AiSP

NEWSLETTER

March 2024

NEWS & UPDATE

New Partners

AiSP would like to welcome Genesis Networks and Telstra as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

New Corporate Partners

Genesis NETWORKS

Telstra

Continued Collaboration

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

CYBERSAFE YOUR SECURITY, OUR PRIORITY

eclypsium

News & Updates

Seamless Asia from 20 – 21 February

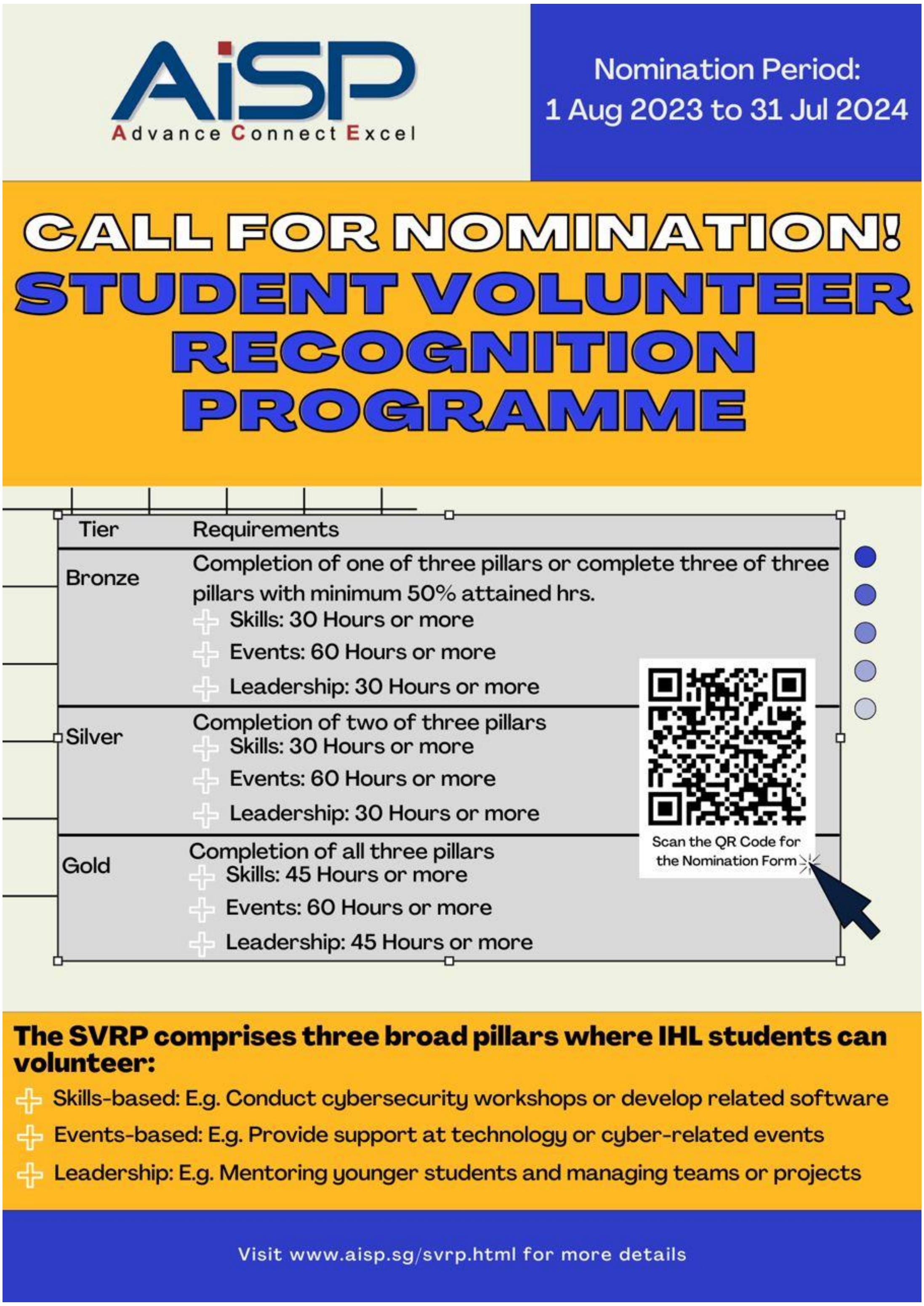
AiSP was invited to set up a booth at Seamless Asia on 20 -21 February at Suntec Convention Centre to share about AiSP to the participants. Thank you Seamless Asia for inviting us!

Chinese New Year Celebration with AiSP Advisory Council on 23 February

On 23 February, the last AiSP Advisory Council meeting has ended for this term and a Lohei session was held after the advisory meeting at Ensign Office. AiSP would like to take this opportunity to thank Prof Steven Wong for his unwavering support and invaluable contributions to the council.

back to top

Student Volunteer Recognition Programme (SVRP)



AiSP
Advance Connect Excel

Nomination Period:
1 Aug 2023 to 31 Jul 2024

CALL FOR NOMINATION!
STUDENT VOLUNTEER RECOGNITION PROGRAMME

Tier	Requirements
Bronze	Completion of one of three pillars or complete three of three pillars with minimum 50% attained hrs. Skills: 30 Hours or more Events: 60 Hours or more Leadership: 30 Hours or more
Silver	Completion of two of three pillars Skills: 30 Hours or more Events: 60 Hours or more Leadership: 30 Hours or more
Gold	Completion of all three pillars Skills: 45 Hours or more Events: 60 Hours or more Leadership: 45 Hours or more

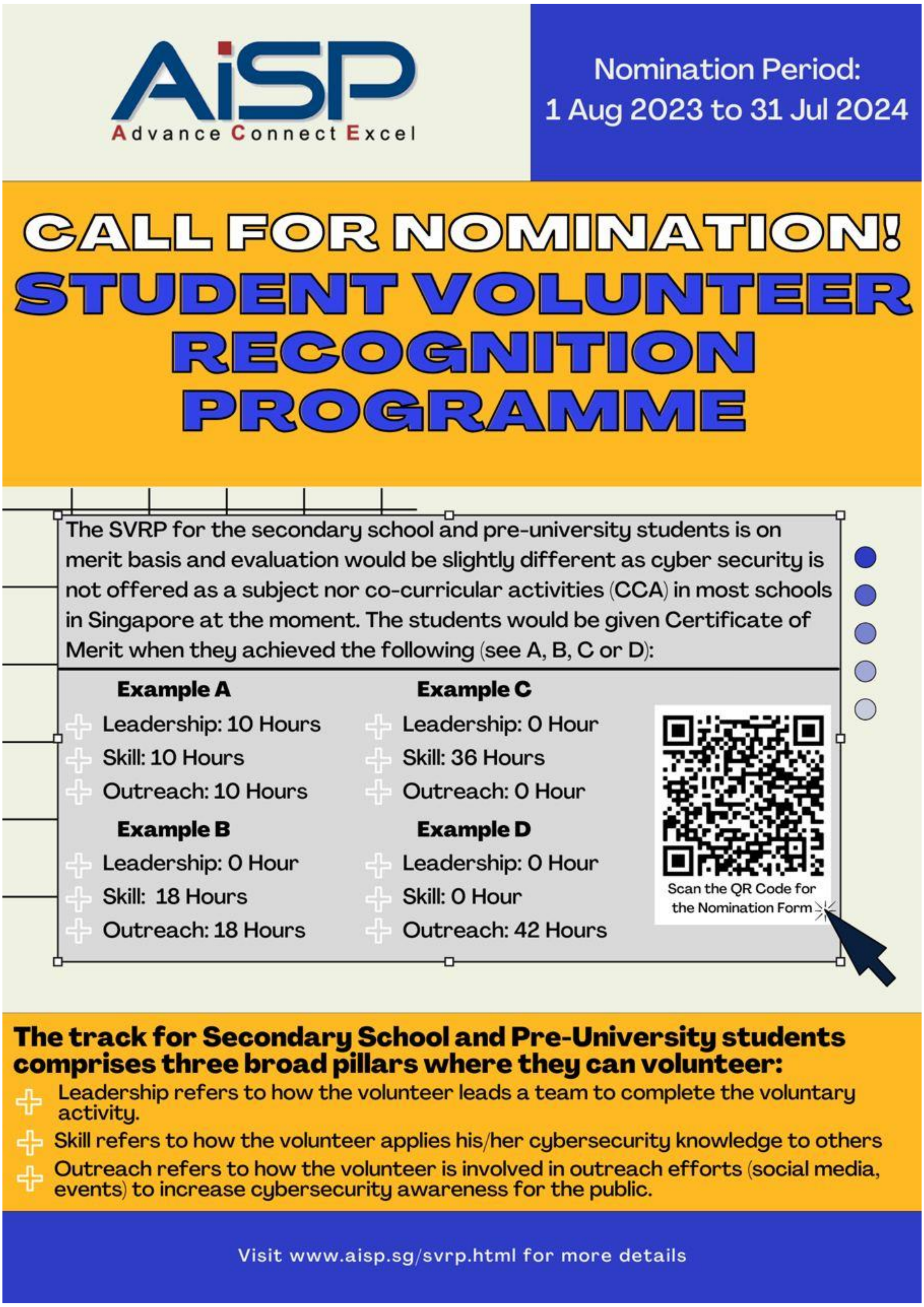
Scan the QR Code for the Nomination Form

The SVRP comprises three broad pillars where IHL students can volunteer:

- Skills-based: E.g. Conduct cybersecurity workshops or develop related software
- Events-based: E.g. Provide support at technology or cyber-related events
- Leadership: E.g. Mentoring younger students and managing teams or projects

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

back to top



Advance Connect Excel

Nomination Period:
1 Aug 2023 to 31 Jul 2024

CALL FOR NOMINATION!

STUDENT VOLUNTEER RECOGNITION PROGRAMME

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

Example A
- Leadership: 10 Hours
- Skill: 10 Hours
- Outreach: 10 Hours

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

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

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

Scan the QR Code for the Nomination Form

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

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

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

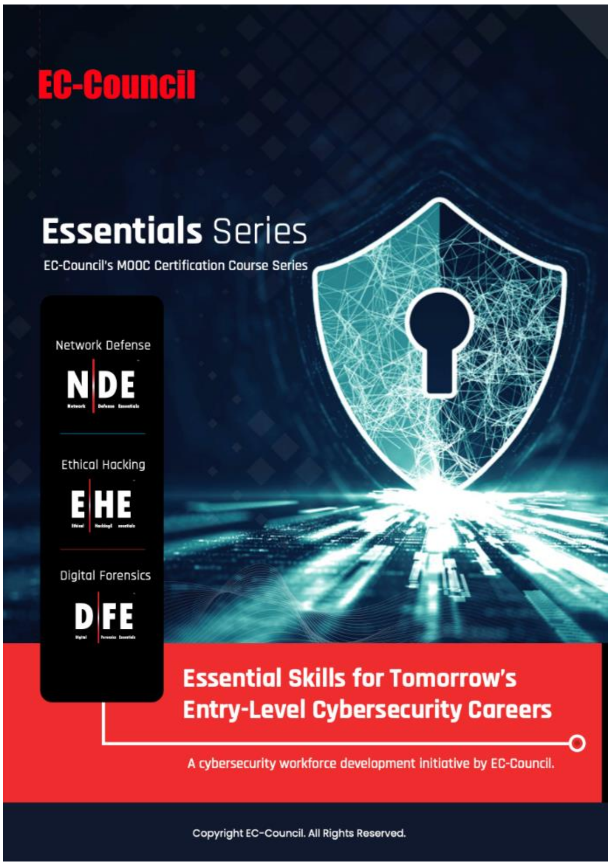
back to top

Elevating Cybersecurity Education Through Unprecedented Collaborations

In a pioneering initiative, EC-Council and Wissen have forged a collaboration with AiSP. This collaboration includes a sponsorship of 500 EC-Council Cyber Essentials certification vouchers. These vouchers aim to empower Polytechnic and Institute of Technical Education (ITE) students pursuing cybersecurity programs, enabling them to attain their inaugural industry certificate and commence their journey with EC-Council Essential certificates (NDE, EHE, DFE), thereby initiating their cybersecurity credentialing process.

