

News & Update

- Knowledge Series
- CAAP
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Special Interest Groups
- The Cybersecurity Awards
- IOT Innovation Day
- Cyberattack Summit
- CREST
- Upcoming Events

Contributed Contents

- Data & Privacy SIG: Extrahop Report
- Forrester names Elastic a Strong Performer in the Endpoint Detection and Response Wave
- How Phishing Assessment Really Simulates Hacking
- Globally, Ransomware Attacks Growing Fastest in APAC
- Skybox research reveals a perilous threat landscape
- Securing critical infrastructure: 3 actions to take ASAP
- The Cybersecurity Awards 2021 Winner – Responsible Cyber

Professional Development

Membership

NEWS & UPDATE

New Partners

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



Continued Collaboration

AiSP would like to thank BCG, Checkmarx, Extrahop, Fortinet and our academic partner, Temasek Polytechnic for their continued support in developing the cybersecurity landscape:



News and Updates

AiSP has signed an MOU with Singapore Institute of Technology (SIT) on 11 May during the IoT innovation day at Suntec Convention Centre. We look forward to further the collaborations with SIT in the ecosystem. Thank you Senior Minister of State Dr Janil Puthucheary for witnessing the signing of the MOU and the event.



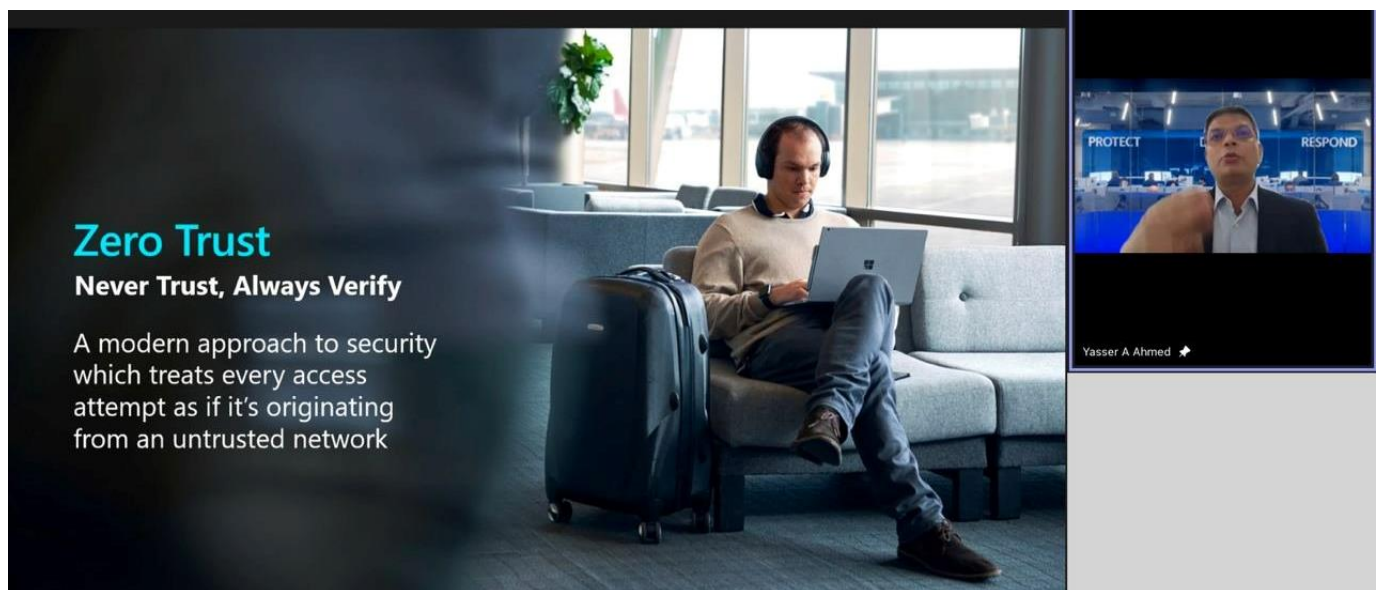
AiSP has signed an MOU together with ISACA Singapore Chapter on 25 May at NTUC One Marina Boulevard. We would like to thank Minister of State Tan Kiat How for gracing the event and NTUC Singapore U Associate for hosting us.



Knowledge Series Events

Identity & Access Management on 24 May 22

As part of Digital for Life movement, AiSP organized a series of events in hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. In collaboration with Microsoft on 24 May, our participants had the pleasure to hear from Mr Yasser Ahmed to speak on Identity & Access Management. It was an insightful time for the attendees as they learned about Zero Trust management and the 5 steps in securing this critical aspect of Identity security.



Incident Response Management on 6 Jul 22



AiSP Knowledge Series – Incident Response Management

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

The Path to Zero Trust: From Ambition to Reality

Speaker: Kevin Pang, Solutions Engineer, BeyondTrust

Remote working is now commonplace, while hybrid and multicloud footprints continue to rapidly expand. In this increasingly perimeterless world, organizations must embrace zero trust security principles, such as least privilege, continuous authentication and monitoring, segmentation, and microsegmentation to stay secure, while moving digital transformation forward.

Join BeyondTrust to understand:

- What Is Zero Trust?
- Zero Trust vs. Zero Trust Architecture – Are They Different?
- The Path to Zero Trust
- How Privileged Access Management (PAM) Enables Zero Trust

Beyond Incident Response - The Rise of Ransomware

Speaker: Victor Tan, Business Development Manager, Blackpanda

Cyber breaches happen quick and can cause serious damage. Being prepared in the event of a cyber breach allows organizations to successfully manage its impacts and reduce operational, financial and reputational damages by activating an efficient incident response plan, helping your business through a cyber catastrophe. In this webinar, Victor delves deep into the impacts of the various types of cyber incidents due to system vulnerabilities and human errors. Join us to learn more about the correct approach to managing a ransomware based on past cases Blackpanda has successfully handled.

Date: 6th July 2022, Wed

Time: 3PM – 4.30PM

Venue: Zoom

Registration:

https://us06web.zoom.us/webinar/register/8816536323919/WN_MShJhWjQQ4u0Gg8SxqDR6A

About our Knowledge Series

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its [Information Security Body of Knowledge 2.0](#) topics. Our scheduled topics for webinars in 2022 are as follows (*may be subjected to changes*),

1. Incident Response Management, 6 July 22
2. Cyber Threat Intelligence, 20 July 22

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

Please refer to our scheduled 2022 webinars in our [event calendar](#).

Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP x Microsoft CAAP Roundtable on 5 May

In collaboration with Microsoft, AiSP organised a roundtable on 5 May to share on the current state of cybercrime and how to be more cyber resilient. We would like to thank Mr Tony Low, Ms Veronica Tan and Mr Richard Koh for sharing insights with our attendees. We would also like to thank NTUC Singapore U Associate for hosting us.



Anti-Ransomware Day 2022 on 12 May

As part of World Anti-Ransomware Day, AiSP has collaborated with Fortinet on 12 May to share more on Cyber Essentials & Cyber Trust, ransomware attack trends and cybersecurity tools to stay cyber safe. We would like to thank all the speakers and participants who joined us physically for the event.



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

In collaboration with Palo Alto Networks, AiSP conducted a webinar on Zero Trust Strategy for SMEs on 17 May. Our attendees had the pleasure to hear from Mr Ian Lim from Palo Alto on Zero Trust strategy and Ms Veronica Tan from Cyber Security Agency of Singapore (CSA) on Cyber Trust and Cyber Essentials. AiSP EXCO Member, Mr Freddy Tan also shared with the attendees on what CAAP Programme and its focus on security knowledge and awareness.




Ian Lim
Field Chief Security Officer,
Asia Pacific & Japan
Palo Alto Networks

- Over 20 years of dedicated cybersecurity experience.
- 15 years in a CISO role for Fortune 500 companies.
- Experience across financial, real estate, logistics and healthcare verticals and has done on-the-ground work in the US, EMEA and APAC.
- Co-authored three books between 2003 and 2013.
- Executive Committee at the Cybersecurity Policy and Research Institute in the University of California Irvine.
- Grew up in a F&B and Retail family business

Strategic Thrusts, that anchor our vision

Vision	A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem.		
Mission	Pillar for the Information Security Profession and Professionals in Singapore		
Strategic Goals	Achieved Sustainability	Increased Collaboration	Increased Recognition
Strategic Thrusts	Advance	Connect	Excel
	Innovation Knowledge Series Specialization Certifications Special Interest Groups	Regional Ecosystem Local Ecosystem	Corporate Partners Academic Partners Letters in Cyber Cybersecurity Awareness & Advisory Program AISP Validated Security Professionals (AVIP) Cyber Security Awards Student Volunteer Recognition Program (SVRPS)
	MEMBERS		

AiSP Cybersecurity Awareness E-Learning

	
<h3>AiSP Cybersecurity Awareness E-Learning</h3>	
<p>On 7 January 2022, the Association of Information Security Professionals (AiSP) launched the Cybersecurity Awareness E-Learning. It was launched by Ms Gwenda Fong, Assistant Chief Executive (Policy & Corporate Development) of Cyber Security Agency of Singapore.</p> <p>In this E-Learning, we will bring you through a set of materials that will prepare your Business and your employees to embark on an exciting journey in digital transformation and start your Business to be more secure.</p> <p>We will be covering:</p> <ol style="list-style-type: none"> 1. Providing businesses with an understanding of the current digital business landscape 2. Deep dive into understanding the Digital better Transformation Journey 3. Risk and threats for the Business to understand some of the most crucial aspects and assessments. 4. How you can start to explore and secure your Business by handling data securely and setting up your initial cybersecurity framework 5. Providing an understanding of your Business Obligations and the various regulations that will impact your process and impact the Business. Sharing of different policies and guidelines such as PDPA, Cybersecurity Act, Computer Misuse Act 6. Your responsibility to ensure in the event of an incident, how the enterprise should handle 	 <p>AiSP Cybersecurity Awareness E-Learning</p> 
<p>Why Should You Take This E-Learning & How Will It Help You?</p> <p>Through this E-learning, we prepare your business and your employees to kickstart your journey in digital transformation and be more cyber safe. With the various contents provided in the E-Learning</p>	

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

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

Why Is this E-Learning Special?

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

Subscription Plan

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

^{*}Minimum 1 year subscription

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

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

Payment Details

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

SME Cybersafe provides



Enhanced Security
Awareness & Training



Cohesive Security
Knowledge Resources



Security Solutions &
Services Support

Click [here](#) to find out more about the E-Learning.

Student Volunteer Recognition Programme (SVRP)

Learning Journey to Huawei office on 25 May

As part of the Digital for Life Festival, AiSP brought a group of students from ITE West on a learning journey to our Corporate Partner Huawei Singapore office. They had the opportunity to explore the office and view the upcoming and ongoing digital gadgets developed by Huawei itself. It was an insightful and memorable day for the students.



AiSP Youth Symposium

As part of Singapore Youth Day 2022, AiSP will be organising the inaugural Youth Symposium where we will invite about 100 to 150 Youths (Subjected to COVID restrictions) from our Student Chapters to come together physically for a day of celebration and enriching activities ranging from Dialogue Session, Recruitment Talk, Internship Opportunities by some organisations and free Courses to help the students improve in their digital skills and booths from our partners to promote and share more on their plans of involving more Youths in the future.

Event Date: 2 July 2022

Event time: 12.30 PM – 4PM


Event Venue: SCAPE*

[back to top](#)


AiSP Youth Symposium

2 JUL 2022 | 12.30PM - 4PM | SCAPE*





Save the Date







Organised by:




Supported by:


Sponsors:

Our student volunteer drive is ongoing till Dec 2022 for those who are interested to volunteer but not sure where to start. Please click [here](#) to apply today. Nomination period is from 1 Aug 2021 to 31 Jul 2022.




Nomination Period:
1 Aug 2021 to 31 Jul 2022




Nomination Period:
1 Aug 2021 to 31 Jul 2022

CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

Tier	Requirements	
Bronze	Completion of one of three pillars or complete three of three pillars with minimum 50% attained hrs. Skills: 30 Hours or more Events: 60 Hours or more Leadership: 30 Hours or more	 Scan the QR Code for the Nomination Form
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	

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


 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

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

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

AiSP Cyber Wellness Programme

<p>Organised by:</p> 	<p>Supported by:</p> 	<p>In Support of:</p> 
<p>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."</p>		
<p>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.</p>		
 <p>Scan here for some tips on how to stay safe online and protect yourself from scams</p>	 <p>Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship & Ethics.</p>	
 <p>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.</p>	 <p>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.</p>	
 <p>Want to know more about Information Security? Scan here for some career advice on Information Security.</p>	 <p>To find out more about the Digital for Life movement and how you can contribute, scan here.</p>	
<p>Contact AiSP Secretariat at secretariat@aisp.sg to find out more on how you can be involved or if you have any queries.</p>		

Click [here](#) to find out more!

