# NEWSLETTER

July 2023



# NEWS & UPDATE

## New Partners

AiSP would like to welcome Czech Republic and Fidelis as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partners

# News & Updates

**SIT N0H4TS A Week of Cyber on 20 June**

As part of our academic partnership with Singapore Institute of Technology N0H4TS - A Week of Cyber, AiSP EXCO Member and IT Advisor, James Tan and AiSP Member Ronin O'Malley did a sharing on 20 June "Stepping into the Cybersecurity Landscape: Job Scope, CTFs, and Your Future".


**CYSummit on 23 June**

We were at the CYS Summit on 23 June at Marina Bay Sands Convention! Thank you Cyber Youth Singapore for inviting us.


back to top

# Knowledge Series Events

## Upcoming Knowledge Series

**Operations & Infrastructure Security on 19 July**

**AiSP Knowledge Series – Operations & Infrastructure Security**


In this Knowledge Series, we are excited to have Acronis, Eclypsium and Trend Micro to share with us insights on Operations & Infrastructure Security. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

**The importance of training up talent in Singapore for Operations & Infrastructure Security roles**
Speaker: Gabriel Lim, Director, Government Relations & Partnerships, Acronis

Operations and Infrastructure Security is becoming an increasingly important area of focus for modern tech companies and service providers. With new tools and growing use of AI in such environments, engineers need to be equipped with the right skillsets in order to flourish in such roles. In this webinar, Acronis' Director of Government Relations, Gabriel Lim, will share more about the general growth in demand for such business and talent needs, and share some interesting plans that Acronis has in the next few months to address these needs.

**Enhancing Operational and Infrastructure Security: Safeguarding Your Critical Systems**
Speaker: Dr. Yuriy Bulygin, Chief Executive Officer and Co-Founder, Eclypsium

back to top

In today's evolving threat landscape, ensuring the integrity and resilience of your operational and infrastructure networks is paramount.

During this session, we will delve into the key aspects of Operational and Infrastructure Security, the different layers of an IT/OT network, and the role Supply Chain Security has as a critical element in maintaining the integrity of each layer of devices and systems.
We will discuss the different layers of an IT/OT network and highlight the role Supply Chain Security as a critical element in maintaining the integrity of devices and systems, and the importance of protecting against Cyberattacks in your devices and systems.

Additionally, we will touch upon the evolving threat landscape for Operational Technology (OT), including risks posed by insider threats, malware, and physical attacks.
Finally we will share best practices and mitigation strategies to safeguard your infrastructure and ensure the resilience of your critical operations.

**Preventing Ransomware with Cybersecurity Monitoring**
Speaker: Ransomware and other cyber attacks routinely take advantage of misconfigurations in cloud and IT systems and accounts. Gain insights on how cybersecurity monitoring tools can help strengthen overall attack surface risk management to improve your organization's cybersecurity posture.

Date: 19 Jul 2023, Thursday
Time: 3PM – 5PM
Venue: Zoom
Registration:
https://us06web.zoom.us/webinar/register/1016853407196/WN_QSNCXsTgT7O5Ekol1bC4-g

back to top

## IoT on 30 August

### AiSP Knowledge Series – Internet of Things


In this Knowledge Series, we are excited to have Cybersafe, CYFIRMA and DTAsia to share with us insights on Internet of Things. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

**IoT In Cybersecurity - Risk and Reward**
Speaker: Dave Gurbani, CEO, Cybersafe

In this presentation, Dave will be sharing insights into the risks and rewards associated with utilizing IoT in the context of cybersecurity. He will discuss common IoT devices found in business environments and shed light on how they can serve as vectors of attack. Dave will emphasize the importance of implementing robust security measures to protect organizations from potential vulnerabilities. Moreover, he will explore how strategic deployment of IoT technologies can effectively safeguard businesses when used correctly. Attendees can expect to gain practical knowledge and strategies for ensuring a secure and resilient business ecosystem amidst the evolving landscape of IoT.

**How to Assess the Threat Landscape and Make Intelligence-Led Decisions in a Hyperconnected World**
Speaker: Mike Henry, CTO, CYFIRMA

A wise man once said: knowing your enemy and knowing yourself is key to winning a thousand battles. The same applies to war on the wire where the adversary operates in the

back to top

dark and defenders need to adapt strategies in real-time to counter attacks. In this session, Mike will share the methods to gain visibility of the fast-evolving threat landscape, map out attackers' motives, uncover their attack techniques, and build an agile approach to managing cybersecurity.

**Enhancing security by using Zero Trust approach for OT access**
Speaker: Raymond Ma, Regional Director, SSH APAC, DTAsia

The Zero Trust philosophy is continuing to gain momentum across the globe with various industries adopting and regulators imposing the best practices of using passwordless, just-in-time access. However, Zero Trust access has thus far been seldom mentioned or applied to OT/IoT access, despite the fact that the technology can enhance security for another layer. Therefore, Zero Trust access for OT/IoT will be introduced and explored.

Date: 30 Aug 2023, Wednesday
Time: 3PM – 5PM
Venue: Zoom
Registration:
https://us06web.zoom.us/webinar/register/4716868205413/WN_3q7zvOj2SSaD2pTutmiVsQ

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its **Information Security Body of Knowledge 2.0** topics. Our scheduled topics for webinars in 2023 are as follows (*may be subjected to changes*),

1. IoT, 30 Aug
2. Red Team, 20 Sep
3. DevSecOps, 25 Oct
4. CTI, 22 Nov

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

back to top

# Student Volunteer Recognition Programme (SVRP)


back to top


back to top

# AiSP Cyber Wellness Programme

Organised by: AiSP Advance Connect Excel

Supported by: INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In Support of: DIGITAL FOR LIFE

The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."

Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website (https://www.aisp.sg/aispcyberwellness) to get updates on the latest Cyber tips, Cyber news, activities, quiz and game happenings related to Cyber. Scan the QR Code to find out more.

**Scan here for some tips on how to stay safe online and protect yourself from scams**

**Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship & Ethics.**

**Have the knowledge and think you are safe? Challenge yourself and participate in our monthly quiz and stand to win attractive prizes. Scan now to take part.**

**Scan here if you are looking for activities / events to participate in for knowledge exchange / networking / get to know more people / stay protected & helping others.**

**Want to know more about Information Security? Scan here for more video content.**

**To find out more about the Digital for Life movement and how you can contribute, scan here.**

Contact AiSP Secretariat at secretariat@aisp.sg to find out more on how you can be involved or if you have any queries.

Click here to find out more!

back to top


# Ladies in Cybersecurity

**AiSP Ladies in Cyber Annual Socials on 31 August**

AiSP will be organising our AiSP Ladies in Cyber Annual Socials on 31 Aug 23 at Bar Bar Q as part of the International Cyber Women Day Celebrations held every year on 1 Sep. We would like to invite you and your female friends to join us in the event.

Objective : Networking, Inspiration and Career Development

Join us on 31 August 2023 for an empowering Ladies in Cyber Socials Event dedicated to supporting and celebrating women in the Cybersecurity & Tech industry. This event will feature a Tech and Tunes Networking session that provides an opportunity to connect with like-minded individuals, expand your professional network, and foster valuable connections. Engage in quick, dynamic conversations with professionals from various sectors of the Cyber & tech industry and make lasting connections. Don't miss out on this exciting opportunity to support the advancement of women in the field.