Visit (https://www.wissen-intl.com/Essential500.html) and register to start your cybersecurity credentialing journey! Terms & Conditions apply.

About the EC-Council Cyber Essentials Certification
EC-Council's Essentials Series is the first MOOC certification course series covering essential skills in network defense, ethical hacking, and digital forensics. The Network Defense Essentials (N|DE), Ethical Hacking Essentials (E|HE), and Digital Forensics Essentials (D|FE) are foundational programs that help students and early career professionals choose their area of competency or select a specific interest in cybersecurity. The Essentials Series was designed to give students the foundation on which to build and develop the essential skills for tomorrow's careers in cybersecurity. These programs educate learners in a range of techniques across industry verticals, such as securing networks, mitigating cyber risks, conducting forensic investigations, and more.



EC-Council

Essentials Series

EC-Council's MOOC Certification Course Series

Network Defense
N|DE

Ethical Hacking
E|HE

Digital Forensics
D|FE

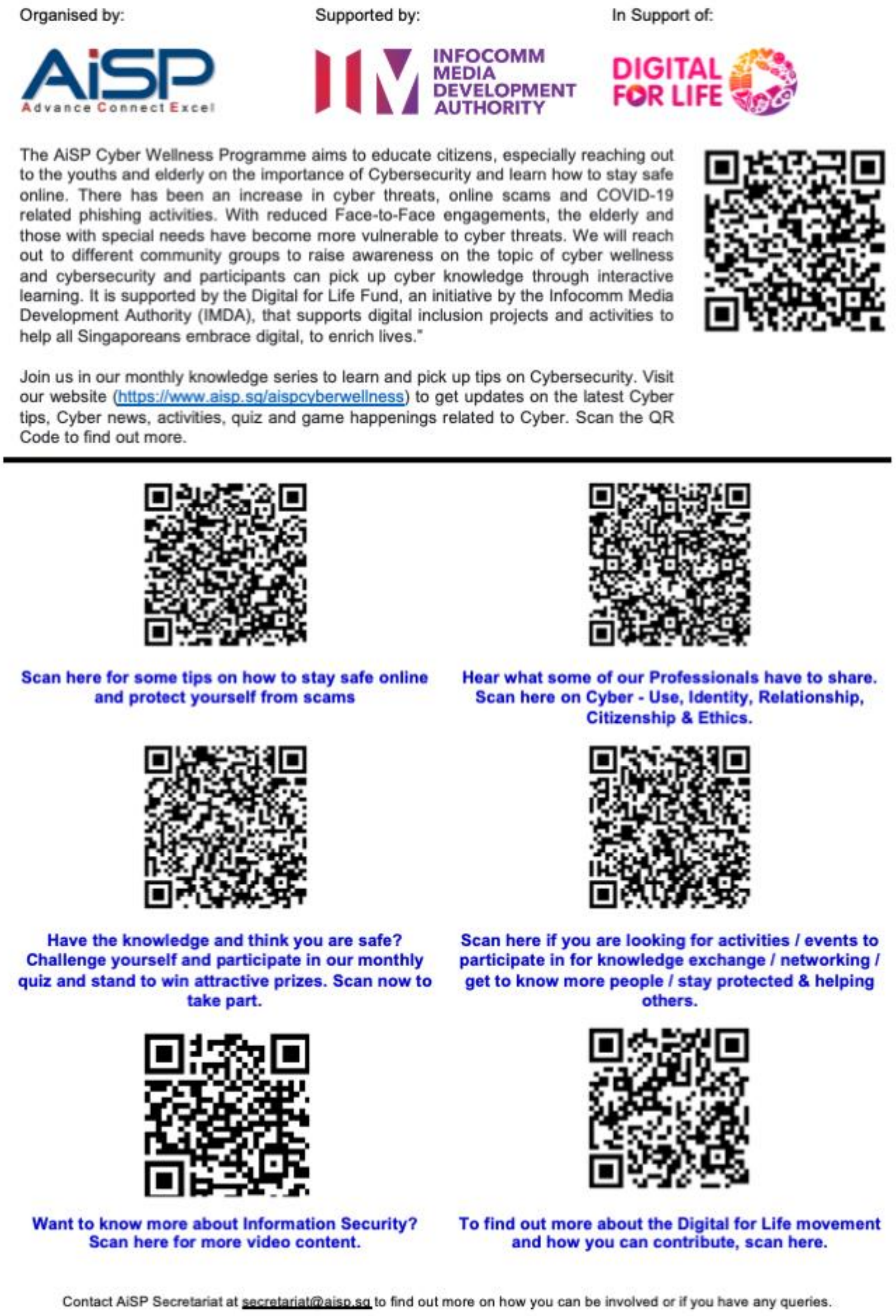
Essential Skills for Tomorrow's Entry-Level Cybersecurity Careers

A cybersecurity workforce development initiative by EC-Council.

Copyright EC-Council. All Rights Reserved.

back to top

AiSP Cyber Wellness Programme



Organised by: Supported by: In Support of:

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

Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP Cybersec Conference 2024 on 15 May

AiSP CyberSec Conference 2024

Sustaining Growth and Innovation Securely In This Challenging Business Environment

15 May 2024

9.30AM - 3PM

Suntec Convention Centre, Summit 1

SAVE THE DATE!
AiSP
Advance Connect Excel

AiSP
SILVER SPONSORS
BeyondTrust
KnowBe4
MAGNET FORENSICS
Veracity Trust Network
BRONZE SPONSORS
BLACKPANDA
CYBERSAFE
softScheck
xcellink.pte.ltd.
SUPPORTING PARTNERS
AEIS
AmCham
ASPRI
ASME
AUTOMATION SG
British High Commission Singapore
CREST
CSA cloud security alliance
CSCIS
CzechTrade
HFCAS
IASA
ISACA Singapore Chapter
SINGAPORE
OT-ISAC
associate
SCS
SFA
SGTECH
AHK
Spanish Chamber
U.S. COMMERCIAL SERVICE
Tech Talent Assembly

back to top

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

Our theme for this year conference is "Sustaining growth and innovation securely in this challenging business environment".

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.

Date : 15 May 2024
Time : 9AM – 3PM
Venue : Suntec Convention Centre
Guest of Honour:
Morning: AiSP Patron – Senior Minister of State, Ministry of Communications and Information & Ministry of National Development - Mr Tan Kiat How
Afternoon: Member of Parliament for Pasir Ris-Punggol GRC & NTUC U SME Director – Ms Yeo Wan Ling

Register here

back to top

Special Interest Groups

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

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

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

back to top

AiSP CISO SIG Networking & Lohei on 20 February 2024

AiSP organised our very first CISO SIG networking & Lohei event with the joyous vibes of Chinese New Year. Huge thanks to our speakers Johnny Kho, Andre Shori, Eric Wong, Wong Choon Bong, Sean Lim, and Chai Chin Loon for sharing their insights with our attendees. Thank you to our Corporate Partner, Wissen International for supporting the event!

We hope everyone enjoyed the networking and Lohei session.

back to top

The Cybersecurity Awards

THE CYBERSECURITY Awards 2024

The Cybersecurity Awards 2024 nominations is now OPEN!

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)

In its seventh year, The Cybersecurity Awards 2024 seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems. The Awards are organised by the Association of Information Security Professionals (AiSP), and supported by Cyber Security Agency of Singapore and the following professional and industry associations that are part of the Singapore Cyber Security Inter Association – Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Chapter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)2 Singapore Chapter, Operational Technology Information Sharing and Analysis Center (OT-ISAC), The Law Society of Singapore, Singapore Computer Society and SGTech.

back to top

If you know any individuals and companies who have contributed significantly to the cybersecurity industry, it is time to be recognized now! Nomination forms are attached for the submission according to the categories.

THE CYBERSECURITY Awards 2024

Professionals

Leader

Professional

Enterprises

MNC (Vendor)

MNC (End-User)

SME (Vendor)

SME (End-User)

Students

WWW.THECYBERSECURITYAWARDS.SG

NOMINATIONS NOW OPEN

PLEASE SEND YOUR NOMINATIONS TO THECYBERSECURITYAWARDS@AISP.SG

Send in your nominations to thecybersecurityawards@aisp.sg

For any enquiries, please email thecybersecurityawards@aisp.sg

Nomination will end on **3 May 2024**. All submissions must reach the secretariat by **3 May 2024**.

For more details on the awards, visit our website here!

back to top

THE CYBERSECURITY Awards 2024
Organised by
AiSP Advance Connect Excel
Supported by
CSA SINGAPORE
Supporting Associations
CSA cloud security alliance SINGAPORE CHAPTER
CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES
HTCIA
ISACA Singapore Chapter
ISC2 SINGAPORE
OT-ISAC
SCS Singapore Computer Society
SGTECH WHERE TECH MEETS
THE LAW SOCIETY OF SINGAPORE
Platinum Sponsors
CISCO
HUAWEI
ST Engineering
Gold Sponsors
BeyondTrust
DBS
ENSIGN INFOSECURITY
SANS
SIT SINGAPORE INSTITUTE OF TECHNOLOGY
TREND MICRO
wizlynx group

Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors for The Cybersecurity Awards 2024! Limited sponsorship packages are available.

back to top

Regionalisation

ASEAN-Japan Cybersecurity Board Meeting on 5 – 7 February

AiSP President, Mr Johnny Kho attended the ASEAN-Japan Cybersecurity workgroup meeting in Bangkok with Cybersecurity Association Leaders from both ASEAN and Japan on 5-7 February. We are pleased to share that AiSP has been appointed as the Vice-Chair for the ASEAN-Japan Cybersecurity Community Alliance.

2024 1st ASEAN - JAPAN
CYBERSECURITY WORKING GROUP MEETING
6 - 7 February 2024
Bangkok, Thailand
AJCCA
CYBER SECURITY BY ALL FOR ALL

