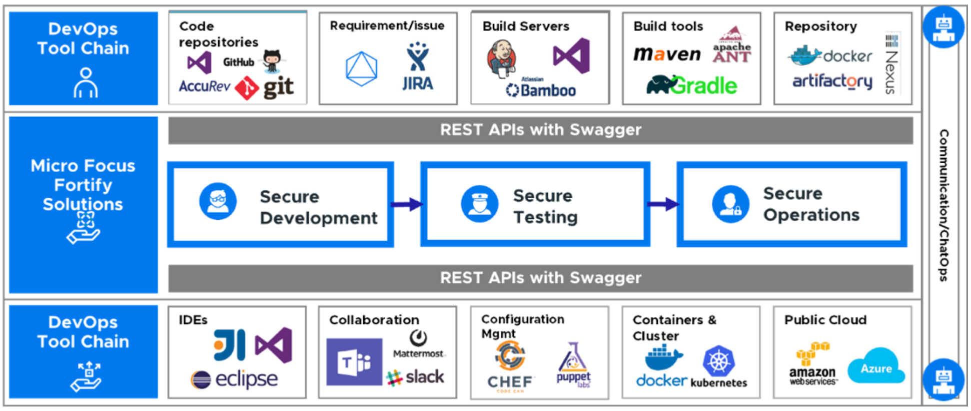
We at Micro Focus invest in R&D for application security testing, where our engineers study the structure of coding and how it can become vulnerable.

As developers write code we can scan the code for vulnerabilities and highlight these and suggest methods of remediation. Static code analysis is our SAST offering.

We also provide dynamic application security testing, DAST, where we can simulate attacks against a web interface.

The key to tools for Application Security testing is strong integration into the developer tools. We want to make security easy for developers.

Secure Applications Ecosystems



Return to the top

There are several stakeholders when it comes to Application Security and it's important to have the right DevSecOps program in place that can drive collaboration and culture across Application Development, Operations and Security teams. This has been the biggest challenge in maturing a DevSecOps program.

It is tools, people and process – with the ability to demonstrate efficiency and risk mitigation. The Fortify solution also provides reports to help with compliance requirements. These reports detail vulnerabilities identified and map against OWASP.

With workloads moving to cloud, all that we have mentioned in this article can be delivered in cloud and a hybrid deployment.

With an approach that looks at Data and Application we can deliver continuous security across application and data.

Return to the top

Article from our CPP Partner, IBM

IBM Security announced the results of a global study which found that data breaches now cost surveyed companies **$4.24 million** per incident on average – the highest cost in the 17-year history of the report. Based on in-depth analysis of real-world data breaches experienced by over 500 organizations, the study suggests that security incidents became more costly and harder to contain due to drastic operational shifts during the pandemic, with costs rising 10% compared to the prior year.

Businesses were forced to quickly adapt their technology approaches last year, with many companies encouraging or requiring employees to work from home, and 60% of organizations moving further into cloud-based activities during the pandemic. The new findings suggest that security may have lagged behind these rapid IT changes, hindering organizations' ability to respond to data breaches.

The annual Cost of a Data Breach Report, conducted by Ponemon Institute and sponsored and analyzed by IBM Security, identified the following trends amongst the organizations studied:

- **Remote work impact:** The rapid shift to remote operations during the pandemic appears to have led to more expensive data breaches. Breaches cost over $1 million more on average when remote work was indicated as a factor in the event, compared to those in this group without this factor ($4.96 vs. $3.89 million.)

- **Healthcare breach costs surged:** Industries that faced huge operational changes during the pandemic (healthcare, retail, hospitality, and consumer manufacturing/distribution) also experienced a substantial increase in data breach costs year over year. Healthcare breaches cost the most by far, at $9.23 million per incident – a $2 million increase over the previous year.

- **Compromised credentials led to compromised data:** Stolen user credentials were the most common root cause of breaches in the study. At the same time, customer personal data (such as name, email, password) was the most common type of information exposed in data breaches – with 44% of breaches including this type of data. The combination of these factors could cause a spiral effect, with breaches of username/passwords providing attackers with leverage for additional future data breaches.