Date: 31 August 2023 (Thu)
Time: 6PM - 8.30PM
Venue: Bar Bar Q at 3 Temasek Boulevard #01-602
Suntec City Tower 4, Singapore 038983
Dress Code: Casual

back to top


You can sign up at https://forms.office.com/r/c1rmAYwHGz or scan the above QR Code. Registration will close 31 July 23.

back to top

# Special Interest Groups

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

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

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

**Cloud Security Summit on 17 August**


back to top

ORGANISED BY

SUPPORTING AGENCIES

GOLD SPONSORS

SILVER SPONSORS

BRONZE SPONSOR

SUPPORTING PARTNERS

back to top

The AiSP Cloud Security Summit 2023 is an important event of the year, organised by the AiSP Cloud Security Special Interest Group. The programme schedule comprises of key notes, solutions, panel discussion and workshop. The theme for the summit is Simplifying Cloud for a Safer Future. This event is organized for anyone with an interest or wish to find out more or understand more on the landscape of Cloud Security.
Cloud computing has become an integral part of modern businesses and organizations. The cloud offers a wide range of benefits, including increased flexibility, scalability, and accessibility. However, many users still struggle to navigate the complex landscape of the cloud and face security concerns. This summit aims to simplify the cloud experience and make it safer for everyone. Experts in cloud computing will share their insights and best practices for utilizing the cloud in a straightforward manner while maintaining security.

This event is organized for anyone with an interest or wish to find out more or understand more on the how to simplify and secure their cloud operations and reap the benefits of the cloud with confidence. We are expecting 150 attendees at this physical event. We have invited AiSP Patron - Senior Minister of State, Ministry of Communications and Information & Ministry of National Development Mr Tan Kiat How, to be our distinguished Guest of Honour for the opening. We will also be engaging CISOs, reputable services providers and vendors to present key development of Cloud Security.

Event Date: 17 Aug 2023
Event Time: 9.30AM – 2PM
Event Venue: Suntec Convention Centre
Guest of Honour: AiSP Patron - Senior Minister of State, Ministry of Communications and Information & Ministry of National Development Mr Tan Kiat How

Register here now

back to top

# The Cybersecurity Awards

**Thank you for all your nominations**
**TCA 2023 Call for Nominations has ended on 14 May.**

Professionals
1. Hall of Fame
2. Leader
3. Professional

Enterprises
5. MNC (Vendor)
6. MNC (End User)
7. SME (Vendor)
8. SME (End User)

Students
4. Students

Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors for The Cybersecurity Awards 2023! Only Silver sponsorship packages are available.

**TCA2023 Sponsors & Partners**

Organised by

Supported by

Supporting Associations

Platinum Sponsors

Gold Sponsors

Silver Sponsors

back to top

# Digital for Life

**East Coast Digital Festival on 10 June**

As part of the Digital for Life Movement, AiSP was invited to Heartbeat@Bedok for Celebrate Digital @ East Coast where we setup a booth to share with the public on how to stay safe online and beware of scams.

Thank you to Grassroot Advisors – Deputy Prime Minister Heng Swee Keat, AiSP Patron – Senior Minister of State Tan Kiat How, MP Jessica Tan, MP Cheryl Chan for visiting our booths. Thank you AiSP Cyberwellness EXCO Co-lead, Dennis Chan for taking time off on 10 June to share with more than 30 Elderlys on 网络安全人人有责 at Heartbeat@Bedok.


back to top

**DFL at Senja Hawker Centre & launch of Zhenghua CONNECTS on 10 June**

As part of the Digital for Life Movement, AiSP team participated in the opening of the Senja Hawker Centre & launch of Zhenghua CONNECTS together with our Corporate Partner - Contfinity Pte Ltd where we setup a booth to share with the public on how to stay safe online and beware of scams.

Thank you to Grassroot Advisors (GRA) - Minister Vivian Balakrishnan, Senior Minister of State Sim Ann, MP Edward Chia & MP Liang Eng Hwa for visiting us. Also thank you to our AiSP Cyberwellness EXCO Co-lead Dennis for joining us on 10 June morning to share with our GRA on AiSP & Contfinity.


back to top

**Fajar Road Community Day on 25 June**

As part of the Digital for Life Movement, Team AiSP was invited to the Fajar Road Community Day to share with 1000 Fajar residents where we setup a booth to share with the public on how to stay safe online and beware of scams. Thank you to Grassroot Advisor MP Liang Eng Hwa for visiting us at our booth.




back to top

## AiSP x PA x Huawei - Scam Awareness and Dialogue Session on 26 September


Register here

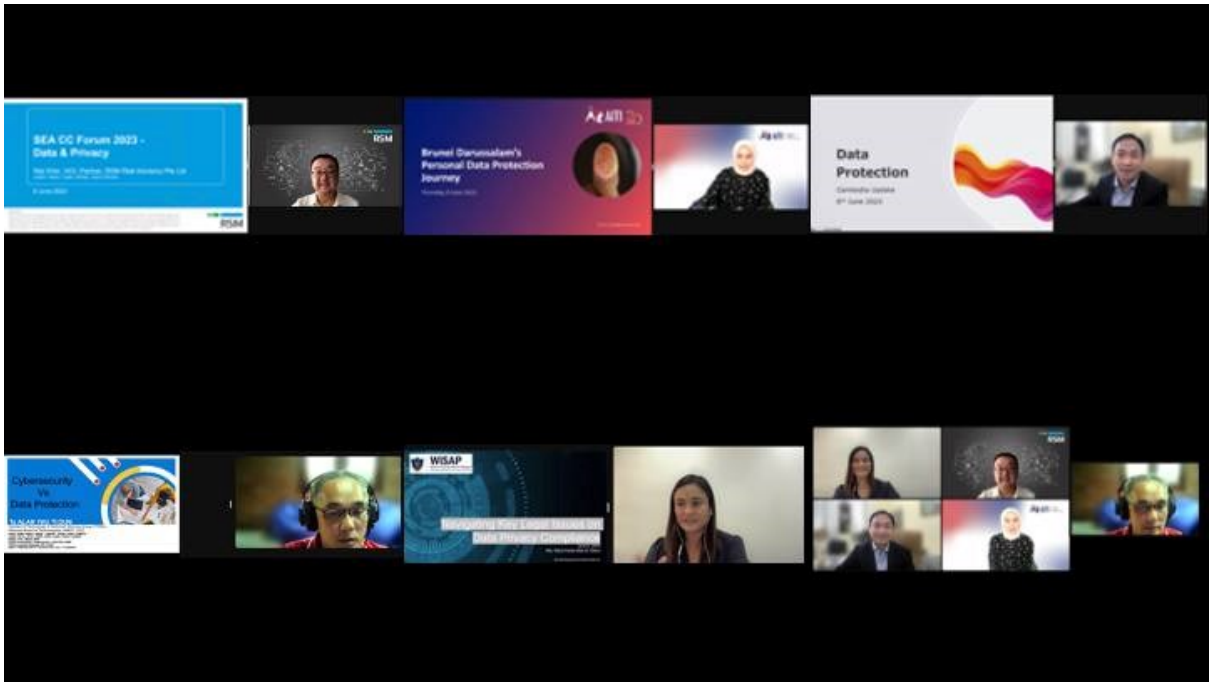
back to top

# Regionalisation

## SEA CC Webinar – Data & Privacy on 8 Jun

The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2023. The first webinar was conducted on 8 June, focusing on Data & Privacy where our speakers shared insights on the best practices for data protection.




back to top

## Upcoming Event

### SEA CC Webinar – Cloud Security


The South East Asia Cybersecurity Consortium will be organising a series of webinars leading up to the SEA CC Forum 2023. The second webinar will be focusing on Cloud Security where speakers will be sharing insights on the best practices for cloud security.