back to top

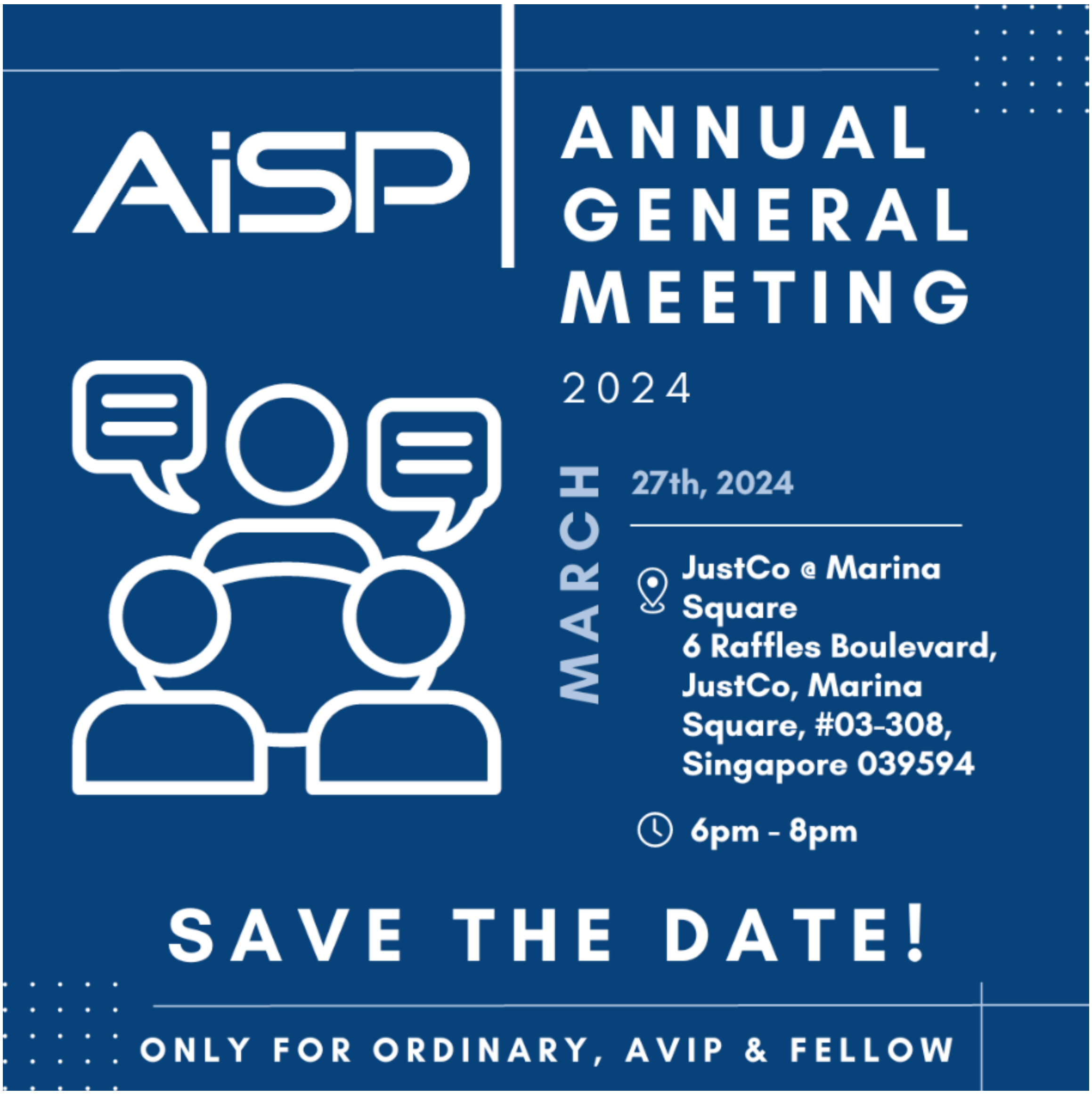
XCION 11th Conference 2024

AiSP will be supporting the XCION 11th Conference at Bali happening from 4 March 2024 to 6 March 2024. The Theme for 2024 is Charting the Future with Innovative and Secured Technologies. It will be attended by the Indonesian CIO Network (https://www.linkedin.com/groups/3942786/). As our valuable AiSP Corporate Partners, we are pleased to offer you a 20% if you are interested to speak at the event by been a sponsor.

Do contact AiSP Secretariat at secretariat@aisp.sg for the sponsorship package. Please note that it is based on first come first served basis and the organisers have more than 10 sponsors enquiring on it already. There will be 20% discount for our Corporate partners. No discount if you to go direct to the organisers or sign up at the website.
Please see some of the highlights of the video (https://www.youtube.com/watch?v=-eM-hNtMFZ0) happening on the 10th XCION 2023 that took place earlier this year March 2023.

XCION
XCION 11th Conference & Exhibition
CHARTING THE FUTURE WITH INNOVATIVE AND SECURED TECHNOLOGIES
4-6 March 2024
Nusa Dua, Bali, Indonesia

Annual General Meeting



AiSP

ANNUAL GENERAL MEETING

2024

MARCH 27th, 2024

JustCo @ Marina Square
6 Raffles Boulevard,
JustCo, Marina
Square, #03-308,
Singapore 039594

6pm - 8pm

SAVE THE DATE!

ONLY FOR ORDINARY, AVIP & FELLOW

Only for Ordinary, AVIP & Fellow Members
Please Register here by **13 March 2024**

Corporate Partner Event

Stop Ransomware Attacks Before They Start: Implement Prevention Techniques Today on 13 March

BeyondTrust

AiSP Advance Connect Excel

Stop Ransomware Attacks Before They Start: Implement Prevention Techniques Today

March 13, 2024, 1:00 pm – 2:00 pm UTC+08

Johnny Kho

Jon Barham

Register Now

Ransomware incidents have surged in recent years, hitting unprecedented levels with staggering statistics from 2023. Payments doubled to over $1.1 billion [1], signaling a significant comeback from the decline in 2022. The expanded use of cloud deployments, increased remote access, and other digital transformation initiatives have significantly widened the attack surface.

Fortunately, this malware variant has a critical weakness. No matter how it is delivered, almost all ransomware requires admin privileges to execute its payload, encrypt data, and further spread its tendrils.

Join Johnny Kho, President of AiSP and Jon Barham, Senior Solutions Engineer, BeyondTrust on March 13, 2024, at 1:00pm SGT, as they explore the

back to top

evolving landscape of ransomware, delving into common tactics, techniques and procedures and the most effective prevention strategies.

By attending this webinar you will:

- Learn how privileged identity plays a key role in ransomware attacks.
- Understand key ransomware mitigations based on the MITRE ATT&CK Framework.
- Learn how prevention techniques, including Privilege Account Management, User Account Control and Execution Prevention, are key in stopping ransomware.

1 – Chainalysis – "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline"

back to top

Securing Tomorrow: Mastering Zero Trust Segmentation on 26 March

AiSP Advance Connect Excel

STACK Meetup with AiSP: Securing Tomorrow – Mastering Zero Trust Segmentation

ORGANISED BY

AiSP Association of Information Security Professionals

STACK MEETUP

STACK Meetup with AiSP:

Securing Tomorrow - Mastering Zero Trust Segmentation

EVENT DETAILS

26 March 2024

6.30pm - 9pm

GovTech HQ, 10 Pasir Panjang Road, Mapletree Business City, Singapore 117438, Level 10, The Big Place

SUPPORTED BY

GOVTECH SINGAPORE

illumio

JOHNNY KHO
President
AiSP
Moderator

JOHN KINDERVAG
Chief Evangelist
Illumio
Panellist

BERNARD TAN
Director,
Cybersecurity Group
GovTech
Panellist

STEPHEN GANI
Chief Information
Security Officer
Maxeon Solar
Technologies
Panellist

In an era where cyber threats evolve at an alarming pace, organizations must adapt their security strategies to safeguard their digital assets effectively. Hosted by industry-leading experts, this event delves into the fundamental concepts of Zero Trust, emphasizing the critical need to contain the spread of breaches and ransomware across the hybrid attack surface when a breach occurs. Prevention and detection tools like firewalls, EDRs, or SIEM only give surface-level visibility into traffic flows that connect these applications, systems, and devices that are communicating across IT. They were not built to contain and stop the spread of breaches. Securing for tomorrow requires a different approach – the Zero Trust approach. Attendees will gain insights into the Zero Trust principles, which replace traditional perimeter-based security to focus on breach containment.

Win the Cyberwar with Zero Trust
Speaker: John Kindervag, Chief Evangelist, Illumio

Zero Trust is revolutionizing network security architecture: it is data and device-centric and designed to stop data breaches while protecting critical infrastructure and making cyber-attacks unsuccessful. In this session, the Creator of Zero Trust, John Kindervag, will discuss the reality of the concept of Zero Trust. Additionally, John will explain how adopting Zero Trust leads to accelerated and more secure cloud adoption. Learn how your Zero Trust journey will help you achieve tactical and operational goals that make cybersecurity a business enabler, not a business inhibitor.

back to top

Is Zero Trust a silver bullet?
Speaker: Bernard Tan, Director, Cybersecurity Group, GovTech

With the proliferation of cloud services, many organizations have begun embracing Zero Trust (ZT) security, in varying degree, to enhance their security posture. We have also begun our ZT journey, by baking ZT security principles in our architecting and solutioning for Government ICT systems, to ensure trusted exchange for both users-to-services and services-to-services transactions. I will share our on-going ZT journey thus far, and thoughts of ZT architecture alone is not a silver bullet to deter all cyber threats.

Zero Trust Segmentation: Strategies, Best Practices, and Real-World Implementations
Moderator: Johnny Kho, AiSP President

Panelists:
John Kindervag, Chief Evangelist, Illumio
Stephen Gani, Chief Information Security Officer, Maxeon Solar Technologies
Bernard Tan, Director, Cybersecurity Group, GovTech

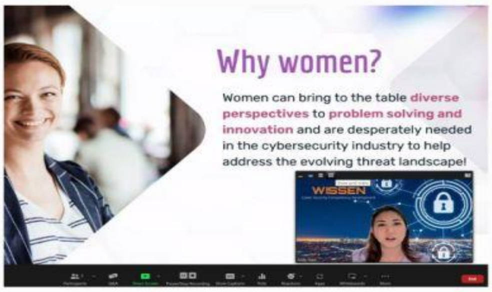
Date: 26 March 2024, Tuesday
Time: 6.30PM – 9.00PM
Venue: GovTech HQ, 10 Pasir Panjang Road, Mapletree Business City, Singapore 117438, Level 10, The Big Place
Registration: https://forms.office.com/r/FVJV6d4Rfs

back to top

Ladies in Cyber

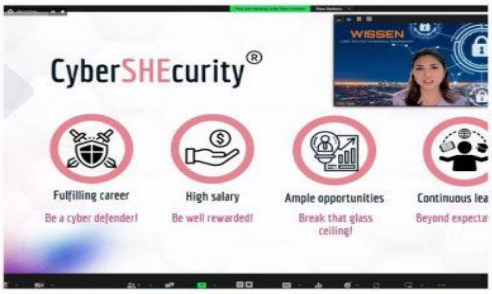
Sharing at BCSA's first Ladies in Cyber Event on 16 February

Our AiSP Ladies in Cyber Co-Lead Ms Judy Saw was invited by Brunei Cyber Security Association (BCSA) to speak at BCSA's first Ladies in Cyber Event virtually. Judy shared on the importance of Empowering Women in Cybersecurity with Certifications and participated in a panel discussion on "The Future of Cybersecurity: Emerging Trends and Women's Roles".



Why women?

Women can bring to the table diverse perspectives to problem solving and innovation and are desperately needed in the cybersecurity industry to help address the evolving threat landscape!



CyberSHEcurity®

Fulfilling career
Be a cyber defender!

High salary
Be well rewarded!

Ample opportunities
Break that glass ceiling!

Continuous lea
Beyond expecta

back to top

AiSP International Women Day Celebrations 2024 on 8 March

AiSP International Women Day Celebrations 2024 @ CISCO Office
8 MARCH 2024 | 6.30PM - 8.30PM

SUN XUELING
Panellist
Minister of State, Ministry of Home Affairs & Ministry of Social and Family Development

AILEEN YAP
Panellist
Assistant Director, Anti-Scam Command, Commercial Affairs Department, Singapore Police Force

TAY BEE KHENG
Panellist
President, Cisco ASEAN

SIMRAN TOOR
Panellist
CEO, SHE
(SG Her Empowerment)

SHERIN Y LEE
Moderator
AiSP Vice-President & Founder of AiSP Ladies in Cyber Charter

Organised By:

Supported By:

AiSP Association of Information Security Professionals
LADIES IN CYBER
CISCO
People's Association
SHE SG HER EMPOWERMENT
U associate an NTUC initiative

We are honoured to have Ms Sun Xueling, Minister of State in the Ministry of Home Affairs & Ministry of Social and Family Development as our Guest of Honour for the dialogue session together with Ms Aileen Yap (Assistant Director, Anti-Scam Command, Commercial Affairs Department, Singapore Police Force), Ms Tay Bee Kheng (President, CISCO ASEAN) and Ms Simran Toor (CEO, SHE – SG Her Empowerment). Ms Sherin Y Lee, AiSP Vice-President and Founder for Ladies in Cyber Charter will be the moderator for this event. The event is open to females only.

The details for the event are as follow:
Date: 8 Mar 24 (Fri)
Time: 6.30pm to 8.30pm
Venue: CISCO Office at 80 Pasir Panjang Rd, Building 80, Level 25 Mapletree Biz City, Singapore 11737
Dress Code: Smart Casual
Guest of Honour: Ms Sun Xueling, Minister of State in the Ministry of Home Affairs & Ministry of Social and Family Development
*Dinner will be provided at the event

Programme includes:

1. Sharing by Singapore Police Force on the Latest Scams
2. Sharing by CISCO Systems
3. Dialogue Session with MOS Sun Xueling
4. Dinner & Networking

Registration has closed.

back to top

Women in Tech + SkillsFuture Advice on 9 March

Presented by:

Central Singapore Community Development Council

Women In Tech

+ SkillsFuture Advice

Join our webinar to learn more about

- Latest workforce trends & future skills
- Useful resources for career & personal development
- Staying relevant in the tech era

Attendees will be eligible for a course sponsored by Central Singapore CDC. Terms & Conditions apply.