Digital for Life Events

Digital for Life Festival from 21-29 May

In support of Digital for Life Festival, AiSP was invited to set up a booth at Suntec Convention Centre on 21-22 May and Heartbeat@Bedok on 28-29 May to educate the public on cyber wellness. They also had the opportunity to participate in our cyber wellness quiz and a mini game to learn more about the importance of Cybersecurity and how to stay safe online. Prizes were redeemed during the events as a token of participation. We were thrilled to see so many people of all ages who were interested to learn more about cyber wellness and how they can stay safe online. DFL Patron, President Halimah, Minister Josephine Teo, Minister of State Tan Kiat How, Parl Sec Ms Rahayu and Members of Parliament of East Coast GRC visited our booths during the festival, and it was a rare opportunity for our student volunteers to introduce AiSP booth to them. We would like to thank Acronis, Fortinet, Huawei and Just Hacking for joining us in the Digital for Life Festival Activities.





Pathlight Students trip to Acronis office on 26 May

As part of the DFL Festival, AiSP brought students from Pathlight Secondary School on a learning journey to our Corporate Partner Acronis office for a morning of industry experience and scam awareness. We hope the students have gain more insights through the visit and interaction with the staff working on site.



Aiya I Won't kena SCAM Lah!

On 27 May, AiSP organised a webinar titled "Aiya I Won't Kena SCAM Lah" to share with the attendees how to protect yourselves against scams and malware. AiSP would like to thank AiSP EXCO Member, Ms Faith Chng for giving the opening address and Dennis Chan and Norman Kuo from our CPP Partner, [Huawei Singapore](#) for sharing the knowledge with the attendees.



Ladies in Cybersecurity



Ladies Talk Cyber Series

For the Thirteenth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Xenia Kim who in the R&D department of Acronis. Most of her day involves working on the different microservices that make up Acronis' products.

How to be successful in cybersecurity field

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

Introducing women with a deep interest in cybersecurity

Xenia is in the R&D department of Acronis. Most of her day involves working on the different microservices that make up Acronis' products. She does a mix of designing of the service, including designing how the different services can communicate with people, and the actual implementation of the service itself. She also occasionally volunteers to help at events to promote cybersecurity and Acronis to the public.

Please click [here](#) to view the full details of the interview.



LIC Talk for ITE West Students on 13 May

AiSP Ladies in Cyber Team were at ITE West on 17 May and met with more than 40 female year one students in a closed-door cybersecurity career sharing. AiSP would like to thank AiSP EXCO Member, Alina Tan & Sherin Lee for sharing their experience and providing advice to the students and thank ITE West for having us.



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



The Cybersecurity Awards



Less than a Month to closing of TCA 2022 Call for Nominations!

ONE MONTH LEFT!

PROFESSIONALS

- Leader
- Professional

ENTERPRISES

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

STUDENTS

ONE MONTH LEFT!

NOMINATION OPEN UNTIL 17 JUNE 2022

www.thecybersecurityawards.sg

ONE MONTH LEFT!

REGIONAL AWARDS CATEGORY

NOMINATE A NONPROFIT / ASSOCIATION NOW!

NOMINATION OPEN UNTIL 17 JUNE 2022

www.thecybersecurityawards.sg

ORGANISED BY

AISP
Advance Connect Excel

Visit www.thecybersecurityawards.sg for more information.

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

Professionals

1. Hall of Fame
2. Leader
3. Professional

Students

4. Students

Enterprises

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

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

THE CYBERSECURITY Awards 2022

Organised by



Supported by



Supporting Associations



Community Partner



Supporting Organisation



Platinum Sponsors



Gold Sponsors



Silver Sponsors



IoT Innovation Day

On 11 May, AiSP organised the first inaugural IoT Innovation Day at Suntec Convention Centre. We had the pleasure to hear from CSA and GovTech keynote speakers, Mr Lim Soon Chia (CSA) and Mr Goh Jing Loon (GovTech) sharing on building towards a secure and trusted IoT ecosystem as well as identifying the vulnerabilities in the ecosystem.

AiSP would like to thank Senior Minister of State for MCI & MOH and Minister In-Charge for GovTech, Dr Janil Puthucheary for gracing the event. We would also like to thank our sponsors Cisco, Elastic, ExtraHop, SecureCraft and Vectra AI for contributing to the success of the event.

We hope all the participants enjoyed the insightful event as much as we do.



[back to top](#)

Cyberattack Summit

AiSP was down at Swissotel Stamford Ballroom on 25 May as one of the supporting organizations for Cyberattack Summit organized by HTCIA (Singapore) Chapter. AiSP Member, Mr Dennis Chan from Huawei (AiSP Corporate Partner) also shared his insights with the participants on Building a Secure & Trustworthy Intelligent World. AiSP would like to thank HTCIA (Singapore) Chapter for the opportunity to spread awareness.



CREST

An update from CREST

CREST has been working with multiple internal and external stakeholders to redefine our vision and mission. When CREST was initially formed back in 2005, it was built to serve the needs of the technical assurance industry in the UK. As we reflect on 2022, the organisation has come a long way. We are now a truly international organisation with almost 300 members; we deliver examinations in all corners of the globe and Asia, and across the multiple cybersecurity disciplines, including penetration testing, threat intelligence, Intelligence-led testing, vulnerability assessments, SOC, and incident response. As a result, it is time for us to recalibrate our focus and publish updated statements on where we are heading on what we strive to achieve.

An evolved identity

CREST is rebranding. We are listening, adapting, and responding to our member's needs. We have a newly appointed leadership team — evolving and improving our organisation process and examination strategy. The rebrand is an evolution, not a revolution; however, it is a clear signal that we are changing, with a renewed focus on our members and our exam takers.

A new website aimed at connecting buyers with CREST member companies.