**Challenges for Secure Cloud Adoption at scale in Singapore**
Speaker: Tony Low, AiSP Vice-President [Association of Information Security Professionals]

Will like to look at the trends in Cloud Adoption especially with security around the region. A look at some of the policies that Singapore government has rolled out how it has affected the organisations in drive cloud implementation. Meanwhile there have been a lack of talents in the space across the board, what are some of the initiatives that has been implemented with joint partnership with the private sector.

**Protecting Your Assets : Unravelling the Unique Security Deployment Requirements of On-Premise Vs. Cloud**
Speaker: Sutedjo Tjahjadi - Head of Cloud Computing Committee APTIKNAS [APTIKNAS]

The drive to move the workload into the cloud due the digital transformation adoption is significant. The cloud solution offers the simplification to the infrastructure operation because it offers as a service. One aspect which should not be overlook is Cyber Security.

We'll address questions such as: What are the key considerations for securing your cloud environment? How does on-premise security differ from cloud security? And what are the foundational elements required to implement a robust Zero Trust security model in the cloud?

back to top

**Risks and Mitigation Strategies for SMEs on Cloud IaaS**
Speaker: Ye Thura Thet, Principal Analyst, Kernellix [MISA]

Many SMEs today leverage cloud technology to enhance their business functions. While the cloud is no longer a new technology, technology teams with limited capacity tend to overlook some fundamental security controls when implementing a cloud computing model in SMEs.
This presentation discusses common pitfalls for SMEs and presents a pragmatic approach to covering the basics.

**Serverless Security Model and Function Level Security**
Speaker: Rey Supan, Senior Solutions Architect [WiSAP (Women in Security Alliance Philippines)]

Understanding the security model of serverless computing and how it differs from traditional architecture and best practices for securing individual functions in a serverless architecture.

Date: 23 August 2023, Wednesday
Time: 3PM – 5PM (SGT)
Venue: Zoom
Registration:
https://us06web.zoom.us/webinar/register/8216862079756/WN_C0gdnb9cTmKFQpAu0ZN_ig

# AiSP Validated Information Security Professionals (AVIP)

**AVIP Meeting with SMS Tan Kiat How on 9 June**

AiSP AVIP Members had an engagement session with AiSP Patron SMS Tan Kiat How on 9 June. It was a fruitful discussion for our AVIP members as they exchanged thoughts with one another. The next AVIP event will be a National Day Celebration hosted by our AiSP Advisory Council on 4 August. Join AVIP membership if you would like to participate in such closed door events!

Details on AVIP can be found here https://www.aisp.sg/avip.html

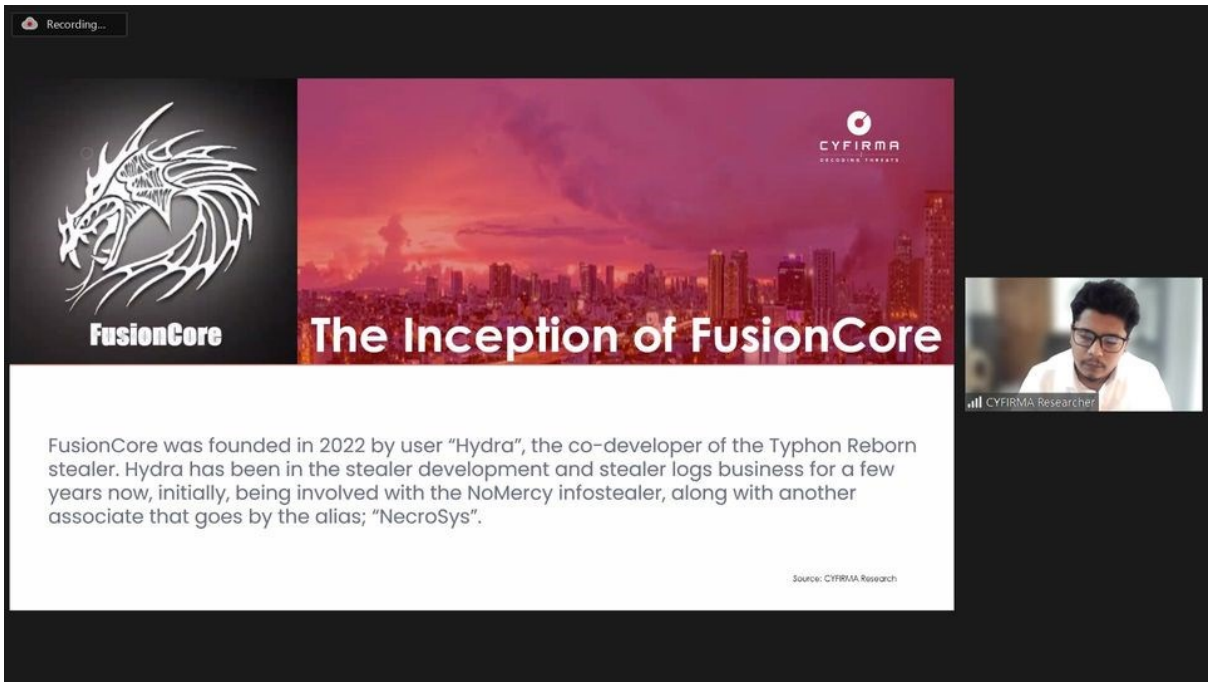
back to top

# Corporate Partner Events

**Cyber intelligence Briefings - The Rise of FusionCore An Emerging Cybercrime Group from Europe on 7 June**

In collaboration with our Corporate Partner, Cyfirma, AiSP will be organising a series of webinars. On 7 June, we shared about FusionCore: An emerging cybercrime group from Europe.




back to top

**Cyber intelligence Briefings: Tense China-Taiwan Relations - Engagement on the Cyber Battlefield on 21 June**

Working with our corporate partner CYFIRMA, AiSP has hosted the second Cyber Intelligence Briefing on the topic: Tense China-Taiwan Relation and Engagement on the Cyber Battlefield on 21 June. In the briefing, CYFIRMA researcher shared analysis of cyber campaigns from Chinese threat actors targeting Taiwan government and businesses against the backdrop of increased geopolitical tensions. Research findings stated that if Taiwan is to maintain its de facto independence, it needs to invest a lot more into preparing diplomatic, economic, and military responses to fend off the China threat, and this includes investments in its cyber defenses.

Watch the full recorded briefing here https://youtu.be/6UNjmgKuphI


back to top

**AiSP x wizlynx group - Understanding Red teaming and Purple Teaming Exercise on 28 June**

As part of Digital for Life Movement, AiSP collaborated with our Corporate Partner, wizlynx group, where we shared insights on Red Team & Purple Team. Thank you Gerard De Las Amas, Lei Yeh, Kang Meng Chow, Leow Kim Hock, Darrel Huang & AiSP EXCO Member, Sunny Neo for sharing insights with our attendees on 28 June.






back to top

## Cyfirma Webinar on 5 July

**Cyber intelligence Briefings**
**SEO Poisoning - Malware Attacks via Google Ads**


Dear Cybersecurity Professionals,

We are excited to invite you to an informative webinar that sheds light on the growing threat of malware attacks leveraging the Google Ads platform. Recent research has uncovered alarming campaigns that exploit the platform to distribute malware, specifically targeting novice users searching for popular applications and cracked versions of legitimate software.

During this webinar, our expert researchers will present their preliminary analysis of a newly discovered remote access tool (RAT) called "VagusRAT" and its potential attribution to Iranian threat actors. The VagusRAT is deployed to victims through the exploitation of Google Ads.