Saturday, 9 Mar 2024

10am - 11.30am

Webinar

Participate in dialogue with industry speakers:

Ms Joyce Huang
Senior Partnerships Manager, Lufthansa Innovation Hub

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

Joining us:

Ms Denise Phua
Mayor, Central Singapore District

SIGN UP NOW!

Scan QR code or visit go.gov.sg/cscdcsfa to register.

Supported by:

SKILLSfuture SG Lifelong Learning Institute

AiSP Association of Information Security Professionals

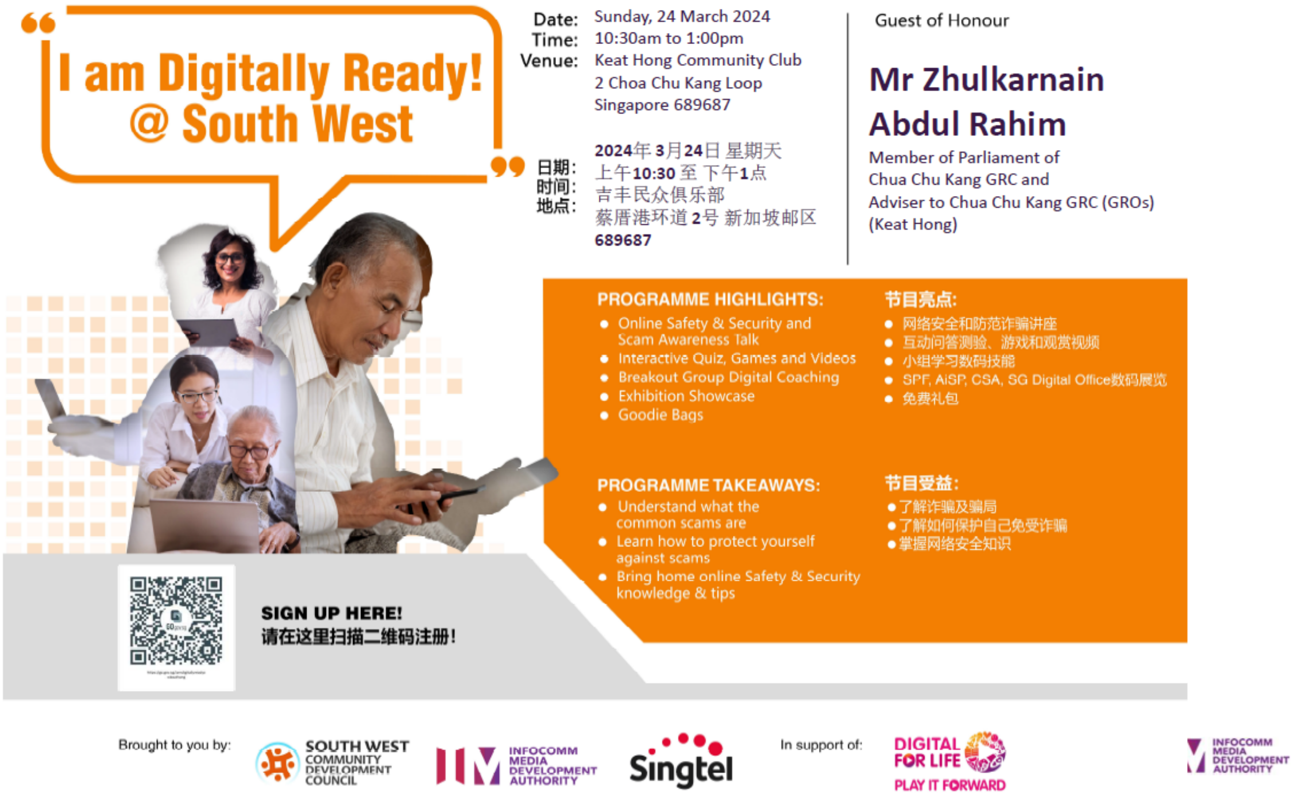
Lufthansa Innovation Hub

Register here

back to top

Digital For Life

I am Digitally Ready! @ South West on 24 March



I am Digitally Ready! @ South West

Date: Sunday, 24 March 2024
Time: 10:30am to 1:00pm
Venue: Keat Hong Community Club
2 Choa Chu Kang Loop
Singapore 689687

日期: 2024年 3月24日 星期天
时间: 上午10:30 至 下午1点
地点: 吉丰民众俱乐部
蔡厝港环道 2号 新加坡邮区
689687

Guest of Honour

Mr Zhulkarnain Abdul Rahim

Member of Parliament of
Chua Chu Kang GRC and
Adviser to Chua Chu Kang GRC (GROs)
(Keat Hong)

PROGRAMME HIGHLIGHTS:

- Online Safety & Security and Scam Awareness Talk
- Interactive Quiz, Games and Videos
- Breakout Group Digital Coaching
- Exhibition Showcase
- Goodie Bags

节目亮点:

- 网络安全和防范诈骗讲座
- 互动问答测验、游戏和观赏视频
- 小组学习数码技能
- SPF, AiSP, CSA, SG Digital Office数码展览
- 免费礼包

PROGRAMME TAKEAWAYS:

- Understand what the common scams are
- Learn how to protect yourself against scams
- Bring home online Safety & Security knowledge & tips

节目受益:

- 了解诈骗及骗局
- 了解如何保护自己免受诈骗
- 掌握网络安全知识

SIGN UP HERE!
请在这里扫描二维码注册!

Brought to you by: SOUTH WEST COMMUNITY DEVELOPMENT COUNCIL, INFOCOMM MEDIA DEVELOPMENT AUTHORITY, Singtel

In support of: DIGITAL FOR LIFE PLAY IT FORWARD, INFOCOMM MEDIA DEVELOPMENT AUTHORITY

CREST

Latest Exam Updates from CREST February 2024

Following the launch of our new syllabuses for our Certified Tester – Infrastructure (CCT INF) and Certified Tester – Application (CCT APP) exams, we wanted to share our next set of exciting updates to these exams.

CREST Certified Tester - Infrastructure
CREST Certified Tester - Application

What are the upcoming changes?

The major updates for both the CCT INF and CCT APP exams are detailed on the new

back to top

web pages for both exams. In addition to the updated syllabuses and content, we have also:

- **Increased the choice of locations:** all elements of the exam are being delivered with our exams delivery partner, Pearson VUE, meaning candidates can take the exams at over 1,100 Pearson VUE centres at locations around the globe, including Singapore and across Southeast Asia

- **Changed the exam components:** the certification has been divided into two parts: a multiple choice and written scenario exam - note the scenario element will no longer be combined with the practical element - and a separate practical exam

- **Created great flexibility in the approach:** candidates are now able to pick the order in which they take the components of the exam

- **Ensured the whole exam can be concluded within a day:** candidates can now book to sit both the written and practical elements of the exam on the same day and

- **Changed the use of own machine and tooling:** candidates will in future be able to access tooling within the Pearson VUE exam environment rather than bringing their own laptops, supported by access to the toolset ahead of the exam and the ability to upload materials in advance to assist you when taking the exams.

Information on these latest updates can be found on our dedicated web pages at:

CREST Certified Tester - Infrastructure
CREST Certified Tester - Application

Subsequent updates to watch out for

- Updated syllabuses for the Certified Simulated Attack Specialist (CCSAS) and Certified Simulated Attack Manager (CCSAM) exams

- Don't forget to check out our recently relaunched exams in Singapore for CRT and CPSA

Let's stay in contact!
To get the latest CREST communications via email, message marketing@crest-approved.org and ask to 'Subscribe to CREST News'.
You can also see us on social media here: https://www.linkedin.com/company/crest-approved/ and here: CREST (@CRESTadvocate) / X (twitter.com), and on our website www.crest-approved.org.

back to top

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
2 Mar	Be Cyber Safe Workshop for Seniors	Partner
4 - 6 Mar	XCION	Partner
8 Mar	AiSP International Women Day Celebrations @ Cisco	AiSP & Partner
9 Mar	Women in Tech + Skills Future Advice Webinar	AiSP & Partner
11- 13 Mar	Lag and Crash 2024	Partner
14 Mar	Agile Cyber Security BFSI Summit	Partner
26 Mar	AiSP x Illumio CPP event	AiSP & Partner
27 Mar	Securing digital assets in an AI-powered era	Partner
28 Mar	Bridging The Gap: Strengthen Your Cyber Security Posture	Partner
3 – 4 Apr	Cyber Security for Critical Assets APAC Summit and APAC Cyber Summit	Partner
3 - 5 Apr	Milipol Asia Pacific - Booth	Partner
16- 19 Apr	Black Hat Asia	Partner
16 Apr	Learning Journey to Crowdstrike for ITE West	AiSP & Partner
17 Apr	Learning Journey for Assumption English School	AiSP & Partner
18 Apr	AiSP 15th Anniversary Dinner	AiSP
18 – 19 Apr	PROTECT 2024	Partner
23 Apr	AiSP x BT Event (April)	AiSP & Partner
25 Apr	Smart Cybersecurity Summit	Partner

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

back to top

CONTRIBUTED CONTENTS

Article from CTI SIG

5 Essentials of Advanced Threat Intelligence

With thanks to input from friends at Fortinet & Rapid7.

CyberSecurity teams are today inundated with many more vulnerabilities and alerts than they can possibly address. A mandatory component of an effective cyber defense is a prioritized and automated response to threats relevant to your organization.

The traditional Common Vulnerability Scoring System (CVSS) lacks valuable context, including hacker motivation, intentions, and readiness to exploit vulnerabilities. Since all vulnerabilities cannot and should not be remediated at the same time, automated prioritization of critical vulnerabilities is essential.

At the same time, an explosion of increasingly sophisticated malware is creating a highly dynamic cybersecurity threat landscape, and many organizations struggle to keep up. The problem is compounded by the shortage of cybersecurity talent.

With advanced threat intelligence, an organisation can quickly evolve its security posture to address the latest threats and trends. Since exfiltration of data by a bad actor can occur within mere minutes, it's no longer feasible to rely on signatures or manual mitigation alone.

It's critical to integrate advanced threat intelligence into its enterprise cyber threat response processes, so one can quickly understand an impending threat, what entry points are vulnerable, and what actions you need to take.

The threat landscape for small and large organizations is growing more dire and complex every day. This requires a strategic response, and no network security strategy is workable without quality threat intelligence.

Information on known threats remains critical as their volume increases at staggering rates. But no threat intelligence program is complete without the ability to detect unknown threats—which now make up close to one-third of all new malware.

Companies building their threat intelligence infrastructure should look for solutions that use vast amounts of threat data, analyze that data using artificial intelligence (AI) and machine learning (ML), perform sandbox analysis when other methods are not definitive, and provide actionable intelligence for both strategic and tactical purposes.

When building a threat intelligence infrastructure, organizations need to consider a number of factors, including the amount and type of data collected, how well an organization's

back to top

threat intelligence is integrated with external threat intelligence, and how well threat intelligence can be shared across the organization.

Here are five essentials that organizations should look for in any threat intelligence solution:

1. A large intelligence network

While analysis of log data from an organization's own security infrastructure can provide a contextual picture, the best approach is to combine this threat intelligence with data from millions of other sources to provide a larger view of the global threat landscape. This is a case where more data is always better—as long as that data can be accurately refined into actionable intelligence.

2. Advanced threat detection using sandboxing

Sandboxing is a critical capability for detecting advanced persistent threats such as ransomware. With sandboxing, potential threats are observed in a simulated environment before being allowed onto the main network. The problem is that subjecting a large amount of traffic to full sandbox analysis is a time- and processor-intensive process, and it can slow network performance to a crawl. Organizations should look for a sandboxing solution that prefilters a big majority of that traffic safely, so that only the traffic that needs further analysis goes into the sandbox.

3. Advanced threat detection using AI/ML

When an organization depends on threat data from millions of sources over many years of time, analyzing that data and distilling it into something that can be used is daunting. Cyber criminals are now using AI and ML to design the next generation of malware, and making AI and ML a part of an organization's threat detection infrastructure is no longer an option.

Look for solutions that train their systems using all three learning modes of ML—supervised, unsupervised, and reinforcement learning—as such systems will become more and more accurate over time.