We have launched a new website that supports governments, regulators, and buyers to engage with CREST accredited companies. This allows our members to create content that showcases their capabilities. The site works harder to guide buyers to capable service providers. We provide sales

leads, data, and analytics to members about what buyers are searching for to provide our members with commercial opportunities.

Exam updates in 2022

A new exam delivery model is coming that will leverage remote proctoring to provide exam takers with the ability to take exams anytime and anywhere. This will allow us to deliver exams across the globe whilst enabling exam takers to take examinations from the convenience of their own homes. The movement to this model will take time. However, it will commence in 2022, with both registered and certified exams available during the year.

Improved pathways into CREST

CREST is delighted to announce strategic relationships with Hack The Box and Immersive Labs. We are working together to develop training pathways through Hack The Box and Immersive labs that will enable exam takers to better prepare for CREST examinations. As part of the relationships, CREST accredited companies will be given access to dedicated environments that will provide a series of CREST aligned learning and development instances.

In addition, by being a member of CREST, Hack The Box and Immersive Labs will provide reduced-cost access to some of their wider lab environments. This is a massive win for both exam takers wanting to build skills and member companies looking to develop learning and development pathways.

Evolving accreditation process

We have launched an updated accreditation process requiring all individuals involved in scoping, delivering, and sign-off of a CREST accredited service to demonstrate their current skills and competencies. As we move through 2022, we will run a series of industry consultations to shift to a tiered accreditation model that we hope to launch in 2023.

A consistent international governance structure

At the end of 2021, CREST ran a series of elections across all our regions. We now have elected council members operating in Asia, Australasia, the US, Europe, and the UK. This new structure facilitates local decision-making geared to supporting CREST member companies domestically and internationally. Through these new councils, we are already forming new strategic alliances with multiple governments and regulatory stakeholders, all with the intention of driving opportunities for CREST member companies.

The cybersecurity industry is evolving rapidly, and the needs and expectations of members and external stakeholders are continually increasing. We aim to be the go-to global organisation for cybersecurity accreditation and certification through our continuous focus on improvement.

With a renewed focus on the exam candidate experience and significantly enhanced member benefits, we aim to enhance the CREST member company experience continually. CREST is committed to all our exam takers and our CREST member companies. We are laser-focused on supporting our members to build and enhance their skills and competencies across the industry in Asia. We are actively pursuing pathways that drive inclusion and maximise existing returns on investment.

We are here to enhance the cybersecurity ecosystem. Please feel free to get in touch with our Regional Advocate and Chair for CREST Asia, Emil Tan - emil.tan@crest-approved.org

Visit our website for further news and updates: www.crest-approved.org

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
1 June	Learning Journey to Singtel with RP Students	AiSP & Partner
01 – 03 Jun	InnovFest 2022	Partner
01 – 03 Jun	Asia Tech X Singapore 2022	Partner
7 June	MOU Signing with MBOT	AiSP & Partner
17 – 19 Jun	STANDCON 2022	Partner
27 Jun	School Talk at Broadrick Secondary School	AiSP & Partner
27 – 30 Jun	Israel Cyber Week	AiSP & Partner
29 Jun	AiSP x Elastic Webinar	AiSP & Partner
29 Jun	AiSP x JTC PDD Networking Session	AiSP & Partner
2 Jul	AiSP Youth Symposium	AiSP
4 Jul	Learning Journey to Singtel with ITE West Students	AiSP & Partner
6 Jul	Knowledge Series – Incident Response Management	AiSP & Partner
7 Jul	SCCCI CAAP Workshop	AiSP & Partner
12 Jul	Learning Journey to Acronis with ITE West Students	AiSP & Partner
15 Jul	AiSP x WISAP Spill the Tea Webinar	AiSP & Partner
20 Jul	Knowledge Series – CTI	AiSP & Partner
27 Jul	Cyber Leaders Series	AiSP & Partner

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

CONTRIBUTED CONTENTS

Article from IoT SIG

ExtraHop Report: 83% of Asia Pacific Organisations Suffered a Ransomware Incident in the Past Five Years; 68% Tried to Keep it Quiet

ExtraHop, the leader in cloud-native network detection and response, shared findings from a new survey that shows 83% of organisations in Asia Pacific were breached by ransomware at least once in the past five years, but only 32% publicly disclosed that an

[back to top](#)

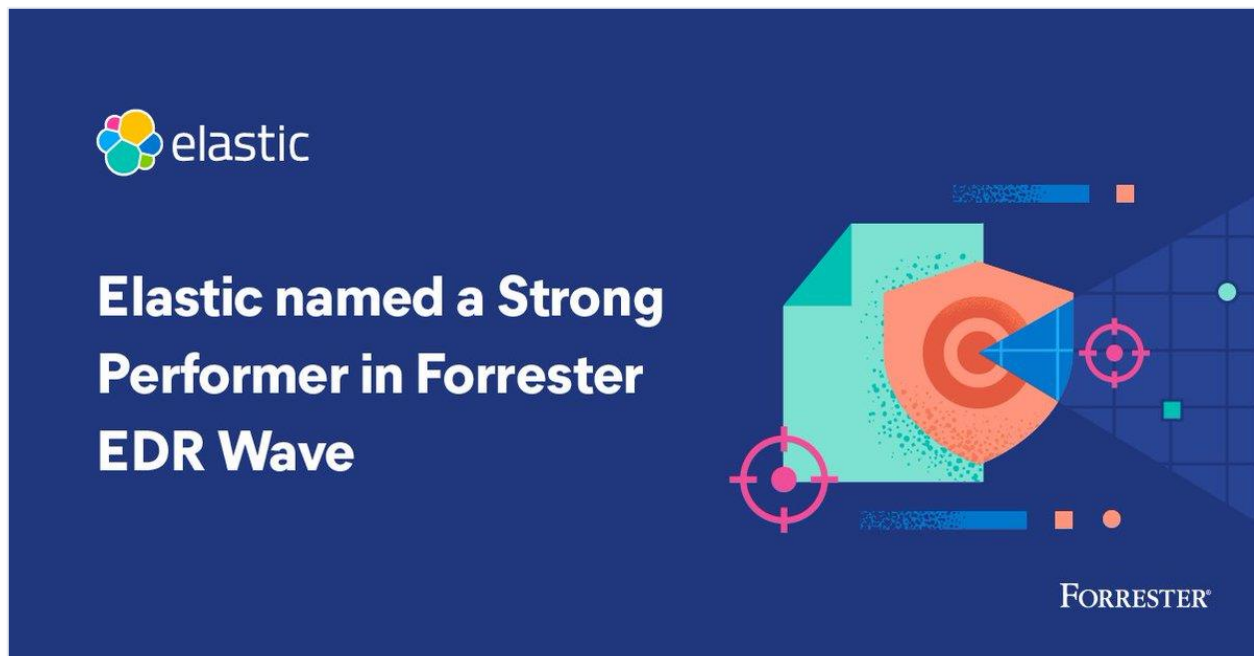
incident occurred. The [ExtraHop 2022 Cyber Confidence Index—Asia Pacific](#), conducted by StollzNow Research and covering Australia, Singapore, and Japan, sheds light on the efficacy of current security practices and the reality of the ransomware attack landscape.