**Key Webinar Highlights:**

- Emerging Malware Campaigns:
  - Understanding the abuse of Google Ads to deliver malware
  - Cloned websites and typosquatting techniques employed by threat actors
- Introducing VagusRAT:
  - Comprehensive analysis of the remote access tool
  - Its capabilities and availability as Malware as a Service (MAS)
- ETLM Attribution:

back to top

- Insights into VagusRAT being offered as a customizable service to other threat actors
- The potential for customized versions with advanced features

By attending this webinar, you will gain essential knowledge to fortify your defences against malware attacks originating from Google Ads. Don't miss this opportunity to stay informed and strengthen your organization's resilience against malware attacks facilitated through Google Ads.

Feel free to extend this invitation to your colleagues and peers who would benefit from understanding the latest tactics employed by threat actors and enhancing their cybersecurity posture.

**SEO Poisoning - Malware Attacks via Google Ads**
Date: 5 July 2023
Time: 11:00AM SG Time (GMT +8:00)
Registration:
https://us06web.zoom.us/webinar/register/2616841181498/WN_esvqIAhhQOirC6BcgjtREA

## SOC 101 TRUST NO FILES! I Votiro BFSI Workshop on 12 July


back to top

Financial institutions face an ever-growing threat from incoming files. Every loan application uploaded to a web portal emailed spreadsheet or signed PDF sent to an account manager can contain malicious code that threatens the organization. All files are suspect. Ransomware campaigns and other destructive malware are running rampant as malicious actors seek out high-value targets to coerce and compromise. And the need for strong security is more critical now as the risk of file-borne threats has never been greater.
Join us in this evening workshop together with Votiro and Industry experts to further deep dive and discuss:

- The challenges facing financial institutions in countering the risk of file-borne threats.
- The threats and regulations, address why current security solutions offer inadequate protection to organizations.
- Recommendations for how financial institutions can confidently mitigate the threat of file-borne malware, optimizing security in conjunction with business continuity and productivity.

**Date**: 12 July 2023 Wednesday
**Time**: 6pm SGT
**Venue**: JustCo @ Marina Square, 6 Raffles Boulevard, #03-308, S( 039594 )

**Agenda**

| | |
|---|---|
| 06:15 – 06.45pm | Registration & Refreshment |
| 06:45 – 07.00pm | Welcome & Introduction |
| 07:00 - 07.20pm | Zero Trust Framework |
| 07:20 - 07.40pm | MAS TRM Best Practice & Compliance |
| 07.40 - 07.55pm | Why Votiro and addressing to TRM |
| 07.55 - 08.15pm | Panel Discussion |
| 08.15 - 08.30pm | Demo Session |
| 08.30 – 09.00pm | Q&A & Networking |

Click here to register.

back to top

## Operational Technology Cybersecurity Expert Panel Forum 2023 on 22-23 August


OTCEP Forum 2023 will be held from 22 to 23 August 2023 at Resorts World Convention Centre, East Ballroom.

The event will comprise of plenary presentations, industry participation, Capabilities Development Showcases, technical presentation and concurrent tracks in the domains on Operations, Engineering and Governance.

We are also pleased to share that all panel members will be physically in Singapore for OTCEP Forum this year.

We are now ready for registration to attend OTCEP Forum 2023. The broad programme outline is as follows:

back to top

Day 1 - (22 August)
- Main Plenary Presentations and Panel Discussion
- Capability development Showcase

Day 2 - (23 August)
- Concurrent Track on Operations, Engineering and Governance Domains
- Capability development Showcase

Please scan the QR code to register or visit us at https://www.otcep.gov.sg .
See you at the event!

# Upcoming Activities/Events

**Ongoing Activities**

| Date | Event | Organiser |
|---|---|---|
| Jan – Dec | Call for Female Mentors (Ladies in Cyber) | AiSP |
| Jan – Dec | Call for Volunteers (AiSP Members, Student Volunteers) | AiSP |

**Upcoming Events**

| Date | Event | Organiser |
|---|---|---|
| 5 Jul | Learning Journey to Singtel for RP | AiSP & Partner |
| 5 Jul | Cyfirma Webinar | AiSP & Partner |
| 10-13 Jul | CYDES 2023 | Partner |
| 11 Jul | Learning Journey to ASUS for Pri Sch | AiSP & Partner |
| 12 Jul | Learning Journey to RSM for Pri Sch | AiSP & Partner |
| 12 Jul | SOC 101 \| Trust No Files | AiSP & Partner |
| 14 Jul | Scam Talk for NLB workshop | Partner |
| 17 – 19 Jul | CISO Melbourne | Partner |
| 18 Jul | Learning Journey to Grab for Pri Sch | AiSP & Partner |
| 19 Jul | Cyfirma Webinar | AiSP & Partner |
| 19 Jul | Knowledge Series – Operations & Infrastructure Security | AiSP & Partner |
| 25 – 26 Jul | BYTES Singapore | Partner |
| 26 Jul | Cyfirma webinar | AiSP & Partner |
| 26 Jul | Detect the Undetected and Fortify Your Cyber Defenses | Partner |
| 26 – 27 Jul | CyberSecAsia Indonesia Conference | Partner |
| 28 – 29 Jul | Skills for Good Festival | Partner |
| 28 Jul | ITE West Security Summit | Partner |
| 2 Aug | Cyfirma Webinar | AiSP & Partner |
| 2 Aug | Learning Journey to Trendmicro for Pri Sch | AiSP & Partner |
| 4 Aug | National Day Celebration with Advisory Council | AiSP |
| 9 -10 Aug | CISO Exec Network Sydney | Partner |

back to top

| | | |
|---|---|---|
| 11 Aug | Cyfirma Webinar | AiSP & Partner |
| 15 - 16 Aug | SMEICC | Partner |
| 16 Aug | Cyfirma Webinar | AiSP & Partner |
| 16 Aug | ASEAN Bug Bounty | AiSP & Partner |
| 17 Aug | **Cloud Security Summit** | AiSP |
| 22 -23 Aug | CISO Singapore | Partner |
| 23 Aug | SEA CC Webinar – Cloud Security | AiSP & Partner |
| 23 Aug | School Talk @ Westwood Sec | AiSP & Partner |
| 24 Aug | ISACA Singapore GTACS Conference | Partner |
| 25 Aug | ISC2 Workshop | AiSP & Partner |
| 29 – 30 Aug | IndoSec 2023 | Partner |
| 30 Aug | Knowledge Series - IoT | AiSP & Partner |
| 30 Aug | Cyfirma Webinar | AiSP & Partner |
| 31 Aug | International Cyber Women Day Celebrations | AiSP |

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

# CONTRIBUTED CONTENTS

## Article from IoT SIG

### Five myths of IoT/OT cybersecurity: Far from the (hard) truth!

**Fabien Maisl**

Just like any fast-growing innovative sector, the industrial cybersecurity market largely remains a mystery to many. And where there is mystery, there are myths. In the era of all things being connected and of cybercrime becoming a structured business, the cybersecurity challenge is a daunting one for many companies. This article debunks some of the myths that leave industrial organizations dangerously exposed. While not an exhaustive list, here are five of the big ones:

#### I'm protected because my industrial networks are isolated

False. Industrial information systems are often connected to enterprise networks and sometimes even directly to the internet. It is not uncommon to count a dozen or more internet connections per site, although managers are convinced that their industrial control systems (ICS) are completely isolated. Moreover, laptops and USB drives used by maintenance contractors are major vectors for spreading malware, even on isolated systems.