- **Modern approaches reduced costs:** The adoption of AI, security analytics, and encryption were the top three mitigating factors shown to reduce the cost of a breach, saving companies between $1.25 million and $1.49 million compared to those who did not have significant usage of these tools. For cloud-based data breaches studied, organizations that had implemented a hybrid cloud approach had lower data breach costs ($3.61m) than those who had a primarily public cloud ($4.80m) or primarily private cloud approach ($4.55m).

Return to the top

Additional findings from the 2021 report include:

- **Time to respond:** The average time to detect and contain a data breach was 287 days (212 to detect, 75 to contain) – which is one week longer than the prior year report.

- **Mega breaches:** Average cost of a mega breach was $401 million, for breaches between 50 million and 65 million records.[3] This is nearly 100x more expensive than the majority of breaches studied in the report (which ranged from 1,000-100,000 records.)

- **By industry:** Data breaches in healthcare were most expensive by industry ($9.23m), followed by the financial sector ($5.72m) and pharmaceuticals ($5.04m). While lower in overall costs, retail, media, hospitality and public sector experienced a large increase in costs vs. the prior year.

- **By country/region:** The US had the most expensive data breaches at $9.05 million per incident, followed by Middle East ($6.93m) and Canada ($5.4m).

Methodology and Additional Data Breach Statistics

The 2021 Cost of a Data Breach Report from IBM Security and Ponemon Institute is based on in-depth analysis of real-world data breaches of 100,000 records or less, experienced by over 500 organizations worldwide between May 2020 and March 2021. The report takes into account hundreds of cost factors involved in data breach incidents, from legal, regulatory and technical activities to loss of brand equity, customers, and employee productivity.

To download your copy of the full report, please visit : https://www.ibm.com/account/reg/sg-en/signup?formid=urx-50915

For any enquiries, please contact Mr Nicholas Kwan at Nicholas.Kwan@ibm.com or Ms Soffenny Yap at Soffenny.Yap@ibm.com.

Return to the top

Article from our Ladies in Cyber Sponsor, Trustwave, a Singtel company

Why MDR is Your Most Important Security Investment

The cybersecurity threat landscape is continuously evolving, with the frequency and impacts of threats like malware and ransomware increasing every year. Hence, organisations from all industries should be proactive and search for emerging threats while also actively monitoring possible risks to be able to respond quickly once a threat is identified. However, amidst this challenging threat landscape, organisations are struggling to find enough cybersecurity professionals to staff their teams. Globally, there is a cybersecurity worker shortage of nearly 4 million. So how can companies undertake proactive threat detection and response with a vast skills shortage?

While technologies like extended detection and response (XDR) and security information and event management (SIEM) can correlate data from various sources and help detect threats and facilitate investigations, they lack some of the proactive elements needed to stay secure in today's advanced threat landscape. Without the right expertise, organisations are unable to tap on the full potential of these technologies. Likewise, a traditional managed security service provider (MSSP) that focuses on monitoring logs and alerts is missing a large part of the picture and can generate many false positives and low-value work for their customers.

Increasingly, organisations are turning to managed detection and response (MDR) services. MDR is one of the fastest-growing areas of cybersecurity. The analyst firm Gartner estimates that 50 percent of organisations will be using MDR services by 2025. Yet, there is often confusion in the

Return to the top

industry about what MDR services should include and who is more capable of providing them. Some boutique providers specialise in MDR, with very limited adjacent capabilities and telemetry support. Some MSSPs claim to provide MDR, but they are only reactively investigating automated alerts. Before investing in more cybersecurity technologies and services, organisations must first understand the true value that MDR services can deliver, the differences between MDR and other managed security services, and how to choose the right partner.

Getting the Most Out of Your Security Spend

Even when an organisation has the budget to do so, the effort, time and expertise needed to establish 24/7 threat detection and response capabilities in-house can be overwhelming. Deploying and properly configuring complex technologies like XDR and SIEM platforms across a large number of endpoints, servers, clouds and networks can often take months. Even after these technologies are implemented, it takes time for an organisation's in-house security analysts to gain expertise on the systems, learning how to properly configure and maintain them.