URL for this report can be found here -

<https://www.extrahop.com/resources/papers/the-ciso-realists-of-asia-pacific-form/>

Article from our CPP Partner, Elastic

Forrester names Elastic a Strong Performer in the Endpoint Detection and Response Wave



Elastic was named a Strong Performer in [The Forrester Wave™: Endpoint Detection and Response Providers, Q2 2022](#).

Elastic received the highest scores possible in the product vision, market approach, innovation roadmap, and commercial model criteria within the Strategy category, as well as the highest scores possible in the product security, user experience, and endpoint telemetry criteria within the Current Offering category.

Security at scale

Forrester stated in the [EDR Wave](#) that “Threat hunters can search data and visualize it with graphs and charts, and can also schedule queries.” The analyst firm also mentioned that “Elastic is best suited for security teams with a depth of knowledge that want a flexible offering with features of SIEM and EDR.” Elastic purposefully combined SIEM and EDR so that customers would be able to see, remediate, and address security concerns across any infrastructure environment. This combination helps customers drastically reduce detection and remediation time.

Community collaboration

With regard to Elastic’s online community, Forrester noted: “It has nurtured an online community so that security teams can crowdsource expertise, which customer references find valuable.” Elastic has spent years nurturing its [strong community](#) where users find help, collaborate, and contribute.

The limitless data ingest, analysis, and visualization capabilities made possible by Elastic’s scalable platform means users can relay insights otherwise inaccessible through traditionally data-constrained solutions. This unfettered insight into users’ data provides a positive feedback loop to the rest of the community, as well as the team behind Elastic Security, further improving the product through real-world application.

Security evolution

Forrester further commented on our roadmap and how we decide what to build next. “Its roadmap looks to expand third-party ingestion capabilities, response actions, and workflows, and it prioritizes new ideas by dedicating a week of R&D every two months to focused innovation.” Last fall, Elastic was named a Contender in The [Forrester New Wave\(TM\): Extended Detection and Response \(XDR\) Providers, Q4 2021](#), which, in our opinion, demonstrates our commitment to innovating for our customers’ benefit.

Building on our innovative spirit, we’ve published dozens of [research articles](#) that showcase the various security research we’ve completed in recent weeks to help increase security posture across the industry.

“Elastic has spent a lot of effort bringing our SIEM and EDR capabilities together to deliver limitless security and provide customers with a singular agent to find, protect, and block endpoint threats,” said Mike Nichols, Senior Director of Product Management

for Elastic Security. "Having Forrester recognize our progress in this space means a great deal and we are grateful for the recognition."

To learn more about Forrester vision on EDR and the Elastic placement, [download the Forrester EDR Wave](#).

If you have any questions about Elastic, please get in touch [here](#).

Article from our CPP Partner, Numen Cyber

How Phishing Assessment Really Simulates Hacking

Introduction

It is said that humans are the weakest link in cybersecurity. Indeed, Employees are often a major access point for cyber attackers. Companies need to make sure that their employees are well trained and educated about cyber-attacks.

Cybercriminals today use savvy phishing tactics to trick people into performing actions or divulging confidential information in a real-world case.

The objective of such attacks is to exploit the weakness of human psychology, using universal vulnerable human qualities such as fear, greed, curiosity, compassion, deference to authority, and so on.

According to Verizon's 2019 data, 94% of malware is delivered by email and daily 150 million phishing emails are sent.

While the plots of phishing attacks are constantly evolving but the fundamentals still boils down to the following techniques:

- Social Engineering
- Spear Phishing
- Pretexting
- Baiting and Quid Pro Quo

Phishing is extremely dangerous because it takes only one careless act to open the door for a cybercrime incident and resulting in a significant impact on data breach or infection of a device, server, or network that can severely harm the Organization's financial and reputation.

What is a Phishing Simulation

Phishing Simulation is a phishing campaign run against your team to test if they can identify the phishing attempt. Also, it is used to check the effectiveness of phishing training. The simulated phishing emails may look like coming from the manager, HR, etc. IT team sends identical emails but instead of triggering a malware attack, the links in these emails track different parameters like who linked the link, time taken to click the link, etc, and also inform employees that they fell victim to a simulated phishing attack and show them how they could have identified and avoided it.

It is a good idea to identify employees who are falling victim to these phishing emails before an actual phishing mail lands in their inbox.

Why it is important

Phishing simulation is something that every organization today must perform with their employees. A few reasons why phishing simulation is important :

1. It is an effective way to understand how likely employees will click on the real phishing emails by simulating a phishing attack. Employees who fall for the phishing attack simulation can be trained to identify these attacks which will help them avoid a real phishing attack.
2. It is also a good way to check how the security team deals with phishing attack reporting. With phishing simulation, the company can understand what the security team does once an employee reports a phishing attack to the security team.
3. It is a practical way to show the importance of cyber security and cyber hygiene to the non-IT staff of the company.