#### My firewalls protect me from cyber threats

Building a demilitarized zone (DMZ) between the enterprise and the industrial networks offers a necessary first level of protection. But isolating industrial networks can be an

back to top

obstacle to industry digitization projects, which require data to flow seamlessly between IT, operational technology (OT), and cloud domains. Organizations need to connect more devices, enable more remote accesses, and deploy new applications. You might even find third-party vendors installing cellular modems to gain remote access to your OT environment so that they can easily update or troubleshoot systems and devices. And what about new applications that require access to the cloud? Do you know what all your industrial devices and are you certain they are protected by your firewall? The truth is, the airgap approach to IoT/OT security is no longer sufficient.

### My industrial installation is not a potential target

This cannot be any more false. Even small companies possess sensitive data and can become the target of a cybercriminal. But the biggest threat might come from ransomware. The criminal business model of ransomware is now well established with ransomware-as-a-service (RaaS) making it even easier for anyone to launch attacks. As the fight against these cybercriminal organizations is becoming a priority all over the world, the FBI observed many hackers redirecting ransomware efforts away from 'big-game' and toward mid-sized victims to reduce scrutiny. And because these malware are more numerous, the probability of being unintentionally hit increases. A few years ago, WannaCry and NotPetya affected tens of thousands of industrial control systems, causing hundreds of millions of loss revenues, demonstrating that malware generally spread independently of any targeting strategies.

### I am protected because my industrial systems use proprietary protocols

False! Tenacious hackers can very well understand proprietary protocols. These are often intrinsically even more vulnerable because they have not been subject to much public analysis, unlike standard protocols, which have gone through many public reviews leading to continuous security improvements. Furthermore, taking control of an industrial workstation is all a hacker needs to disrupt production. These workstations usually run Microsoft Windows, which is well known by cybercriminals!

### Adding cybersecurity measures will complicate my daily work

To the slightest extent, yes. Securing your information systems might sometimes force you to operate in downgraded mode or might require modifying some operating procedures. However, downgraded does not mean stopping operations. Security tools are designed to prevent endangering your operations by identifying threats in advance. Letting malware disrupt your systems? Now that will complicate your daily work!
To learn more about how you can secure your industrial infrastructure, visit our IoT security page or contact us to have a conversation around your industrial IoT security challenges.

back to top

# Article from Corporate Partner, DT Asia

## Protecting Sensitive Information at the End of the IT Asset Lifecycle

Data is one of the most valuable assets that an organization owns. In today's world, data increasing value comes the need for greater responsibility for data privacy and security. Data breaches, legal and financial penalties, and reputational damage are disastrous consequences for improper handling of sensitive data. Meanwhile government agencies and industry segments are stipulating the proper handling of data such as Singapore PDPA (Personal Data Protection Act 2012) and Banking Act.

In this article, we will discuss different data destruction methods that are in compliance with global data privacy regulations, explain how data is securely erased in HDD and SSDs, and the features and benefits of Secure Data Erasure method. That is, ensure that data is protected at the end of the IT Asset lifecycle where secure data erasure software solution helps organizations erase data securely and comply with regulations.

**Different Data Destruction Methods**
So, what are the different data destruction method? The 3 main methods of data destruction are Data Erasure, Shredding and Degaussing. There is no one method that fits for all, and according to the issued Guidelines for Media Sanitization of The National Institute of Standards and Technology of the United States (NIST), all the 3 data destruction methods will be used based on the data classification and the data sensitivity.

**Data Erasure of HDD and SSD** uses certified software to destroy data, permanently and irreversibly deleting data from a storage device, such as computer, mobile device or USB Drives. The other two methods are Shredding and Degaussing using physical destruction of particular composite type devices. **Shredding of solid-state drive (SSD**) is the physical cutting to scrap the SSD storage device. Though effective, but also be risky and environmentally damaging. Risky in sense that there is no software generated tamper evident destruction report hence increasing the risk of inaccurate info which is susceptible to human error. **Degaussing of hard disk drives (HDD)** works by exposing the drive to strong magnetic field that disrupts the magnetic particles that store data on the disk. The trend is HDD no longer the standard storage type in almost all IT devices today.

Proper data erasure is demanded by many global data privacy regulations, such as the General Data Protection Regulation (GDPR), and those in ASEAN are Singapore (PDPA), Malaysia (PDPA), Indonesia (PDP), Philippines (DPA), Thailand (PDPA) and recently Vietnam (PDPA). In fact, as of January 2023, there are over 120 jurisdictions that have a data privacy law in place. These regulations require organizations to implement appropriate measures to protect the privacy of personal data, including erasing data securely when it is no longer needed. When these devices are no longer in use, failing to properly erase data can lead to serious consequences, including data breaches, identity theft, financial loss, and reputational damage.

back to top

| | Secure Data Erasure | Degaussing | Physical Destruction |
|---|---|---|---|
| Cost | Cost Effective | High upfront cost + Yearly maintenance of Degausser Hardware | High upfront cost + Yearly maintenance of Degausser Hardware |
| Duration | HDD – 500 GB (1 Hour) SSD – 500 GB (20 minutes) | Quick (Several seconds) | Moderate (Approximately 15 minutes) |
| Dismantling | No need dismantles of media from machine | Need dismantle media from machine (Increases destruction duration) | Need dismantle media from machine (Increases destruction duration) |
| Supported Devices | Efficient for HDD, SSD, USB Pendrive, Mobile Device & Tablets | Works for only HDD & Tapes | Provides highest level of security if shredded to 2mm in size |
| Deployment Flexibility | Performed Remotely, On-site or Off-site | Degausser weights from 25kg – 450kg will need to be move around, not convenient. | Shredder weights from 450kg – 1,350kg, not convenient at all to be moved |
| Reusability | Leaves the storage media / device usable condition ready for re-use or re-sell | Storage media deemed useless | Storage media deemed useless |
| Sustainability | Environmentally friendly | Not environmentally friendly, not healthy for human to be near a degausser | Not environmentally friendly |
| Accountability | Auto report generation upon erasure of tamper proof erasure report | Human generated degaussing report | Human generated degaussing report |

**Mechanism in Secure Data Erasure of HDD and SSD.**

Unfortunately, many organizations still rely on improper methods of data destruction such as simply format a hard drive or a delete files, thinking that this is enough to erase the data. However, these methods only delete the file references and not the actual data, which makes data recovery possible by someone with the right tools and knowledge.

Therefore, the crucial aspect of data handling is Secure Data Erasure. This method involves overwriting the entire drive with industry erasure algorithm, making it impossible to access any previous data stored on the drive. The software can be used to overwrite the entire drive, HDD and SSD, multiple times to ensure that all data is properly erased.

For HDDs, secure data erasure software overwrites the drive multiple times with random data, making it impossible to recover any previous data stored on the drive. This process is known as the Gutmann method and involves overwriting the drive 35 times with different patterns of data. Other erasure algorithm is the NIST Clear (1 Overwriting), NIST Purge (1 Overwriting + 1 Firmware based), DoD 5220.22-M E (3 Overwriting) and so on.

For SSDs, secure data erasure software uses a different process known as the ATA Secure Erase command. The command sends a signal to the drive to erase all data stored on it, including any data that may be in areas that are not easily accessible. This method is

back to top

effective for SSDs because it specifically targets the flash memory cells where data is stored, ensuring that all data is properly erased.

**Features and Benefits of an excellent Secure Data Erasure Software Solution**
A secure data erasure software solution is designed to help organizations securely erase data at the end of the IT Asset lifecycle while complying with global data privacy regulations. The key requirement is to be recognized and certified by the in-country authority such as Cyber Security Agency of Singapore (CSA) under the Common Criteria scheme. This certification ensures that the software solution meets stringent security standards and is recognized by many developed and developing countries that participate in the Common Criteria Recognition Arrangement (CCRA) which allows software solution to be utilized at government level. Other certifications are ADISA, BSI-Federal Office for Information security and Attingo shows no data on the media after a forensic data recovery on erased SSD.