In contrast, an experienced MDR provider can dramatically reduce the time-to-value for cybersecurity solutions, helping an organisation achieve its expected ROI much more quickly. By leveraging endpoint detection and response (EDR) agents that can be rapidly deployed and the XDR evolution of EDR that includes out-of-the box integrations with cloud infrastructure solutions, a good MDR provider can have a high-fidelity service running within an organisation in a matter of hours – ensuring that your organisation is quickly protected from emerging threats.

Another significant benefit of an MDR service is that it can help an organisation improve the return on investment (ROI) of the cybersecurity tools they already own. Many organisations make the mistake of buying top-of-the-line cybersecurity technologies - while lacking the expertise and resources to properly utilise it. A good MDR provider brings a wealth of experience with these technologies, as well as round-the-clock monitoring and threat intelligence from other client sites – providing an instant boost to your cybersecurity capabilities, coverage and expertise.

What to Look for in an MDR provider

A sophisticated mix of people, process and technology is required to effectively detect and respond to the advanced threats targeting organisations today. Knowing what to look for in an MDR provider will help organisations get the value they seek out of their cybersecurity programme:

- **Technology:** Early MDR services were very endpoint-focused, helping organisations operationalise their EDR solutions. Today, threat detection, including threat-hunting, must go far beyond an organisation's endpoints. As businesses have moved more of their IT infrastructure to the cloud and more people are working remotely, the number of potential risks, vulnerabilities and entry points into an organisation has increased exponentially. A strong EDR deployment is still a good starting point, but organisations should look for an MDR provider that is experienced with XDR and SIEM technologies in order to bring together threat telemetry and forensic data from throughout the organisation's broader IT infrastructure, including networks, email, cloud infrastructure and more.

Return to the top

- **Detection:** Threat-hunting is without a doubt one of the more important aspects of MDR services, but the methods used by MDR providers can vary greatly. Most MDR services incorporate threat-hunting on at least a periodic basis, but some providers are more sophisticated in threat-hunting. It's important to look at how a MDR provider detects threats. Is it human-led, hypothesis-driven threat hunting, or is it merely automated searching for IOCs? Many traditional MSSPs claim they offer threat hunting capabilities based on data from logs, but this approach is limited to historical and limited data. Threat hunting needs to involve proactive exploration and interrogating systems for their current state as well as historical data. A quality MDR partner should combine human-led threat hunting with 24/7 monitoring and real-time analysis and investigations.
- **Response:** Response is another area where levels of service can be very different. For some MDR providers, a response means simply making recommendations on how to proceed. To get more value from your MDR services, look for a provider who responds to threats by containing them and keeping them from spreading further. Rather than stopping at notifying and alerting, your MDR provider should be able to take action remotely on your organisation's endpoints, within the network, or other applications to isolate systems and stop threats in their tracks.
- **Research Capabilities:** Threat intelligence is often the foundation for effective detection and threat hunting. Look for an MDR provider with an active research arm and can incorporate other cyber threat intelligence to benefit from the latest information on emerging threats around the globe. It is also beneficial to understand how they conduct their research and curate threat intelligence. By studying adversaries and their techniques, reverse-engineering malware, conducting breach investigations and more, a strong research team helps organisations stay a step ahead of threats.
- **Field-Tested Experience:** If your organisation allows your MDR partner to make changes within your environment in order to respond to threats, you will want to make sure they have field-tested experience with appropriate incident responses. Hasty responses can result in negative consequences like shutting down systems and business processes unnecessarily. You need to know that your MDR provider has field-tested experience in making the right decisions about what actions to take and that they have a mature methodology for the incident response process.
- **Culture:** An important aspect that organisations often overlook is culture. Consider the provider's operating model, how they work with your organisation and their demeanour in your interactions. Are they the type of people you want to work with? Are they credible, and do they enjoy a good reputation in the industry? Is the company large enough such that they'll be able to provide a consistent, long-term partnership? These are all questions to consider when determining if their company culture is a good fit with your own.

A quality MDR provider does much more – actively interrogating endpoints, conducting threat research and hunting, performing forensic investigations, and quickly responding to incidents to mitigate their impact. They bring important insights and contextual knowledge about threats and vulnerabilities derived from other client environments that enable them to be more effective in your environment. Lastly, their expertise on complex cybersecurity technologies and tools enables them to optimise your existing investments, speeding up time to value and improving ROI.