4. Actionable strategic intelligence of emerging threat trends

To be effective, threat intelligence must be distilled so that it can inform an overall network security strategy. It should be broad enough to disrupt an attack "somewhere along the kill chain, from initial system probing to network penetration to the final exfiltration of data."

Organizations should "[establish] a baseline of normal network behavior" so that they can "determine when something is behaving out of character." Good information results in prevention of many threats, early detection of others, and fast mitigation of all of them.

back to top

5. Actionable tactical intelligence on the latest threats and best practices

Threat intelligence also must inform tactical actions on a day-to-day basis. The ability to identify and block an attack in real time is paramount: “Threat intelligence that tips your organization off to an impending cyberattack is timely. Putting together the indications that
an attack was coming after it already happened is not.”

In order to be legitimately called actionable, threat intelligence information must be understood by people who are capable of taking action.

Of course, threat intelligence serves no purpose if the information cannot be acted upon to protect an organization against the threats identified. “It needs to be integrated—in real time—with a larger platform that delivers a layered cybersecurity posture.”

As the speed of advanced threats increases, moving from detection to protection requires the automation of security response. This does not eliminate humans from the process, and enables a more strategic use of scarce cybersecurity talent.

For known threats, organizations should ensure that they have a robust set of security tools that address threats across the entire attack surface. Ideally, these solutions will be a part of an integrated security architecture that allows for centralized visibility and control — and therefore true automation.

For advanced and unknown threats, organizations should have policies in place for automatic response to threats detected via a sandboxing solution, AI/ML, or other methods.

The current threat landscape requires both detection and response to occur at machine speed. Companies should consider adding services such as virus outbreak prevention (VOS) to disable zero-day threats before their signatures are developed, and content disarm and reconstruction (CDR) to create sanitized copies of previously infected files.
Dealing with advanced threats requires a strategic, proactive approach, and every network security strategy is only as good as the threat intelligence it is based on.

Actionable strategic and tactical information gleaned from a global threat intelligence network—and analyzed with AI/ML and sandboxing techniques—enables an organization to move into a proactive security posture.

This, combined with a strategic and integrated security architecture, reduces risk and supports the business in its digital transformation efforts.

Advanced Threats call for the need for Advanced Threat Intelligence, as illustrated above, and also call for the need for Advanced Threat Protection.

back to top

Advanced threat protection (ATP) refers to security solutions that protect your organization from advanced cyberattacks and malware that aim to exfiltrate, corrupt, or steal sensitive data. ATP can help an organization stay a step ahead of cyber criminals, even predicting attack vectors, putting the IT team in a better position to defend against them.

How Does Advanced Threat Protection (ATP) Work?

1. Cache Lookup

ATP systems, like Microsoft advanced threat protection and others, perform a cache lookup that examines a file to determine whether or not it is malicious.

2. Antivirus Scanning

Antivirus scanning is a key element of ATP security because it targets viruses trying to infiltrate your system through email or other vulnerable areas.

3. Static Analysis

Static analysis is the process of examining a file to see if it shows signs of malicious code or suspicious instructions.

4. Dynamic Analysis

With dynamic analysis, the suspicious file is executed in a controlled environment to allow the IT team to observe how it behaves. This can be performed by a managed security service provider (MSSP) advanced threat service using sandboxing. Because it contains the threat and renders it harmless, dynamic analysis can be a useful ransomware defense as well.

Problems Addressed By Advanced Threat Protection

1. Point-of-Sale (POS) Malware

POS malware can scan a point-of-sale system to find weaknesses. These can then be exploited by hackers for financial gain.

2. Malware Targeting the Banking Industry

Malware that targets online banking systems uses Domain Name System (DNS) cache poisoning, which involves directing someone to a fake website. The site looks like a legitimate one, and the user enters their login information, which is collected by the bad actor.

3. Ransomware

Ransomware holds a computer or its files hostage by encrypting them and then demanding that a ransom be paid to get a decryption code. Supposedly, the user will then be able to decrypt their system and regain control of it.

back to top

What Are the Most Common Tactics of Advanced Threat Attacks?

1. Phishing

In a phishing attack, the malicious actor sends links that seem to come from a trusted source. They then try to abuse this trust to gain access to sensitive information.

2. Installing Malware

After malware has been installed, cyber criminals can get inside the network, observe activity, and steal sensitive data.

3. Password Cracking

Not even the services of an MSSP can defend against cracked passwords, particularly if a company does not implement multi-factor authentication (MFA), which requires the presentation of more than one set of identification credentials.

4. Creating a Backdoor

When a hacker creates a backdoor, they open the way for re-entry into the system at a later date. They can use the backdoor as often as they like—at least until a proper ATP solution is deployed in place to eliminate the vulnerability.

How To Defend Against Advanced Threats

ATP for enterprises will often use sandboxing to protect against advanced threats. With sandboxing, the suspicious file is examined and then placed in a protected environment where it is shielded from the rest of the network. Here, it can be studied by the cyber defense team.

However, even sandboxing cannot protect a system from all threats. It is important therefore to not only use other tools, like next-generation firewalls (NGFWs), but also educate users within your company regarding the need to avoid:

- Clicking suspicious links or downloads
- Giving out sensitive login information to anyone they do not know
- Not protecting their passwords

back to top

Understand the Scale of Today’s Advanced Threats

The scale of the advanced threats faced by today’s organizations will vary based on the organization’s attack surface, vulnerabilities, and the type of assets it has that might attract attackers.

In some cases, an organization may under-protect their system because they fail to properly outline all facets of their attack surface. In other situations, a company may over-invest in a system that provides adequate protection but ends up wasting funds that could be better spent elsewhere.

Measure and Monitor the Effectiveness of Your Current Security

It is important to establish metrics that can be used to measure how effective your current security solution is. For some companies, it may be possible to tweak the current system or make minimal additions to make it adequate. In other cases, a complete overhaul may be necessary.

Leverage Your Vendor’s Expertise To Optimize Your Current Installation

While your IT team may have an impressive body of knowledge regarding the tools you have, your MSSP or another vendor will likely have even more. Take the time to glean insights from their knowledge regarding how to best configure your system to get the most out of your investment.

Take a Network-based Approach for 20/20 Visibility Into All Threats

The best way to defend your organization is to focus on attaining network-wide visibility. This involves analyzing all network traffic throughout its lifecycle, as well as the endpoints and devices that connect to the network.

Implement a Life-cycle Defense, Not Piecemeal Solutions

A lifecycle defense solution involves implementing a closed-loop system that studies the complete lifecycle of a threat, as well as the data that moves throughout your network. While tracing these lifecycles, you are able to observe the threat and its behavior from start to finish, as well as the path that network traffic takes—the same path it could expose to threats.

back to top

Author Bio

Anthony Lim
MAISP
Fellow, Cybersecurity, Governance & Fintech, Singapore University of Social Sciences

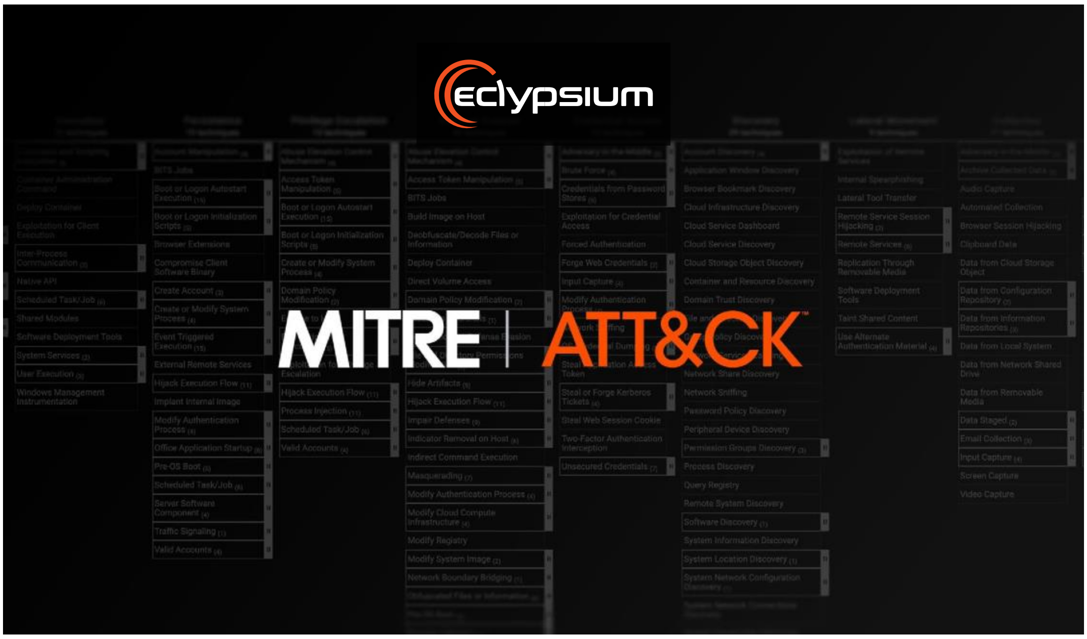
Anthony is a pioneer of cyber-security and governance in Singapore and the Asia Pacific region, with over 25 years' professional experience, as a business leader, consultant, advocate, instructor and auditor.

He has managed some national-level cybersecurity readiness assessment projects in Singapore and the region and was a co-author of an acclaimed international cloud security professional certification. He has held inaugural senior regional business executive appointments at Check Point, IBM and CA (now Broadcom), and was also client CISO at Fortinet and NCS. He has been active in industry association circles for nearly 2 decades, and is currently Advocate at (ISC)2 Singapore Chapter.

Anthony is an adjunct instructor and module developer for some tertiary academic & professional institutions. He has presented and provided content at many government, business, industry and academic seminars, committees, executive roundtables, workshops, trainings and media (print, broadcast, internet, including CNA, CNBC, Bloomberg, BBC) in Singapore, the region, and also for NATO, at Washington DC, Stanford University, ITU, Guangzhou Knowledge CIty and TsingHua University. He is a life alumni member of the University of Illinois, Urbana-Champaign.

back to top

Article from Corporate Partner, Eclypsium



FIRMWARE AND MITRE ATT&CK

As cybersecurity exploits and attacks have increased, few tools have proven as essential at stemming the tide and aiding defenders as the MITRE ATT&CK® framework. MITRE ATT&CK is a global, curated knowledge base that models and defines specific cyber adversary behavior "in the wild." The goal is to detail adversarial attack methods, lifecycles and known target platforms, and thereby enable defenders to see not only who and what they're up against, but precisely how to counter specific assaults.

Firmware is critical software that is embedded within every device. This is true whether enterprises deploy devices locally or rent them from cloud platforms. In either case, firmware is the first code to run and some of the most privileged code on any device, the bedrock that everything else relies on. Any compromise of this critical layer can undermine and subvert everything above it including the operating system, applications, and security controls.

It should be no surprise then that firmware also plays a critical role in modern cyberattacks, serving as a highly popular initial infection vector, as well as providing some of the most powerful methods of security evasion, persistence, and command-and-control.

In this paper, we'll analyze how firmware security— meaning boot integrity, component code, and hardware configurations—applies to the ATT&CK framework. In addition to covering firmware-specific attacker techniques and sub-techniques named in the framework, we'll also analyze the key role that strong firmware security plays in mitigating risk and disrupting threats across various phases of an attack. Specifically, readers will learn:

- Background on the ATT&CK Framework
- The role firmware in ATT&CK tactics and techniques

back to top

- Examples of real-world firmware attacks and risks
- Countermeasures and practices to mitigate firmware risks

MITRE ATT&CK BACKGROUND_

The MITRE ATT&CK Framework is a "globally-accessible knowledge base of adversary tactics and techniques based on real-world observations." The terms "tactics" and "techniques" have a specific meaning in the context of ATT&CK. The MITRE ATT&CK Philosophy Paper (PDF) defines the terms as follows:

1. Tactics - Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical objective: the reason for performing an action.
2. Techniques - Techniques represent "how" an adversary achieves a tactical objective by performing an action.