Secure data erasure software solution is a comprehensive and user-friendly solution that offers features including the following: **1) Data Security**: By using advanced data erasure algorithms, permanently and irreversibly erases data from storage devices, making it impossible to recover even with sophisticated data recovery tools. This ensures that sensitive data remains secure and confidential, protecting organizations from data breaches and cyber-attacks. **2) Cost Savings**: By securely erasing data at the end of the IT Asset lifecycle, organizations can avoid costly data breaches and regulatory fines. Additionally, its user-friendly interface and ability to erase data remotely can help organizations save time and resources. **3) Comprehensive Solution:** By offering multiple data erasure methods and generating detailed erasure reports. It can be used on a wide range of storage devices such as Laptop, Desktop, Server, Storage, Loose HDD/SSD, USB storage devices & Mobile Device (iOS & Android) and can be used on-site, off-site or remotely, providing flexibility for organizations with varying needs. The detailed erasure reports provide a comprehensive and auditable record of the erasure process, ensuring that organizations can demonstrate compliance to internal and external stakeholders. **4) Environmental Responsibility:** By securely erasing data and properly disposing of IT Assets, organizations can reduce their environmental impact and promote sustainability. The software solution helps organizations comply with e-waste regulations by providing detailed erasure reports and chain of custody documentation**.** On top of that, upon secure data erasure the reusability of the media allows organization to re-use, donate, or re-sell the media or devices**.**

With the ever-increasing amount of sensitive data being generated and stored on electronic devices, the need to protect sensitive information from falling into the wrong hands avoid the risk of data breaches and regulatory fines. With Secure Data Erasure, not only organizations can have peace of mind knowing that their data is being securely erased and that they are complying with all relevant data privacy regulations, but also saving cost and contributing to the green environment.

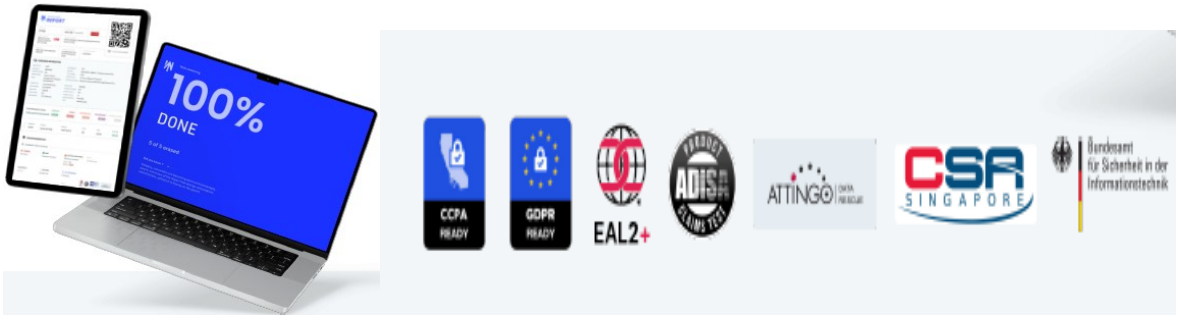
Contributor: Irving Oh
DTAsia Pte Ltd

back to top

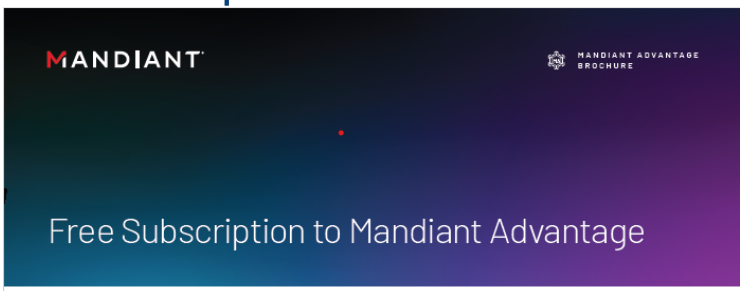
 

irving@dtasiagroup.com
21 Jun 2023

Adapted from Securaze whitepaper: Protecting Sensitive Information at the End of the IT Asset Lifecycle – Discussing the Importance of Secure Erasure.
Securaze® — A modern approach to securely and confidently erase data and diagnose assets — any device, anytime, anywhere.




# Article from Corporate Partner, Mandiant




**See more. Know more. Defend better.**

The Mandiant Advantage SaaS platform offers a controls-agnostic suite of modules to help organizations understand their external and internal risks and help automate operationalization.

With a free subscription, your organization—no matter what size—can get up-to-the-minute, relevant cyber threat intelligence, discover exposures and analyze internet assets across dynamic, distributed environments.

The free subscription includes both Mandiant Advantage Threat Intelligence and Mandiant Advantage Attack Surface Management.
**There's just one choice to make:**

**WHERE DO YOU START?**

**Mandiant Threat Intelligence Free**

Access real-time public data on threat actors, malware families and atomic indicators to discover who is targeting you. Make smarter security investments and better manage risk without added capital or operational expenditures.

**What's included?**
- Global dashboards providing actor, malware and vulnerability activity trends
- Access to open-source intelligence (OSINT) and indicators with contextual scoring
- News analysis with Mandiant expert judgements and commentary
- Multiple access options, including portal and browser plugin

Upgrade to Security Operations or even Fusion, which has FINTEL reports, dark web monitoring and more!

Start here: mandiant.com/ti-free

**Mandiant Attack Surface Management Free**

Get a comprehensive, true view of your environment through the eyes of the attacker. Continuously monitor, map and analyze external asset inventory to illuminate risks, prioritize vulnerabilities and help operationalize intelligence with speed and agility.

**What's included?**
- A collection of internet-facing assets, known and unknown, from across the organization
- Quarterly exposure monitoring across external assets and infrastructure
- Active and passive checks for vulnerabilities and misconfigurations
- Vulnerability and exposure remediation recommendations
- Mandiant expertise and intelligence automatically applied to exposed areas

Upgrade for full feature functionality, continuous exposure monitoring and access to the 250+ data integrations and more!

Start here: mandiant.com/ASM-free



Mandiant Threat Intelligence Freemium: mandiant.com/ti-free
Mandiant Attack Surface Management Freemium: mandiant.com/ASM-free

back to top

# Article from Corporate Partner, Contfinity

## Getting to Know Contfinity : A Chat with Alex Chan

***Contfinity** is a rising star in Singapore's cybersecurity constellation. We talk to their Head of Sales Alex Chan to find out what drives the company's leaders and employees, the vision for the industry and business, and advice for those who wish to develop a career in this fast-growing and exciting space.*

***Can you share with us Contfinity's growth journey in the cybersecurity space and what have been keeping you and your team busy lately?***

We just celebrated our second anniversary in June. The first two years were not easy. We started out on our own with little external help. The ride was rough and uneven, and we encountered many challenges. But we did not give up. The team persevered and overcame the odds. Today, as we enter our third year, I am proud to say that Contfinity is established as a key member of Singapore's cybersecurity ecosystem, helping businesses to be cyber secure and safe.

We have been appointed by Cyber Security Agency of Singapore (CSA) as a CISO as-a-Service consultant to help SMEs develop their cybersecurity health plans and attain industry certifications. We are humbled by the trust placed on us, and am working hard to fulfil stakeholder expectations.

We are now planning our next phase of growth. We started out as a systems integrator, expanded into cybersecurity consultancy, and now we are building a portfolio of solutions to provide holistic end-to-end security for customers. More importantly we are developing our human capital—

back to top

they are the key to success in any organisation.