Return to the top

What Makes Trustwave MSS & MDR Different

A key component of our leadership position is our ability to successfully integrate our elite SpiderLabs team and their world-class threat intelligence into our core MSS offerings. Leveraging data from across Trustwave's 5,000+ MSS global customers along with discreet security research to hone in on attack vectors, indicators of compromise (IoCs) and attacker behaviours across a multitude of verticals, SpiderLabs makes Trustwave who we are.

Trustwave's ability to infuse its MSS offering with this actionable threat intelligence along with advanced analytics in the purpose-built and cloud-native Trustwave Fusion open XDR platform has been critical in helping to meet enterprises' strenuous needs as they embrace digital transformation and combat the continuously evolving threat landscape.

In the first Forrester Wave for MDR, Trustwave stood out and achieved the highest scores possible in the following categories:

- Threat intelligence for faster detection and response
- Collaboration with clients for superior outcomes in detection, investigation, and response.
- XDR collection, correlation, and APIs.

Trustwave has made significant investments in its MDR capabilities and offerings. We've developed the Trustwave Fusion Platform to perform and enable threat detection and response capabilities as well as provide powerful analytics and insights to our customers. Trustwave has also doubled its investment in rapid geographic expansion and top security talent. We continue to add highly skilled and specialised security practitioners to our teams worldwide.

Fancy a discussion to advance your organisation's security posture? Contact us now. For more enquiries, please email to g-security@singtel.com

Complimentary cost analysis calculator

Managed Detection & Response

Return to the top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Our ALC Training

The Strategic Role of the Security Architect

Information Security has never been about the pure deployment of technology solutions. It has always been about business enablement – allowing the business to maximise opportunities whilst ensuring risk is managed at all times to acceptable levels.

The Information Security Architect is a strategic role that provides the critical link between two domains – that of senior management and that of the technical subject matter expert. It is a senior-level role tasked with ensuring the effective planning, design, testing, implementing and maintaining of an organisation's security infrastructure. The Security Architect has to understand the organisation – its assets, motivation, processes, governance as well as its information technology.

SABSA® Security Architecture

SABSA® is the leading information security architecture framework and methodology. SABSA® uses a top-down approach as part of a continuous improvement lifecycle, with its key stages of strategy and planning, design, implement, and manage and measure, fully aligned to the Deming lifecycle of Plan-Do-Check-Act.

SABSA® is business-driven. This is the key to its power and its global acceptance. It is all about empowering the organisation to do business as it needs and wants to do, while ensuring that it is secured and fully enabled in accordance with its business priorities. SABSA® is open source, adaptable and extensible and readily integrates with other frameworks and standards such as NIST Cybersecurity Framework, ISO/IEC 27000 series, COBIT, TOGAF, Zachmann, and PCI DSS.

SABSA® Certification Roadmap

SABSA® has a comprehensive certification program at three levels: SABSA Chartered Foundation (SCF), SABSA Chartered Practitioner (SCP) and SABSA Charted Master (SCM).