For example, Persistence is a tactic, and Pre-OS Boot is a technique used to establish persistence. In the most recent iteration of ATT&CK (last modified in November of 2021) there are 14 tactics and 218 underlying techniques. Of these 14 tactics, 2 are designated as PRE or preparatory steps, while the remaining 12 focus on the active phase of the attack.

The 14 tactics include:

- Reconnaissance (PRE)
- Resource Development (PRE)
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

It is worth noting that ATT&CK maintains separate matrices for Enterprise, Mobile, and ICS target types. While the underlying techniques vary between the matrices, the core tactics remain largely the same with the exception of small differences in the ICS matrix. For this document, we will use the Enterprise matrix as a reference, knowing that the core concepts apply to all versions of ATT&CK.

FIRMWARE AND ATT&CK_

Firmware is the most fundamental code on any given device. From the first moment that a device starts up to its every runtime operation to end-of-life, firmware is the gateway from the world of code to the physical processing and sharing of information required in all of computing. It is the bedrock that higher layer abstractions such as operating systems and applications rely on.

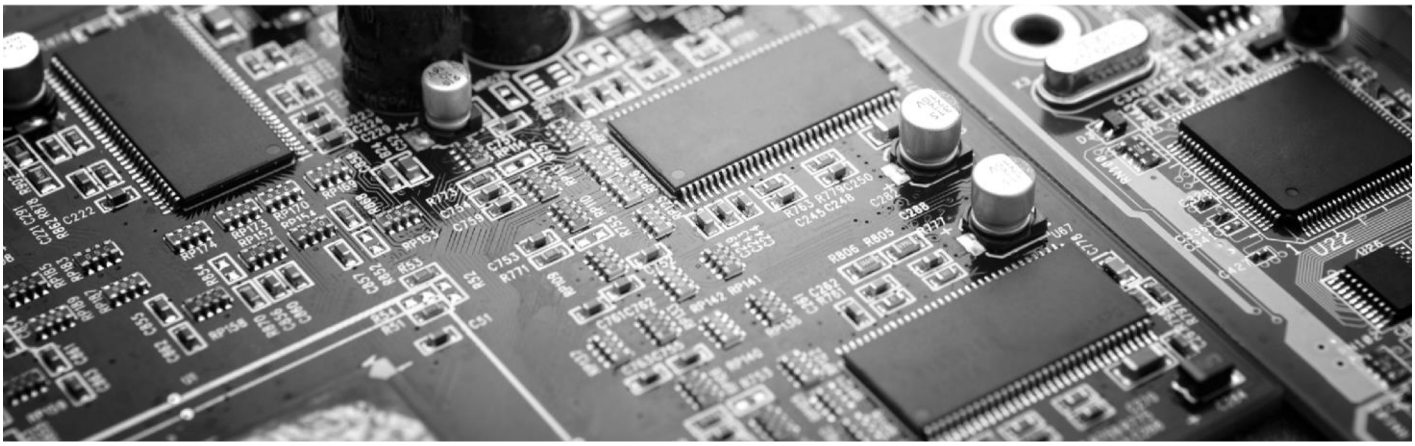
back to top

It used to be assumed that firmware code was sacrosanct: pristine, untouched, "black box" code. This caused cybersecurity teams to overlook firmware, or to provide a litany of reasons why they didn't want to assess, manage and secure it. Now, of course, many attackers know firmware better than defenders do. And compromising this firmware layer gives them the chance to subvert virtually any and all controls running in the "higher layers" of operating systems and applications.

Nation-state threat actors have heavily invested in firmware level threats for this reason, and those techniques and tools have trickled down to more financially motivated threat actors. However, firmware remains relatively unguarded in many organizations. This combination of motive, means, and opportunity creates considerable risk that we can see in the context of the ATT&CK Framework.

RECONNAISSANCE_

Reconnaissance is the first of the PRE tactics, and involves a variety of active and passive adversary techniques to identify target assets and vulnerabilities that can be targeted in later phases of the attack. Hardware and firmware play a key role in this technique. Vulnerabilities within the firmware of network devices such as VPNs have become one of the most popular initial access vectors into enterprises. Firmware vulnerabilities in particular have become a favored initial vector in these attacks because firmware is rarely updated as often as other code, and because exploiting these vulnerabilities can give an attacker full control over the device. Additionally, threat actors can scan to identify externally facing devices including servers, routers, and other infrastructure. Because of the lack of updates mentioned earlier, attackers can often infer the presence of firmware vulnerabilities based on the observed hardware version of the device.



Relevant ATT&CK Techniques	• Active Scanning - Vulnerability Scanning • Gather Host information - Hardware - Firmware • Network Security Appliances
References and Further Reading	• Widespread exploitation of VPN vulnerabilities • Publicly discoverable vulnerabilities in MikroTik routers

back to top

Firmware Countermeasures	Reconnaissance techniques are difficult to directly mitigate as they typically take advantage of systems and information that is inherently exposed to the public. However, this means it is all the more important for organizations to have highly reliable visibility of all their devices and any vulnerabilities they may have, so that any issues can be addressed before they are found by attackers.

RESOURCE DEVELOPMENT_

The second of the two PRE tactics, Resource Development allows an adversary to acquire infrastructure that will support the active phases of the attack. This could be acquiring servers or network devices that could provide command-and-control as well as trusted relationships with which to further expand in the environment. It is possible for attackers to implant firmware backdoors in networking devices such as switches as well as servers supporting bare-metal cloud services. These backdoors could be used by attackers to send malicious traffic and could persist even after the server is reprovisioned and used by other customers. Customers should independently verify the integrity of all networking gear and bare metal cloud assets not only to ensure the security of their data and assets, but also to ensure their hardware is not used as part of other attacks.

Relevant ATT&CK Techniques	• Compromise Infrastructure
References and Further Reading	• Backdoors in bare metal cloud services • CISA advisory on BlackTech threat group • Network Devices Whitepaper
Firmware Countermeasures	Scan all bare metal cloud assets to verify the integrity of the firmware and identify any vulnerabilities.

INITIAL ACCESS_

Initial Access is the first of the active phases of the ATT&CK Tactics, and firmware has proven to be one of the most popular vectors for initial access in real-world attacks. At a high level, firmware can be exploited remotely over networks, in the technology supply chain, or by attackers with physical access to a device.

Firmware within enterprise network devices such as VPNs, routers, and security appliances have become top targets across a wide range of threat actors. The trend was observed in Russian, Chinese, and Iranian state-based threat actors and quickly spread to financially motivated attackers including more than 20 ransomware groups and all five of the top ransomware groups. Exploiting vulnerabilities in the firmware and integrated code of these devices provide attackers with direct access into an enterprise with the ability to deliver malware to other users and devices.

Attackers can also gain access by compromising the technology supply chain of a device. Modern supply chains involve dozens of suppliers and subcontractors, providing attackers with many

back to top

opportunities to compromise a device before it is ever delivered to the enterprise customer. Additionally, supply chains can be compromised via official vendor update processes as was observed in the highly-damaging Solar Winds attacks. In total, the Breaking Trust project has identified 139 supply chain attacks and disclosures from the past ten years.

Attackers can also use physical access to compromise systems, often exploiting firmware within system components. For example, vulnerable components can expose devices to DMA attacks, which can allow attackers to directly read and write to system memory, and extend control over the execution of the kernel itself.

Relevant ATT&CK Techniques	• Exploit Public-Facing Application (e.g. VPN, network devices) • Supply Chain Compromise • External Remote Services - (e.g. Intel AMT, BMCs) • Replication Through Removable Media
References and Further Reading	• Network Devices Whitepaper • Supply Chain Risks • DMA Security and Zero Trust • Compromise by BIOS Disconnect • Remote UEFI Attacks
Firmware Countermeasures	• Proactively discover all devices within an enterprise including network devices • Proactively scan devices for vulnerabilities and prioritize any vulnerabilities used in real-world attacks • Verify the integrity of all system and component firmware of acquired devices • Verify all firmware updates and monitor firmware behavior following updates • Scan device components for vulnerabilities that would allow physical access attacks.

EXECUTION_

Attackers can compromise device boot processes in order to execute malicious code during or after boot. Alternatively, attackers can directly take advantage of component vulnerabilities to gain execution within system memory. Previously referenced DMA attacks provide an example where attackers can gain execution directly within system memory. This can allow an attacker to execute kernel code on the system, insert a wide variety of kernel implants, and perform a host of additional activities such as spawning system shells or removing password requirements. And as with all types of code, attackers can use social engineering to trick users into running the attacker's code such as malware that updates firmware or tricking users into performing malicious firmware updates.

back to top

Relevant ATT&CK Techniques	- Replication Through Removable Media - User Execution
References and Further Reading	- Abusing WPBT to Gain Malicious Code Execution - Evil Maid Attacks - FinSpy UEFI and MBR Bootkit - DMA Attacks
Firmware Countermeasures	- Scan devices to identify components that are vulnerable to DMA attacks and verify that all vendor DMA protections are properly enabled. - Scan devices for vulnerabilities that could allow attackers to compromise the firmware or boot process. - Verify that all available vendor protections are enabled and properly configured including protections included with UEFI, chipset vendor, OS vendor, and any OEM specific protections.

PERSISTENCE_
Persistence has always been one of the key reasons attackers seek to target firmware. Firmware code is integrated into system components themselves, instead of residing on traditional storage drives. This not only hides the attacker's code from traditional security scans but also ensures the code will persist even if a system's drives are completely erased, re-imaged or even replaced. The FIN8 ransomware group modified backup files in compromised NetScaler appliances to have a webshell that persisted even after the device was updated and rebooted.

Attackers continue to escalate their use of firmware implants and backdoors across a wide range of enterprise devices. UEFI implants such as LoJax, MosaicRegressor, and MoonBounce can target any UEFI-based system including laptops and servers. The recent HP iLOBleed implant provides an example of an implant that can target firmware within the powerful baseboard management controllers (BMCs) that enable out of band management of enterprise servers.

TrickBot provides an example of just how common such threats are becoming in the wild and how malware infections can quickly turn into persistent firmware backdoors. Already one of the most widespread and powerful trojans in the industry, TrickBot recently introduced new functionality dubbed TrickBoot, which automatically finds weaknesses in devices that allow the malware to establish persistence within an infected device's system firmware. Attackers can also apply this strategy by hiding within unused regions of memory in firmware known as "code caves".
Additionally, attackers can establish persistence by gaining control of a device's boot process to ensure their malicious code is always run during startup. Firmware rootkits and vulnerabilities such as BootHole can allow an attacker to execute their code before the operating system is even loaded.

back to top

Relevant ATT&CK Techniques	• Pre-OS Boot Techniques • Boot or Logon Initialization Scripts
References and Further Reading	• TrickBoot functionality for ongoing persistence • HP iLOBleed • MoonBounce • LoJax • MosaicRegressor • Code caves and hiding code in firmware
Firmware Countermeasures	• Scan devices to identify any vulnerable components or misconfigurations that would allow attackers to write to firmware or compromise the boot process. • Proactively verify the integrity of all firmware to identify any signs of implants or firmware compromise, particularly after any known malware incident. • Verify that all available vendor protections are enabled and properly configured including protections included with UEFI, chipset vendor, OS vendor, and any OEM specific protections.

PRIVILEGE ESCALATION_

Security teams often think of privilege escalation in the context of escalating from users privileges (Ring 3) to Administrator privileges or seeking out kernel privileges (Ring 0) at the system level. And while these are the highest privileges available to the OS, firmware sits beneath the kernel. As a result, malicious code in the firmware can subvert the kernel and thus possess even higher privileges, often referred to as Rings -1 through -3.

Attackers have a variety of techniques at their disposal to escalate privileges to these “negative” rings, both with user or administrator privileges. This involves a top-down approach to compromising firmware that can allow any standard malware infection to escalate privileges to the underlying firmware layer. This can include the use of malicious or vulnerable device drivers, the aforementioned BootHole vulnerability, and a number of other firmware or boot vulnerabilities.