How Phishing Simulation works

Phishing simulation can be done both manually and by using various tools. Here are some of the ways it can be done manually :

1. **Water hole attack:** Here one can infect sites/forums frequently visited by the employees and then lure them to click on the link. Here first the website is compromised and malicious codes and files are added. As these sites are frequently visited by the employees they can fall victim to it.
2. **Inner group chat tools:** By sending links/files in company WhatsApp group / Teams and identifying how many employees fall victim to it. As today many employees work from home so they connect with their colleagues via instant chatting apps like WhatsApp, Skype, etc. These chatting tools can be used to target the employees and see how aware they are while using these applications.
3. **Reaching out on LinkedIn:** Reaching out to employees on LinkedIn with job offers and asking to click the link for the Job description. With some social engineering skills and knowing the employee and their requirements, this attack can be done with a high success rate.
4. **Disguising as a potential client:** By disguising as a potential client and reaching out to employees and asking them to perform tasks. This technique works well when targeting the sales team as they are constantly looking for new clients.
5. **Evil Twin phishing:** Most employees connect their laptops and smartphones via Wi-Fi. Evil Twin Phishing involves creating a Wi-Fi hotspot that looks like a real one and even setting the SSID as like the real network. When employees connect to it, their account names, passwords, etc can easily be accessed.
6. **Smishing:** Smishing or SMS Phishing is a form of phishing done via SMS. Here SMS can be sent to the target with a convincing template and link. As links sent via SMS are not filtered it is easy to perform this type of attack.
7. **Vishing:** Similar to smishing, vishing is voice phishing. In this attack, the attacker calls up the target (often with a spoofed number) and impersonates someone known to the target, and tries to get information like credit card details, Pin, OTPs, etc.

8. **Spear Phishing:** In most of the above-mentioned techniques, a generic message is sent to many people, and often it might work the best. In spear phishing, a targeted message is sent which is meant for one single individual. The message is customized keeping that particular individual in mind. For example, they may use email subject lines that would be topics of interest to the target.

Manual phishing simulation can be a tedious task as companies have 100s of employees and targeting every employee might not be easy and practical also with manual phishing simulation reporting and creating metrics can be an issue.

Most Phishing simulations are usually done with the help of various phishing simulation solutions that are available on the market. We have plug-and-play phishing solutions with 100s of realistic phishing templates which can be used to target multiple employees at a single click and see how well prepared employees are for a realistic phishing attack.

There are several components to a phishing campaign :

1. **Registering a fake look-alike domain:** A fake domain is registered that looks almost similar to the real domain. This is done to trick the employees into clicking the link/mail.

Some techniques used while choosing a fake domain are :

- **Bitsquatting:** Swapping one or two letters in a domain name with similar characters. example.com to exannple.com
 - **Repetition:** Duplicating a letter in a domain name. example.com to examplle.com
 - **Omission:** Omitting a letter in a domain name. example.com to exmple.com
2. **Phishing templates:** Cybercriminals use different phishing templates to make their phishing email look genuine and convincing. For example, the most popular phishing template currently is covid/covid vaccination-related email templates. The idea of phishing simulation is to introduce an email template and its pattern to employees before an actual cyber-criminal sends them one.

Each phishing template usually includes :

- **An email message:** A convincing email so that people open the mail and click on the links.
- **Landing page:** A fake webpage that will either ask the user to enter personal information or show a google or Microsoft login page.
- **Redirect to Warning message:** Once the user enters the details and clicks the sign-in, it redirects to a warning message page that informs them that they got phished.

Important metrics to collect

When a phishing simulation is done, it is important to collect some key metrics so that the organization can better understand the phishing simulation campaign and can make informed decisions.

Some of the important metrics that can be collected in phishing simulation are :

1. **The minimum time is taken to open the mail:** This will show how fast people fall for the phishing mail.

2. **Link-click rate:** This shows how many people clicked the link out of the number of people who opened the mail.
3. **Credential capture rate:** This shows the number of users who gave their credentials out of the number of people who opened the landing page.
4. **Report rate:** This shows how many people report the email to the security team out of the number of people who received the mail.

Conclusion

With companies moving to the cloud and employees working from home, phishing attacks are increasing daily. For cybercriminals, it is very easy to execute phishing attacks but for businesses, the effects can be catastrophic. Companies need to make sure that employees don't fall for these phishing attacks. With proper awareness training and phishing attack simulation, this can be achieved.

To conduct a Phishing Simulation for your organization or find out more about Phishing Assessment, please contact Numen Cyber Technology Pte Ltd at sales@numencyber.com. Alternatively, you may call us at +65 6355 5555 or visit our website at www.numencyber.com.

Article from our CPP Partner, Mandiant

Globally, Ransomware Attacks Growing Fastest in APAC Check out Mandiant M-Trends 2022 Report to find out more...

Steve Ledzian, VP, CTO – APJ
Mandiant

Mandiant is continuously working behind the scenes to respond to headline making cyber breaches around the world. Organizations often want Mandiant to share details of the breaches they respond to so they can learn, adapt, and improve from the lessons that come out of those incidents. However, many of the details of those breaches are sensitive, and Mandiant honors the confidentiality of its clients and respects the privacy around the situations that they are hired to respond to.

At the same time, Mandiant realizes the importance of community sharing, and so every year, Mandiant releases its M-Trends report. This report aggregates data across all the incident response work Mandiant does and isn't specific to any individual client. Cyber metrics, observations on trends, tactical recommendations, and details on emerging threat actors are all rolled up into a single report. M-Trends 2022 marks the 13th annual edition of the report and it's a "must read" for every cyber security professional.

By The Numbers

For Asia Pacific (APAC), M-Trends 2022 had quite a few interesting observations. Some of the metrics collected relative to APAC showed signs of progress while other metrics indicated that there was much work still to be done.

One interesting metric to consider is how organizations come to learn that they have been breached in a cyber attack. Did the organization discover it on their own or did they learn of it only when an external entity such as law enforcement notified them? It's generally better to discover a breach on your own than to be informed that you've been breached by an external entity. For the incidents that Mandiant responded to in APAC in 2021, 76% of the victims were notified by an external entity and did not discover the breach on their own. This is the highest percentage of any global region.

Another key metric to consider is how long it takes an organization to realize that they are the victim of a cyber intrusion. Here APJ saw very good news. In 2020, it took organizations in APAC 76 days to notice cyber intrusions, and in 2021 that number was reduced significantly to 21 days. Organizations in APAC are noticing intrusions more quickly than they have in the past, which is an encouraging sign, and an indication that investments in detection and response capabilities are paying off.

As predicted in the Mandiant Report "[14 Cyber Security Predictions for 2022 and Beyond](#)", APAC is seeing an increase in ransomware. Only 12.5% of Mandiant's investigations were related to ransomware in 2020, but in 2021 that percentage grew to 38%, a larger growth rate than seen anywhere else in the world.