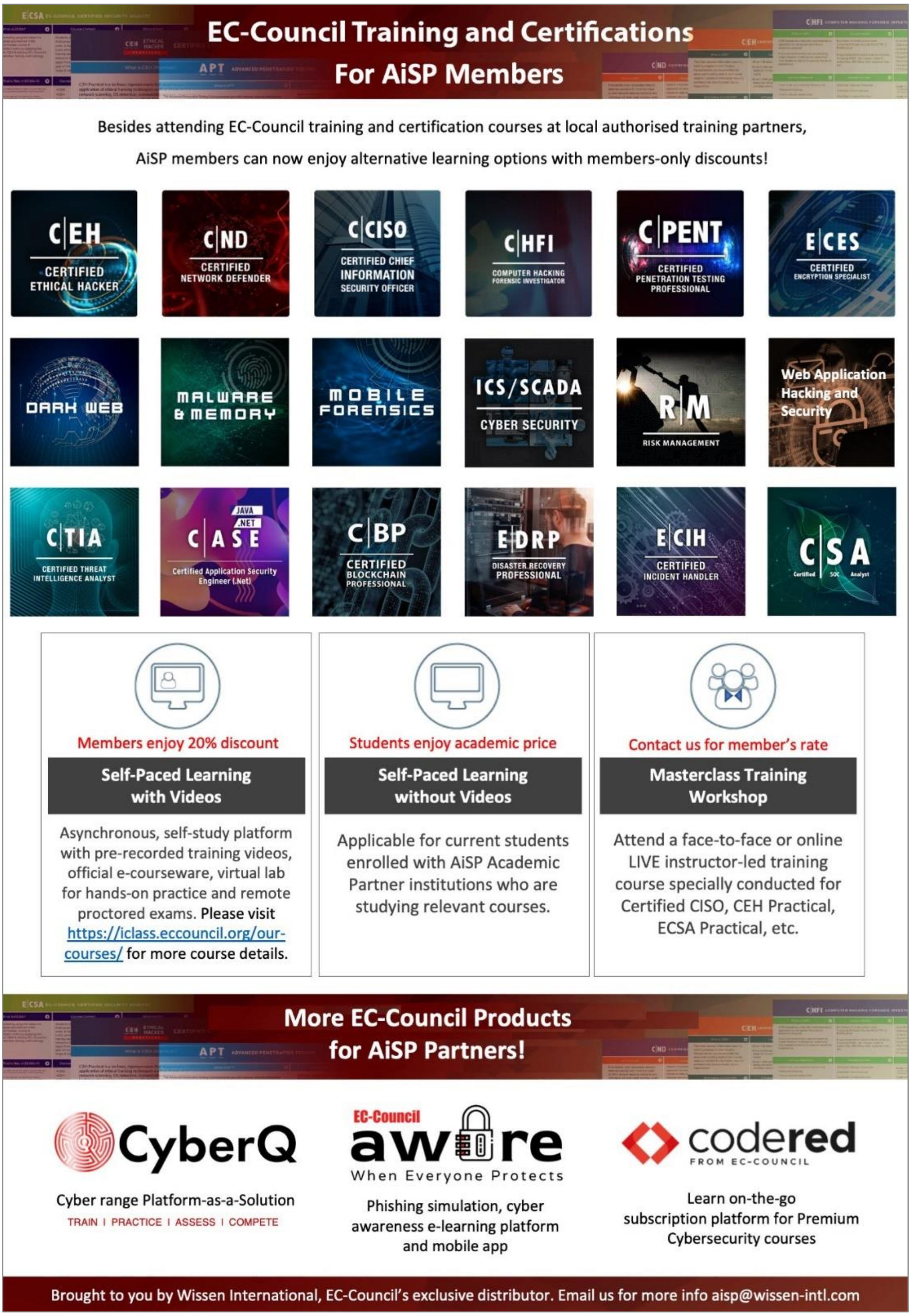
Return to the top

SABSA® training and certification is available from ALC Training with special pricing for AiSP members. Full information on SABSA is available at the website of The SABSA Institute.

For more details contact ALC at customerservice@alctraining.com.sg.

Return to the top

Listing of Courses by Wissen International



EC-Council Training and Certifications For AiSP Members

Besides attending EC-Council training and certification courses at local authorised training partners, AiSP members can now enjoy alternative learning options with members-only discounts!

C|EH CERTIFIED ETHICAL HACKER
C|ND CERTIFIED NETWORK DEFENDER
C|CISO CERTIFIED CHIEF INFORMATION SECURITY OFFICER
C|HFI COMPUTER HACKING FORENSIC INVESTIGATOR
C|PENT CERTIFIED PENETRATION TESTING PROFESSIONAL
E|CES CERTIFIED ENCRYPTION SPECIALIST
DARK WEB
MALWARE & MEMORY
MOBILE FORENSICS
ICS/SCADA CYBER SECURITY
R|M RISK MANAGEMENT
Web Application Hacking and Security
C|TIA CERTIFIED THREAT INTELLIGENCE ANALYST
C|ASE JAVA .NET Certified Application Security Engineer (.Net)
C|BP CERTIFIED BLOCKCHAIN PROFESSIONAL
E|DRP DISASTER RECOVERY PROFESSIONAL
E|CIH CERTIFIED INCIDENT HANDLER
C|SA Certified SOC Analyst

Members enjoy 20% discount

Self-Paced Learning with Videos

Asynchronous, self-study platform with pre-recorded training videos, official e-courseware, virtual lab for hands-on practice and remote proctored exams. Please visit https://iclass.eccouncil.org/our-courses/ for more course details.