Relevant ATT&CK Techniques	• Exploitation for Privilege Escalation • Boot or Logon Initialization Scripts
References and Further Reading	• Escalation via BootHole on devices even when protected by Secure Boot. • Escalation via driver vulnerabilities • SMM Vulnerabilities

back to top

Firmware Countermeasures	• Scan devices to identify any vulnerable components or misconfigurations that would allow attackers to write to firmware or compromise the boot process. • Make sure that devices are using the latest stable OS and bootloaders, and that the dbx revocation database is up to date. • Verify that all available vendor protections are enabled and properly configured including protections included with UEFI, chipset vendor, OS vendor, and any OEM specific protections. • Scan devices for malicious bootloaders and exploit code

DEFENSE EVASION_

Compromising a device's firmware and boot process gives attackers the opportunity to subvert security controls running at the level of the operating system. Firmware also directly controls the functions of device components in ways that may not be visible to the operating system itself. For example, the well-publicized Equation Group implants used malicious firmware to create hidden sections within a drive that were invisible to the operating system itself. This also meant that security tools were blind to these areas of the drive, allowing attackers to hide malicious code and evade security scans.

Additionally, rootkits and other malicious code execution within the UEFI environment can allow attackers to directly patch the OS kernel itself. This makes it possible to silently disable security features within the OS or third-party security tools. The Hacking Team implant, and the derivative MosaicRegressor UEFI implants, are well-known examples of sophisticated tools that use UEFI rootkits in order to evade traditional security controls.

Relevant ATT&CK Techniques	Rootkit Pre-OS Boot
References and Further Reading	Exploiting BootHole to install bootkits on devices. Hacking Team and MosaicRegressor Implants Equation Group SSD implants Demonstration of Firmware-Based Evasion
Firmware Countermeasures	Scan devices to identify any vulnerable components or misconfigurations that would allow attackers to write to firmware or compromise the boot process. Make sure that devices are using the latest stable OS and bootloaders, and that the dbx revocation database is up to date. Verify that all available vendor protections are enabled and properly configured including protections included with UEFI, chipset vendor, OS vendor, and any OEM specific protections.

back to top

	Scan devices for malicious bootloaders and exploit code

CREDENTIAL ACCESS_

Modern devices go to great lengths to protect passwords and credentials on the device. In addition to using firmware threats to steal credentials from system memory (e.g. DMA attacks), attackers can use side-channel analysis to extract credentials from even the most secure components of a system including the Trusted Platform Module. Additionally, firmware attacks against routers and networking gear can allow attackers to perform machine-in-the-middle attacks to steal credentials or intercept MFA challenges.

Relevant ATT&CK Techniques	• Credentials From Password Stores • Adversary-in-the-Middle • Exploitation for Credentialed Access
References and Further Reading	• TPMFail to extract private authentication keys • Router vulnerabilities that can enable machine-in-the-middle attacks. • Spectre and Meltdown to steal passwords • ROCA vulnerability to steal keys from TPM
Firmware Countermeasures	• Scan devices for vulnerabilities in TPM, processors, and other components that can enable side-channel attacks or collection of credentials. • Discover all network devices and identify vulnerable or out of date firmware.

COMMAND AND CONTROL / EXFILTRATION_

Firmware and hardware components can be used by attackers to establish command-and-control channels that are fully independent of the host operating system. For example, Intel's AMT firmware runs inside the management engine (ME) chip and contains its own network stack independent of the operating system. Attackers such as the PLATINUM group have used these capabilities as command-and-control and exfiltration channels that avoid any host-based controls running on the device.

Additionally, compromised firmware on network devices and interfaces can be used to reroute traffic, enabling both command-and-control and data exfiltration.

back to top

Relevant ATT&CK Techniques	• Non-Application Protocol • Ingress Tool Transfer
References and Further Reading	• PLATINUM using AMT to bypass Windows firewall • TrickBot use of MikroTik routers for C2
Firmware Countermeasures	• Scan devices for vulnerabilities in AMT and ensure AMT features are properly secured. • Identify all network devices and IoT components and scan for vulnerabilities. • Verify the integrity of AMT firmware and network device firmware.

IMPACT_
With access to system firmware or firmware on device drives, attackers can easily destroy data, disable components, or disable the system entirely. The BlackEnergy attacks on critical infrastructure in Ukraine in 2014 provided an example of the incredible potential for attackers to cause damage via firmware. Fast forward just a few years and the same concept has gained traction with ransomware such as EFILock ransomware, which uses malicious bootloaders to disrupt the boot process and gain control over victim machines, or the more recent iLOBleed implant, designed to "brick" HPE servers by manipulating the "integrated lights out" functions in their baseboard management controllers (BMCs).

Relevant ATT&CK Techniques	• Data Destruction • Disk Wipe • Firmware Corruption • System Shutdown and Reboot
References and Further Reading	• Using firmware to remotely brick a server • Russian attack on SATCOM networks • MBR Wipers - Hermetic Wiper. WhisperGate, NotPetya • Impacts of attacks on Ukrainian powergrid • QNAP ransomware targeting NAS firmware • VPNFilter attacks
Firmware Countermeasures	• Scan devices to identify any vulnerable components or misconfigurations that would allow attackers to write to firmware or compromise the boot process. • Proactively verify the integrity of all firmware to identify any signs of implants or firmware compromise.

back to top

CONCLUSIONS AND NEXT STEPS_

While ATT&CK covers a broad range of activities, this paper seeks to superimpose a firmware-oriented perspective over the framework and introduce some of the many ways firmware can be used and abused in modern attacks and bridge those technical and procedural gaps

However, it is far from an exhaustive list. As some of the most privileged and powerful code on a device, there are virtually unlimited ways that attackers can use firmware maliciously. In this example, the Cybersecurity and Infrastructure Security Agency (CISA) has used ATT&CK to map Trickbot malware tactics to a number of deep and hard-to-detect techniques, down to and including UEFI firmware compromise.

Firmware risks extend to virtually every phase of an attack, and it requires security teams to take a consistent and comprehensive approach to firmware security within their organizations. As a result, this examination of MITRE ATT&CK through a “firmware lens” may pose new challenges and concerns for cybersecurity strategists and their teams. However, it is important to note that as threat actors continue to shift their focus to firmware, new security tools are also available that can help security teams incorporate and automate firmware security into their existing practices.

Built on industry-leading expertise and research, the Eclypsium supply chain security platform makes it easy for organizations to protect the IT infrastructure that powers their operations. Eclypsium helps security teams to protect critical hardware, firmware, and software from supply chain attacks. With Eclypsium, you gain instant expertise into the below-the-OS attack surface and can quickly and simply implement critical security controls: asset inventory, vulnerability management, and threat detection. If you would like to learn more, we recommend the following resources:

- Take a tour of the Eclypsium platform.
- To stay up to date with latest firmware security news, please subscribe to the Below the Surface Threat Report
- To learn more about Eclypsium, please contact our team at info@eclypsium.com.

ABOUT ECLYPSIUM_

Eclypsium’s cloud-based platform provides digital supply chain security for critical software, firmware and hardware in enterprise infrastructure. Eclypsium helps enterprises and government agencies mitigate risks to their infrastructure from complex technology supply chains. For more information, visit eclypsium.com.

back to top

Article from SVRP 2023 Gold Winner, Johanan Chi Song En (RP)

How do you think SVRP has directly impacted your cybersecurity journey?
SVRP has been a great motivation for me. Last year, I managed to obtain the SVRP Gold Award and it was very motivating to me as it seemed like an appreciation of my efforts and work. Not only that but seeing my fellow peers and teachers at the ceremony has made me appreciative of the people I have around me. These were the people who has helped me throughout my journey and seeing them all in one place, celebrating each other's accomplishments was a great feeling.

How has SVRP inspired you to contribute to the cybersecurity field?
SVRP has inspired my peers to contribute to the cybersecurity field in various ways. When my friends and I first started our cyber security journey, we were clueless as to what to except and honestly didn't even know that there were various awards around in recognition of students' efforts. When we heard about the award, you could tell that there was a spark of motivation which fueled a passion to learn, grow, and contribute to the field. As anyone would be happy to receive an award, this was our first external award that we knew of and which made us contribute and grow step by step closer to the award.

back to top

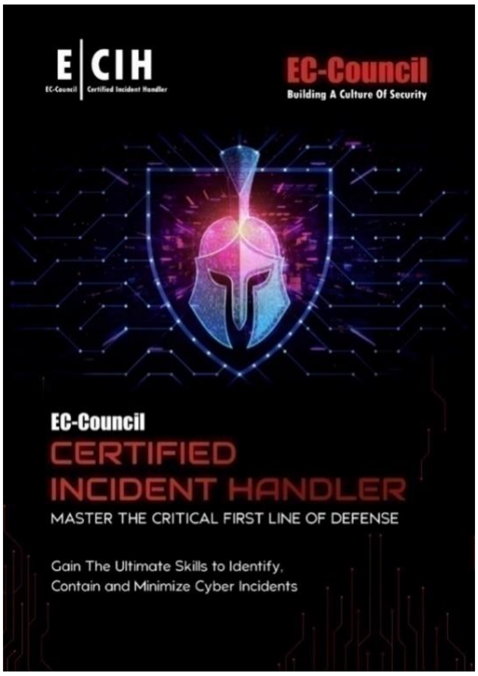
What motivates you to be a student volunteer?
Personally, seeing students my age and younger grow and learn from this field has really motivated me to be a student volunteer. Events like YCEP is especially heartwarming and important to me as we are training the youths by giving them a starting point for not just their interests in cybersecurity but also a platform to develop their talents and knowledge in this field.

How would you want to encourage your peers to be interested in cybersecurity?
Well, depending on the peers and individual mindsets, there are different ways in which I would encourage my peers to be interested in Cyber Security. For example, some people are in it for the money and well, there is a big range for growth financially in this field. Others might be interested in red teaming, in that case I would show them some CTFs and try to get them to maybe try one or two easy boxes, the first spark would be when they solve their first box and feel that sense of accomplishment. All in all, it would vary from person to person, but I think that showing them the results of cybersecurity would peak their interests in the field.

back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International


E|CIH
EC-Council | Certified Incident Handler
EC-Council
Building A Culture Of Security
EC-Council
CERTIFIED
INCIDENT HANDLER
MASTER THE CRITICAL FIRST LINE OF DEFENSE
Gain The Ultimate Skills to Identify,
Contain and Minimize Cyber Incidents

The question is not if, but when a cyber incident will occur?

EC-Council's Certified Incident Handler (ECIH) program equips students with the knowledge, skills, and abilities to effectively prepare for, deal with, and eradicate threats and threat actors in an incident.

The newly launched Version 3 of this program provides the entire **process of Incident Handling and Response** and hands-on labs that teach the **tactical procedures and techniques** required to effectively **Plan**, **Record**, **Triage**, **Notify** and **Contain**.

ECIH also covers **post incident activities** such as **Containment, Eradication**, **Evidence Gathering** and **Forensic Analysis**, leading to prosecution or countermeasures to ensure the incident is not repeated.

With over **95 labs**, **800 tools** covered, and exposure to Incident Handling activities on four different operating systems, ECIH provides a well-rounded, but tactical approach to planning for and dealing with cyber incidents.