A final interesting metric to highlight isn't specific to APAC but rather is a global metric. Often when Mandiant is called to respond to an incident, once inside and scoping the compromise, they find that actually there is not a single but multiple threat actor groups who have intruded into and are present in the victim network. In 2021, this occurred in 25% of the incidents that Mandiant responded to globally.

Notable Threat Actor Groups

Over the years, Mandiant encounters the same threat actor groups in many different victim environments. As we learn more about the groups, our understanding of their motivations and Tools Techniques & Procedures (TTPs) grow. When a critical mass of knowledge on a threat group is reached, Mandiant will "promote" the group to a named group and give it a APTXX (for espionage) or FINXX (for cyber crime) moniker.

2021 saw promotion of the groups [FIN12](#) and [FIN13](#). In addition to these two, M-Trends 2022 covers two other groups : [UNC2891](#) and [UNC1151](#). UNC2891 may be interesting to audience in APAC as this is a group that specifically targets organizations in APAC. The group has been active since at least 2019 and is motivated by financial gain. UNC2891 is fluent in attacking UNIX and Linux systems, and operates with a high level of operational

security. Some of the tooling of this group is believed to target the ATM switching networks of banks.

Ransomware

M-Trends 2022 has a lot to say about ransomware, from the latest trend of attacking virtualization infrastructure to observations about ransomware recovery practices. The report also shares the story of a client that engaged Mandiant to perform a ransomware related [Red Team Assessment](#). The client wanted to understand if their network isolated backup infrastructure was really out of the reach of even sophisticated attackers. This organization had many strong defensive practices in place such as network segmentation with jump hosts and Privileged Identity Management (PIM), but ultimately the Mandiant Red Team was able to compromise the critical backup infrastructure. That client now knows the techniques that Mandiant used to accomplish their mission, and has addressed them so that they will no longer work for real world attackers. Friendly cyber sparring through Red Teams builds experience by testing people, process, and technology systemically.

Case Study of an Incident Response

Lastly, there is a case study of an a Mandiant incident response which started with the detection of a coinminer in the victim environment. Many organizations might be tempted to treat this a low severity incident, but it's notable that the coinminer gained entry through an Internet facing vulnerability. M-Trends 2022 advises :

*“For an incident in which a published vulnerability is suspected to have been leveraged, investigation of the observed effect—such as this coinminer—is a necessary but **insufficient** condition of comprehensive incident response.”*

When the entire organization was scoped for threat activity, it became evident that this organization was one of the 25% that simultaneously had multiple ongoing intrusions beyond just the actors responsible for the coinminer. UNC3061 and APT41 were also active in the environment.

Conclusion

These are just some of the interesting findings in M-Trends 2022. The report covers many other topics including China's changing approach to cyber operations, and a section for practitioners on common misconfiguration that lead to compromise both on premise in and in the cloud. M-Trends 2022 is freely available at [Mandiant.com](https://www.mandiant.com).

For any enquiries, please contact Ms Christina Foo at christina.foo@mandiant.com

Article from our IoT Sponsor, Securecraft

Skybox research reveals a perilous threat landscape

Record-breaking vulnerabilities—especially in OT systems—and accelerating exploits require a new approach to vulnerability management.

Ran Abramson

Security Analyst Skybox Security

The latest [Skybox Vulnerability and Threat Trends Report](#) is now out, and it presents some eye-opening statistics and trends that I and my fellow security analysts at Skybox Research Lab have been tracking over the past year. For anyone interested in the on-the-ground realities confronting security professionals these days, the report makes for compelling reading; get the 2022-report here:

[Vulnerability and Threat Trends Report 2022](#)

Record breaking vulnerabilities, rising OT security risks, and increasing exploits demand a new approach to vulnerability management.

This year's findings chart a threat landscape that's expanding and diversifying at a blistering clip. We observed record growth in new vulnerabilities affecting a wide variety of products. In particular, vulnerabilities in operational technology (OT) skyrocketed, nearly doubling versus the previous year. As vulnerabilities emerged, threat actors moved ever more quickly to weaponize them. New exploits increasingly took aim at the latest vulnerabilities, while malware producers nimbly tuned their product mix to capitalize on cybercrime hot spots like cryptojacking and ransomware. Let's take a closer look at our key findings:

Vulnerabilities have **more than tripled** over the past ten years



New vulnerabilities smashed records, hitting an all-time high in 2021, with 20,175 new CVE (common vulnerabilities and exposures). That's up 10% from 2020—the biggest percentage jump we've seen since 2018 and the first time new vulnerabilities have topped 20,000 for a single year.

[back to top](#)

This latest crop of vulnerabilities adds to a mountain of accumulated security debt. The total number of CVEs published over the last ten years reached 166,938 in 2021—a three-fold increase over a decade.

OT vulnerabilities nearly double in one year

As rapid as the rise in overall vulnerabilities was, security flaws in OT products grew even faster, increasing by 88% year over year. These vulnerabilities are especially worrisome given the precarious state of OT security. The number of OT devices deployed in enterprises has risen dramatically in recent years. Many of these systems have few or no cybersecurity controls in place and are increasingly connected to networks, exposing them to attacks. [Learn how Skybox 'scan less' vulnerability detection helps you find 'unscannable' OT vulnerabilities.](#)

Cryptojacking and ransomware top new malware charts

Malware producers are turning out a widening array of products and services keyed to the latest cybercrime trends. The number of new cryptojacking and ransomware programs grew by 75% and 42%, respectively, reflecting a growing demand for these increasingly lucrative and popular forms of exploit. Easy-to-use malware, exploit kits, and malware-as-a-service (MaaS) have made it remarkably simple for non-expert hackers to mount attacks and reap rapid financial returns.

Faster weaponization of vulnerabilities

One of the more notable trends we identified is the shrinking interval between the appearance of vulnerabilities and the development of exploits designed to take advantage of them. We found 168 vulnerabilities that were published in 2021 and targeted by exploits within the same year. That's **24% more** than the number of vulnerabilities published and subsequently targeted by exploits in 2020. It's another sign that threat actors are upping their game and moving more aggressively to cash in on emerging opportunities.