Students enjoy academic price

Self-Paced Learning without Videos

Applicable for current students enrolled with AiSP Academic Partner institutions who are studying relevant courses.

Contact us for member's rate

Masterclass Training Workshop

Attend a face-to-face or online LIVE instructor-led training course specially conducted for Certified CISO, CEH Practical, ECSA Practical, etc.

More EC-Council Products for AiSP Partners!

CyberQ

Cyber range Platform-as-a-Solution

TRAIN | PRACTICE | ASSESS | COMPETE

EC-Council aware

When Everyone Protects

Phishing simulation, cyber awareness e-learning platform and mobile app

codered FROM EC-COUNCIL

Learn on-the-go subscription platform for Premium Cybersecurity courses

Brought to you by Wissen International, EC-Council's exclusive distributor. Email us for more info aisp@wissen-intl.com

Return to the 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

Return to the top

- Develop and Implement Security Goals, Objective and Strategy and Programs
- Maintain and Review Security Operations

COURSE DETAILS

Date Selection available till December 2021
Time: 9am-6pm
Fees: $2,500 (before GST)*
**10% off for AiSP Members @ $2,250 (before GST)*

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***.

Return to the top

Cybersecurity Essentials Course

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

Return to the top

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

COURSE DETAILS

Date Selection available till December 2021
Time: 9am-6pm
Fees: $ $1,600 (before GST)*
**10% off for AiSP Members @ $1,440 (before GST)*

TARGET AUDIENCE

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

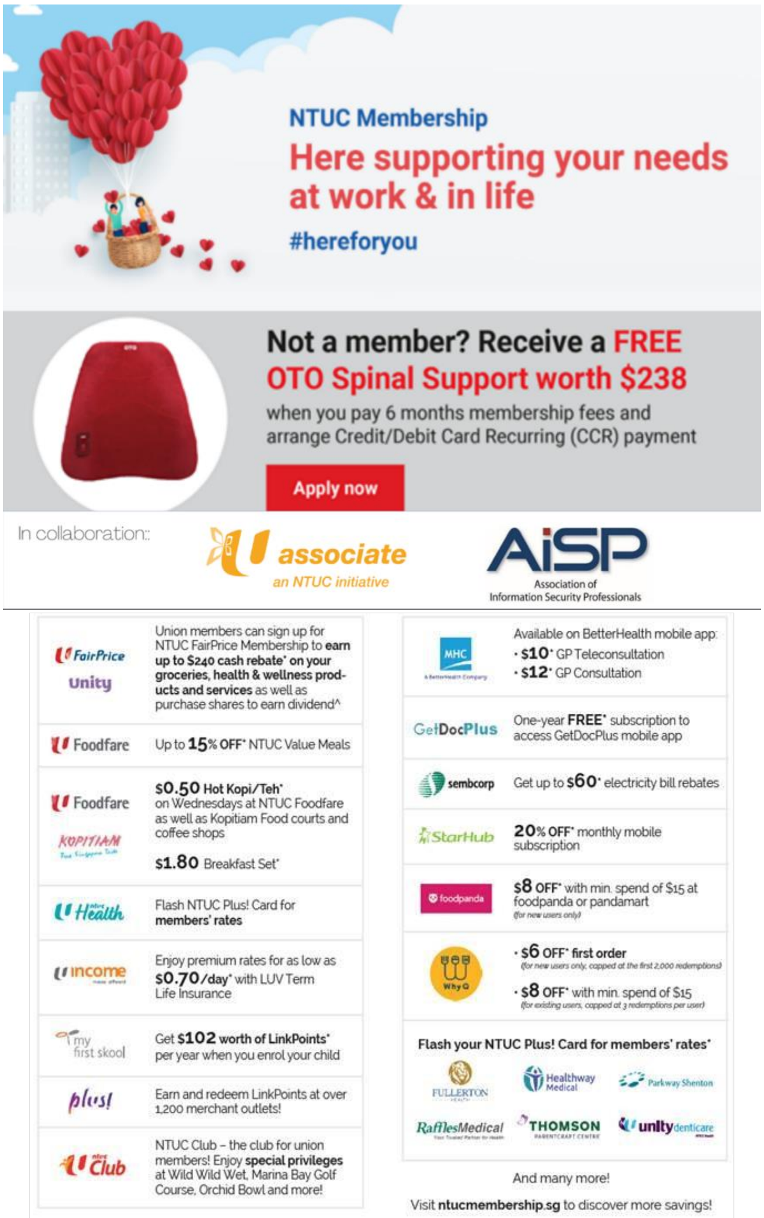
Register your interest here: https://forms.office.com/r/SQuHCcifKS