***What are your views on the industry's challenges and opportunities?***

The key challenges are not just technological but also human. While advances in technology have enabled bad actors to commit more sophisticated cybercrimes, the industry's good actors (regulators, infosec vendors, MSPs, consultants, etc.) have always risen above the challenge to pre-empt and overcome the threats. This is good but it is not enough.

Businesses and individuals also need to play their part to make cyberspace safer for all. I see education, continual engagement, and, in extreme cases, even fear-messaging as necessary to raise the CQ (Cybersecurity Quotient) of those who need help. At Contfinity we constantly reinvent ourselves to play a constructive role in this mission. There are enough opportunities out there for all who wish to stand up and be counted.

***What drives you and your people, and how do you see Contfinity moving on from here?***

The team in Contfinity is mission-focused. Although we are a relatively new company, our people come with decades of experience in telco and ICT. Helping customers solve their problems and making the cyberworld a safer place for all give us the daily adrenalin rush to always do better and climb higher.

As a responsible corporate entity we also do our part for society. On this we are proud to work with AiSP and SG Digital Office to promote digital literacy and cybersecurity awareness in the community. In April we participated in Digital for Life Programme at Bukit Batok where we supported less privileged families in their digital literacy and cybersecurity journey. In June we participated in Celebrate Digital @ East Coast Digital Festival and the launch of Zhenghua CONNECTS at Senja Hawker Centre. We look forward to more such collaborations.

My vision for Contifinity and message to my team is for us to continue with our growth trajectory, overcome challenges cohesively, seize opportunities decisively, and always do good for our stakeholders.

***Finally do you have any advice for people who wish to enter the infosec industry?***

There is a popular Chinese idiom 学如逆水行舟，不进则退 – which means '*learning is like navigating against the waters; if you do not move forward you are regressing*'. Technology is evolving and moving forward endlessly. To stay relevant in the industry one needs to continually learn, relearn, unlearn. I would even venture to say that the same applies for all industries. My advice to all is to stay open-minded, stay curious and never stop learning. And learning needs

back to top

not be confined to textbooks. Every work assignment you take on and every person you meet can be a teacher and useful learning experience.

For any enquiries, please contact Mr Raymond Lim raymond.lim@Contfinity.com

# Article from our TCA 2022 Winner, Nanyang Technological University


**Going Beyond Building a Secure and Cyber-Resilient University**

The constantly evolving cyber landscape and the increasing complexity of cyber-attacks present a formidable challenge for all organisations. As a global leader at the forefront of education, research and innovation, with 40,000 students and employees, it is vital for Nanyang Technological University (NTU) to ensure that our systems remain up-to-date and well-protected. This is also encapsulated in one of our NTU 2025 strategic goals: to develop secure and cyber-resilient systems, as part of enhancing productivity and creativity at the University.

We are honoured to be recognised for our commitment towards cyber resilience, and excited to share the steps we have been taking, to create technology enhanced learning and working experiences for the OneNTU community.

**Empowering our People**

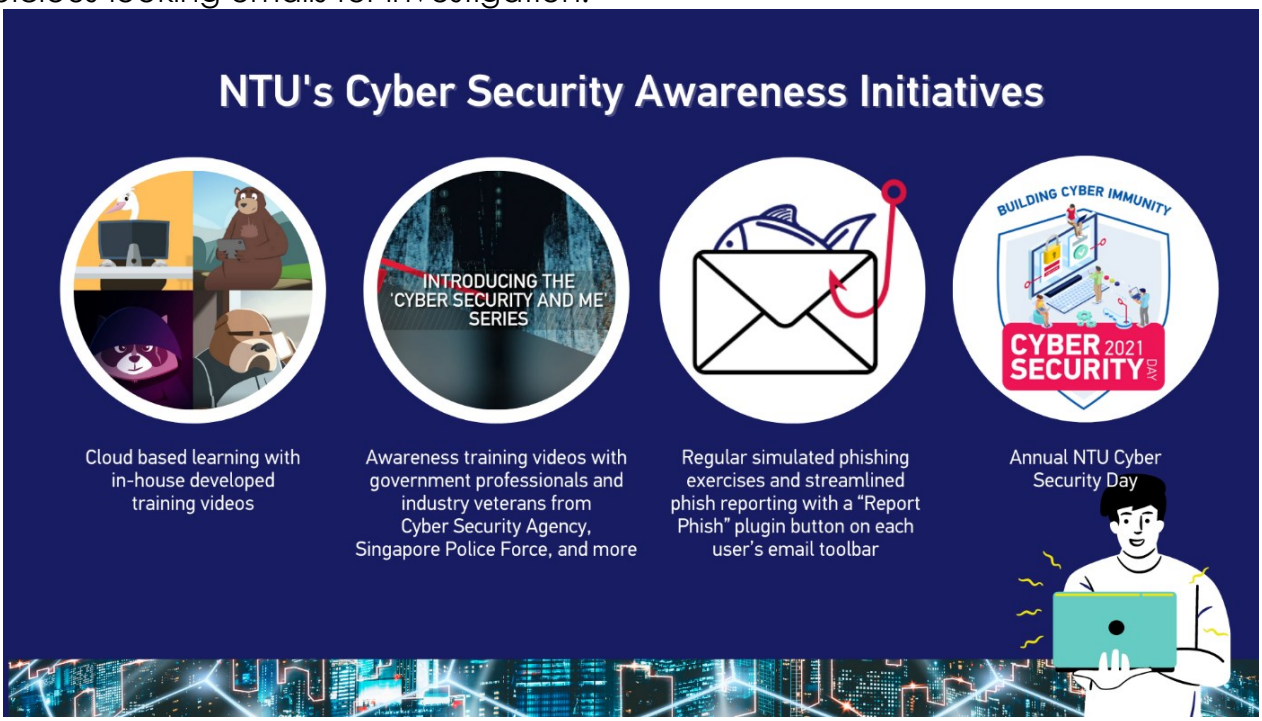
Humans form the first line of defence against cyber threats, but they can also be the weakest link. At NTU, we seek to cultivate a strong culture of vigilance and collective responsibility. People are at the heart of all positive change, which is why we need to empower the community with the right cybersecurity knowledge and practices.

back to top

Resources, such as in-house training videos, help raise crucial awareness on the importance of cybersecurity, and staff are encouraged to familiarise themselves with developments in the digital landscape through online learning tools, including LinkedIn and Coursera. Through expert talks, such as 'Tech Brown Bag' and 'Adaptive Skills Speaker Series', corporate industry leaders are invited to share their insights on how technology and data will shape the future of work.

Beyond education, the larger goal is to establish a comprehensive cybersecurity awareness ecosystem; synergising people, processes and technology to form a comprehensive defence against cyber-attacks. For example, the Centre of IT Services (CITS) worked to streamline phish reporting, by developing a "Report Phish" plugin button that appears on each user's email toolbar. This allows colleagues to promptly report suspicious-looking emails for investigation.




## Making our Cyber Defences Watertight

A system of checks had to be set in place, to ensure that NTU's cyber defences remain robust. All University-wide cybersecurity initiatives are frequently examined and enhanced, under the framework of **Identify, Protect, Detect, Respond and Recover**. A security checklist was also developed to comprehensively assess cybersecurity risks, enabling early detection and the implementation of necessary pre-emptive measures.

During the COVID-19 period, a large volume of interactions was moved online, from lessons, assessments, large-scale events and end-to-end transactions. To combat increased security risk, NTU conducted regular vulnerability and penetration scans on all major systems within its Data Centres. A real-time management dashboard provided a holistic view of the vulnerability statuses across different NTU entities.