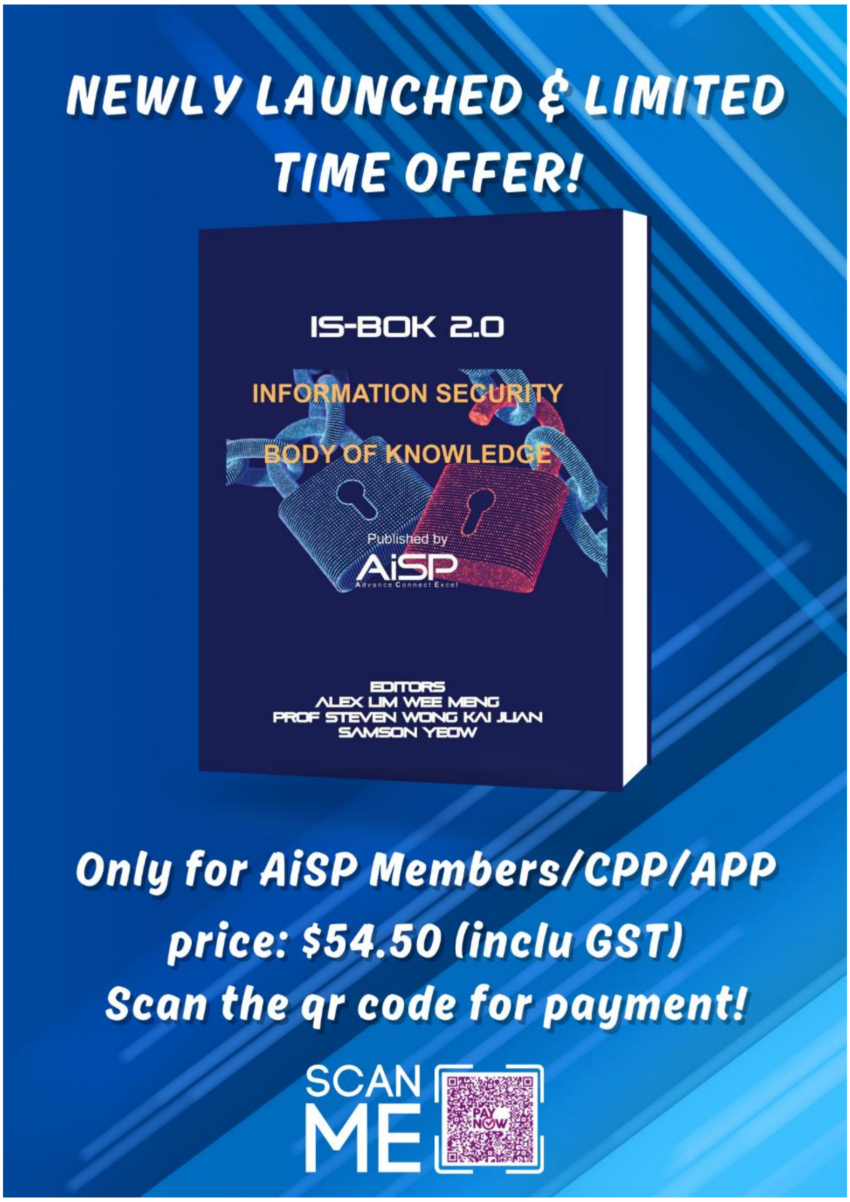
Special discount available for AiSP members, email aisp@wissen-intl.com for details!

back to top

Qualified Information Security Professional (QISP®)

Body of Knowledge Book Promotion!

For a limited time, get our newly launched Information Security Body of Knowledge (BOK) Physical Book (U.P $80 before GST) at the limited promotional price of **$54.50 (inclusive of GST). While stocks last!**

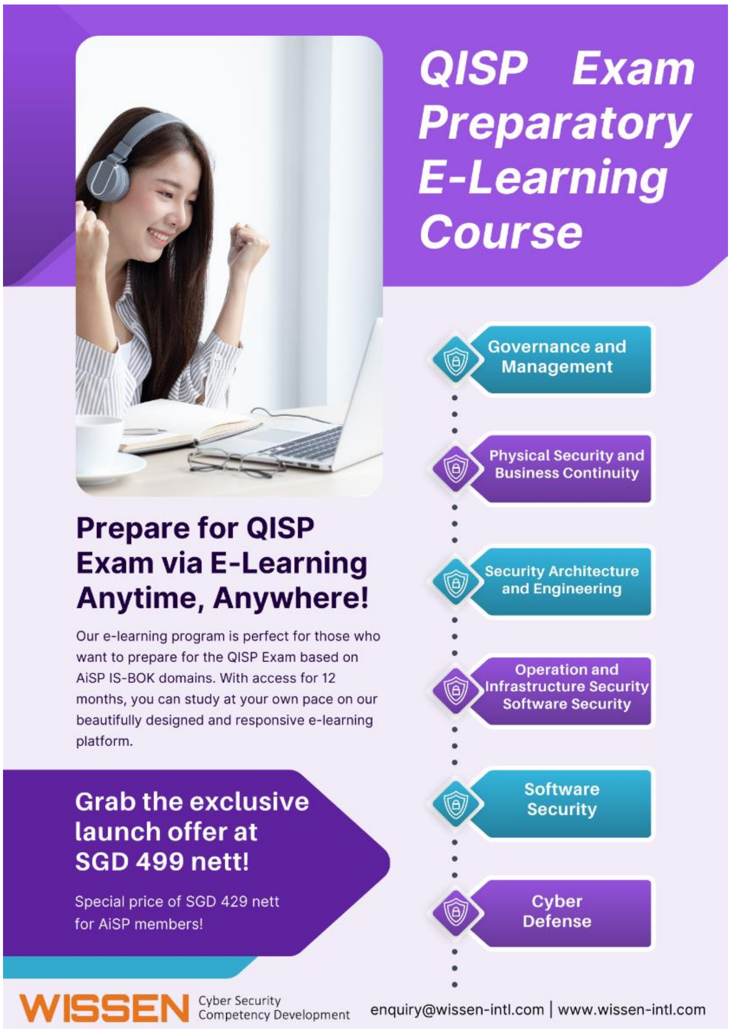

NEWLY LAUNCHED & LIMITED TIME OFFER!
IS-BOK 2.0
INFORMATION SECURITY
BODY OF KNOWLEDGE
Published by
AiSP
Advance Connect Excel
EDITORS
ALEX LIM WEE MENG
PROF STEVEN WONG KAI JUAN
SAMSON YEOW
Only for AiSP Members/CPP/APP
price: $54.50 (inclu GST)
Scan the qr code for payment!
SCAN ME
PAY NOW

Please scan the QR Code in the poster to make the payment of **$54.50 (inclusive of GST)** and email secretariat@aisp.sg with your screenshot payment and we will follow up with the collection details for the BOK book. Limited stocks available.

back to top

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP) COURSE

Online



QISP Exam Preparatory E-Learning Course

Governance and Management

Physical Security and Business Continuity

Security Architecture and Engineering

Operation and Infrastructure Security Software Security

Software Security

Cyber Defense

Prepare for QISP Exam via E-Learning Anytime, Anywhere!

Our e-learning program is perfect for those who want to prepare for the QISP Exam based on AiSP IS-BOK domains. With access for 12 months, you can study at your own pace on our beautifully designed and responsive e-learning platform.

Grab the exclusive launch offer at SGD 499 nett!

Special price of SGD 429 nett for AiSP members!

WISSEN Cyber Security Competency Development

enquiry@wissen-intl.com | www.wissen-intl.com

The QISP examination enables the professionals in Singapore to attest their knowledge in AiSP's Information Security Body of Knowledge domains. Candidates must achieve a minimum of 50-64% passing rate to attain the Qualified Information Security Associate (QISA) credential and 65% and above to achieve the Qualified Information Security Professional (QISP) credential.

Our highly responsive e-learning platform will allow you to learn anytime, anywhere with modular courses, interactive learning and quizzes. Complete the course in a month or up to 12 months! Enjoy lean-forward learning moments with our QISP/QISA preparatory e-learning course. Receive a certificate of completion upon completion of the e-learning course. Fees do not include QISP examination voucher. Register your interest here!

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 2024 to 31 Dec 2024. 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

Join our Corporate Partner Programme
for exclusive benefits and partnership with AiSP!

Contact AiSP Secretariat for the benefits and corporate pricing at secretariat@aisp.sg

For any enquiries, please contact secretariat@aisp.sg

back to top

AVIP Membership

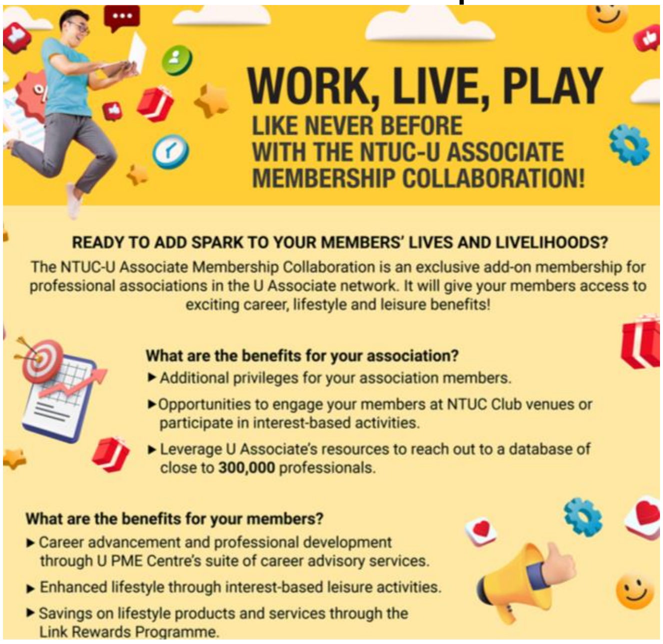
AiSP Validated Information Security Professionals (**AVIP**) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development, and career progression for our professionals.

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!

NTUC U Associate Membership



WORK, LIVE, PLAY
LIKE NEVER BEFORE
WITH THE NTUC-U ASSOCIATE
MEMBERSHIP COLLABORATION!

READY TO ADD SPARK TO YOUR MEMBERS' LIVES AND LIVELIHOODS?

The NTUC-U Associate Membership Collaboration is an exclusive add-on membership for professional associations in the U Associate network. It will give your members access to exciting career, lifestyle and leisure benefits!

What are the benefits for your association?

- Additional privileges for your association members.
- Opportunities to engage your members at NTUC Club venues or participate in interest-based activities.
- Leverage U Associate's resources to reach out to a database of close to **300,000** professionals.

What are the benefits for your members?

- Career advancement and professional development through U PME Centre's suite of career advisory services.
- Enhanced lifestyle through interest-based leisure activities.
- Savings on lifestyle products and services through the Link Rewards Programme.

Some benefits include

Career Advisory services - https://upme.ntuc.org.sg/upme/Pages/CareerCoaching.aspx

Benefits and privileges from RX Community

Member Programme

https://www.readyforexperience.sg/

Please fill in the form below and make payment if you would like to sign up for the membership.

https://forms.office.com/r/qtjMCK376N

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

back to top

AiSP Corporate Partners

Acronis	athena dynamics	AZ ASIA-PACIFIC
BD	BeyondTrust	BLACKPANDA
bugcrowd	CISCO	CLIXER
C8N+FINITY	CROWDSTRIKE	CSA SINGAPORE
CSIT Centre for Strategic Infocomm Technologies	CYBERSAFE YOUR SECURITY, OUR PRIORITY	CYFIRMA DECODING THREATS
CzechTrade SINGAPORE	DBS	DETACK
DSTA Defence Science & Technology Agency	DTASIA Security with Confidence	Eclypsium
ENSIGN INFOSECURITY	Fidelis Services Redefined	FORTINET
Genesis NETWORKS	GETVISIBILITY own your data	GOVTECH SINGAPORE
Grab	HORANGI CYBER SECURITY	HUAWEI

back to top

image engine

INTfinity

IT SEC ASIA

KnowBe4
Human error. Conquered.

MAGNET FORENSICS

mimecast

MySQL

M.TECH
Your Preferred i-Security Partner

ncs

NETWITNESS
An RSA Business

ONESECURE

opentext

OPSWAT.

PARASOFT

RAJAH & TANN CYBERSECURITY

Responsible Cyber

RSM

SailPoint

SCANTIST

Schneider Electric

Security Scorecard

SGS

Singtel

softScheck
We Build Trust

ST Engineering

Telstra

TEMASEK

tenable

TREND MICRO

VECTRA

Veracity Trust Network

VOTIRO

WISSEN
Cyber Security Competency Development

back to top

wizlynx group

xcellink.pte.ltd. completing your technology chain

YesWeHack

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

AiSP Academic Partners

ITE Institute of Technical Education

NYP NANYANG THE INNOVATIVE POLYTECHNIC

NGEE ANN POLYTECHNIC

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

NUS National University of Singapore

REPUBLIC POLYTECHNIC DISCOVER. TRANSFORM. ACHIEVE

SIT SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SMU SINGAPORE MANAGEMENT UNIVERSITY

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek POLYTECHNIC

back to top

Our Story…

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

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

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

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

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

AiSP Secretariat Team

Vincent Toh
Associate Director

Elle Ng
Senior Executive

Karen Ong
Executive

AiSP
Advance Connect Excel

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