Return to the top

MEMBERSHIP

Sharing of Cybersecurity with NTUC Members

Sign up for NTUC Union Membership today and have access to a wide array of benefits from workplace protection to lifestyle benefits (attached below for merchants deals)!



NTUC Membership

Here supporting your needs at work & in life

#hereforyou

Not a member? Receive a FREE OTO Spinal Support worth $238 when you pay 6 months membership fees and arrange Credit/Debit Card Recurring (CCR) payment

Apply now

In collaboration:: U associate an NTUC initiative | AiSP Association of Information Security Professionals

FairPrice Unity	Union members can sign up for NTUC FairPrice Membership to **earn up to $240 cash rebate* on your groceries, health & wellness products and services** as well as purchase shares to earn dividend^
Foodfare	Up to **15% OFF*** NTUC Value Meals
Foodfare Kopitiam	**$0.50 Hot Kopi/Teh*** on Wednesdays at NTUC Foodfare as well as Kopitiam Food courts and coffee shops **$1.80** Breakfast Set*
Health	Flash NTUC Plus! Card for **members' rates**
income	Enjoy premium rates for as low as **$0.70/day*** with LUV Term Life Insurance
my first skool	Get **$102 worth of LinkPoints*** per year when you enrol your child
plus!	Earn and redeem LinkPoints at over 1,200 merchant outlets!
Club	NTUC Club – the club for union members! Enjoy **special privileges** at Wild Wild Wet, Marina Bay Golf Course, Orchid Bowl and more!

MHC	Available on BetterHealth mobile app: · **$10*** GP Teleconsultation · **$12*** GP Consultation
GetDocPlus	One-year **FREE*** subscription to access GetDocPlus mobile app
sembcorp	Get up to **$60*** electricity bill rebates
StarHub	**20% OFF*** monthly mobile subscription
foodpanda	**$8 OFF*** with min. spend of $15 at foodpanda or pandamart (for new users only)
WhyQ	· **$6 OFF* first order** (for new users only, capped at the first 2,000 redemptions) · **$8 OFF*** with min. spend of $15 (for existing users, capped at 3 redemptions per user)

Flash your NTUC Plus! Card for members' rates*

Fullerton Health, Healthway Medical, Parkway Shenton, RafflesMedical, Thomson Parentcraft Centre, unity denticare

And many more!

Visit **ntucmembership.sg** to discover more savings!

Sign up now and receive an OTO Spinal Support worth $238.

Return to the top

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 to 2022) from 1 Sept 2020 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.

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

Return to the top

AiSP Corporate Partners

Acronis
BCG
BitCyber
Securing Your Business
BD
Checkmarx
cisco
DBS
ENSIGN
INFOSECURITY
CONQUER
THE UNKNOWN
ExtraHop
FIREEYE
FORTINET
GOVTECH
SINGAPORE
HUAWEI
HUAWEI CLOUD
IT SEC ASIA
IBM
INSIGHTZ
TECHNOLOGY
Marsh
MICRO FOCUS
MINDEF
SINGAPORE
Privasec
Responsible Cyber
ST Engineering
SecurID
An RSA Business
TANIUM
TREND MICRO

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

Return to the top

AiSP Academic Partners

ITE
Institute of Technical Education
NYP NANYANG
THE INNOVATIVE POLYTECHNIC
NGEE ANN POLYTECHNIC
REPUBLIC POLYTECHNIC
DISCOVER. TRANSFORM. ACHIEVE
SiT SINGAPORE INSTITUTE OF TECHNOLOGY
SINGAPORE POLYTECHNIC SP
SMU
SINGAPORE MANAGEMENT UNIVERSITY
SUTD
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Temasek POLYTECHNIC

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 or message us via Telegram.

Return to the top