In April 2020, NTU also established the **University-wide Security Operations Centre** to strengthen incident response capabilities. By harmonising security operations and incident response processes, NTU is able to provide a swift and coordinated response to cyber incidents.

back to top


The automation of threat investigation and data analysis can also help NTU respond more effectively to cyber threats. CITS deployed a detection and response (XDR) solution that collects and correlates data across multiple security layers (covering emails, endpoints, servers, networks, and cloud workloads). The ability to analyse data across the various technology stacks has improved critical performance metrics such as mean-time-to-detect and mean-time-to-respond. This enables NTU to prioritise its responses to threats across the organisation. Privileged Access Management and Data Protection Technology tools further supplement the University's existing data protection measures.

**Advancing Professionalism of the Cyber Security Community**

Beyond strengthening the University's digital systems, NTU also seeks to contribute to the wider cybersecurity community, by sharing the latest intelligence and nurturing talents in this field.

The NTU Computer Security Incident Response Team (CSIRT) obtained the FIRST (Forum of Incident Response Team) FULL membership in March 2021, which allows NTU to share the latest information on cyber threats and attacks, while learning best practices from experts in cybersecurity.

To address the growing demand for cybersecurity professionals, NTU offers over 20 courses and stackable certification, leading to the Specialist Certificate in Cyber Security. To cater to learners from all backgrounds and expertise levels, NTU's educational offerings also include the Graduate Certificate in Hardware Security Evaluation and Certification and the Master of Science in Cyber Security. With their industry-relevant curricula and rich hands-on learning opportunities, these programmes encourage the mastery of professional cyber security skills.

NTU also hosts key research centres and institutes conducting Cyber Security and Privacy Preservation research that deepens knowledge within these respective fields of study and contributes to Singapore's Smart Nation goals. These include the:

back to top

1) Centre for Smart Platform Infrastructure Research on Integrative Technology@NTU (SPIRIT)
2) Cyber Security Research Centre@NTU (CYSREN)
3) National Integrated Centre for Evaluation (NiCE)
4) Strategic Centre for Research in Privacy - Preserving Technologies & Systems (SCRIPTS)



back to top

**Looking Ahead**

Moving forward, NTU will continue to forge close collaboration with higher learning institutions, industry players and research institutes to enhance our cyber resilience, while accelerating NTU's digital transformation to power innovation and growth.

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

*The content and information provided in the document do not constitute the opinions and views of the Association of Information Security Professionals. AiSP remains neutral to the products and/or services listed in the document.*

# PROFESSIONAL DEVELOPMENT

## Listing of Courses by Wissen International


**EC-Council's Blockchain Certifications Overview**

EC-Council's blockchain certification courses are curated by experts to support the growing demand for skilled blockchain professionals.

These programs have been designed to meet the industry requirements of developers, business leaders, and fintech professionals in this rapidly growing area.

Our blockchain certification courses consist of three knowledge and competency areas: development, implementation, and strategy.

During the course, students get exposure to multiple blockchain implementation concepts and

back to top

a unique guideline for sustainable and scalable blockchain development using quantum-resistant ledgers.

Considering the market opportunity and skills required for different target groups, EC-Council has launched three new blockchain programs:

**1. Blockchain Business Leader Certification (BBLC)**
**2. Blockchain Fintech Certification (BFC)**
**3. Blockchain Developer Certification (BDC)**

Blockchain technology is becoming more prominent in today's digital world, and getting certified is a great way to showcase your knowledge and lend credibility to your resume.

EC-Council's expert-designed courses will provide you with hands-on experience and help you gain valuable insights that are mapped to real job roles.

**Special discount available for AiSP members, email aisp@wissen-intl.com for details!**

# Listing of Courses by ALC Council


## Stand out from the crowd

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

We offer the most in-demand cyber certifications including:

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

## The right training makes all the difference

back to top

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

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

**AiSP Member Pricing – 15% discount**

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

**Upcoming Training Dates**

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

**Special Offers.**

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

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

**Thank you.**

***The ALC team***

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



back to top

# Qualified Information Security Professional (QISP®)

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


back to top

## QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

**Online**


back to top

**Physical**


Companies around the world are doubling down on their security as cyber-attacks see an increase in frequency, intensity and severity. It is thus critical for businesses and organisations to have Qualified Information Security Professionals to manage cybersecurity threats and incidents.

To support the development of personnel in this profession, the Association of Information Security Professionals (AiSP) is offering the Qualified Information Security Professional (QISP) Programme.

This special five-day training programme is based on AiSP's Information Security Body of Knowledge (IS BOK) 2.0. This course will prepare participants for the QISP examinations. After attending this course, participants will also be able to understand and attain knowledge in these areas:

- Enterprise Governance
- Risk Analysis and Management
- Security Controls
- Security Principles and Lifecycle
- Business Continuity Planning
- Develop and Implement Security Goals, Objective and Strategy and Programs
- Maintain and Review Security Operations

**COURSE DETAILS**

**2023 Course dates can be found on https://www.aisp.sg/qisp_training.html**
**Time: 9am-6pm**
**Fees: $2,800 (before GST)***

back to top

**10% off for AiSP Members @ $2,520 (before GST)*
***Utap funding is available for NTUC Member**
*** SSG Funding is available!**

## TARGET AUDIENCE

- Professionals who wish to learn more or embark into Cybersecurity
- Security Professionals who will be leading or taking on a senior management/technical role in ensuring Enterprise Governance is achieved with Corporate, Security and IT Governance

## COURSE CRITERIA

**There are no prerequisites, but participants are strongly encouraged to have:**

- At least one year of experience in Information Security
- Formal institutional training in cybersecurity
- Professional certification in cybersecurity

*For registration or any enquiries, you may contact us via email at secretariat@aisp.sg or Telegram at **@AiSP_SG**.*

Program Partner

Transformists NETWORK

Delivery Partners

Ai Network 360

OPUS ACADEMY

NETASSIST

back to top

# Cybersecurity Essentials Course


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

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

**Course Objectives**

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

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

back to top

- Cloud Computing
- Cybersecurity Operations

**COURSE DETAILS**

**Training dates for year 2023 can be found on**
**https://www.aisp.sg/cyberessentials_training.html**
**Time: 9am-6pm**
**Fees: $ $1,600 (before GST)***
**10% off for AiSP Members @ $1,440 (before GST)*
***Utap funding is available for NTUC Member**
*** SSG Funding is available!**

**TARGET AUDIENCE**

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

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

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: 2023) from 1 Jan 2023 to 31 Dec 2023. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. This does not include Plus! card holder (black-coloured card), please clarify with NTUC on your eligibility.

On **membership application**, please do not email your personal data to us via email if your information or attachment is not password-protected. Please send us your password via **Telegram** (@AiSP_SG).

Once we receive confirmation from NTUC on the validity of your NTUC membership, AiSP would activate your one-year complimentary AiSP Affiliate membership.

**CPP Membership**


For any enquiries, please contact secretariat@aisp.sg

back to top

**AVIP Membership**
AiSP Validated Information Security Professionals (**AVIP**) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development, and career progression for our professionals.

**Membership Renewal**
Individual membership expires on 31 December each year. Members can renew and pay directly with one of the options listed here. We have GIRO (auto - deduction) option for annual auto-renewal. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.

**Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!**

**Please check out our website on Job Advertisements by our partners.**

For more updates or details about the memberships, please visit www.aisp.sg/membership.html

## AiSP Corporate Partners

back to top


































back to top

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

## AiSP Academic Partners

back to top

# Our Story…

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

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

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

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

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

# AiSP Secretariat Team

Vincent Toh
Associate Director

Elle Ng
Senior Executive

Karen Ong
Executive

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

back to top