Among those newly discovered vulnerabilities that were promptly exploited is the [notorious Log4Shell vulnerability](#) — a flaw in the massively popular Log4j open-source library that's used in hundreds of millions of devices. The Log4Shell vulnerability was publicly disclosed in early December 2021. By the end of the month, there were already known 15 malware programs designed to exploit it.

As vulnerabilities mount, attacks follow

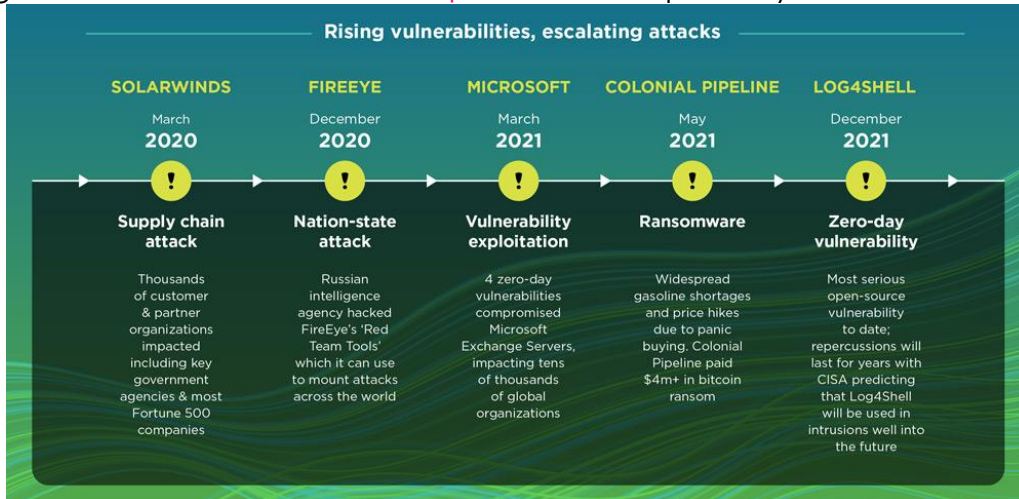
These trends leave security teams between a rock and a hard place. Proliferating vulnerabilities are creating more opportunities for breaches, and new malware and exploits are making it easier than ever for bad actors to capitalize on those opportunities.

It's a worst-of-both-worlds combination, emboldening threat actors and leading to more frequent and more audacious cyberattacks. In 2021 we witnessed some of the most brazen incidents to date. They include:

- **Zero-day attacks more than doubled in 2021**¹. A series of zero-day attacks exploited vulnerabilities in Microsoft Exchange Server, impacting tens of thousands of organizations.

- **Supply chain attacks**, such as those targeting IT software from SolarWinds and Kaseya, as well as the Log4Shell vulnerability.
- **Critical infrastructure attacks**, wreaking havoc on vital operations and services. Examples include the Colonial Pipeline ransomware attack that disrupted fuel supplies in the southeastern U.S.

The average **cost of data breaches hit \$4.24 million**, up nearly 10% from 2020².



Clearly the old vulnerability management playbook that many organizations still rely on is badly out of step with today's threat landscape. Traditional, reactive measures such as scanning and patching are too little, too late in a world where the attack surface is exploding, vulnerabilities are rampant (and are often difficult or impossible to scan and patch), and threat actors are increasingly aggressive. It's time to get out of reactive mode and embrace a truly proactive security posture.

What's next?

SecureCraft is a distributor of Skybox Security since 2019. To find out more about Skybox Security and SecureCraft, please email SecureCraft at sales@securecraftasia.com. Alternatively, you may call us at +65 6291 0508 or visit our website at www.securecraftasia.com.

Article from our IoT Sponsor, Cisco

Securing critical infrastructure: 3 actions to take ASAP

Ruben Lobo

The [Colonial Pipeline](#) attack is another reminder that critical infrastructure needs stronger protection. The problem isn't the lack of available cybersecurity solutions. It's the opposite. With so many solutions available, deciding which ones will provide the most value can be overwhelming. It's a similar feeling to how we felt as children in a toy store, while clutching our pocket money.

[back to top](#)

For basic protections, here are three actions that every critical infrastructure provider should take immediately.

Step 1 – Keep unauthorized people out

Numerous attacks on critical infrastructure can be traced back to a poorly managed user account. Maybe an employee or contractor jotted down login credentials for a rarely used account on a post-it. While that's a violation of security policy, it happens all the time. If you don't use [multi-factor authentication](#) (MFA), anyone who finds the post-it in a coffee shop can log in.

To prevent that scenario, start by creating a central directory (Active Directory or LDAP). Add an account for everyone and everything (camera, meter, etc.) that's allowed to connect to the IT or industrial network. Then require MFA for every internet access attempt—a one-time code sent via email or SMS in addition to the login. Adopting MFA is relatively simple with the [Cisco Duo](#) cloud service because it doesn't require any hardware or software. Duo also checks that devices like laptops or phones comply with your security policy before allowing them to connect.

Step 2 – Know who and what is on your network at all times

Do you know every asset that's connected to your OT and IT networks? About half of the companies we talk to don't. That's a problem because you can't protect what you're not aware of. If you do know, how long before you find out that something foreign has connected—say, an unauthorized sniffer or access point? And can you see who has accessed which files and systems?

To automatically discover every asset connected to your OT network, use [Cisco Cyber Vision](#). It also monitors industrial communications to detect abnormal behavior and raise alerts. To know what's on your IT network, use [Cisco Secure Network Analytics](#) or [Cisco DNA Center](#). To see who is moving what files to which systems, use Secure Network Analytics, and to analyze file trajectories, use [Cisco Secure Firewall Management Center](#). In an earlier job, I managed security for product designs. If we had tools back then like we have now, we could have prevented a theft of intellectual property more effectively and with a less effort.

Step 3 – Minimize the blast radius by segmenting the network

When malware does sneak through the defenses, segmenting the network keeps the threat from spreading to other segments. The smaller the segment, the less the damage. The most basic step is to segment the industrial network from the IT network, by having an Industrial DMZ. Better, segment the industrial network into “zones” containing only assets that need to communicate with each other, using [Cisco Secure Firewall](#). Eventually, you can make each device its own segment using [Cisco Identity Services Engine \(ISE\)](#) and our [industrial ethernet switches](#). That's the gold standard because you can build rules to strictly control which devices can communicate, under what circumstances.

Act before attackers do

The three steps I've outlined—access controls, visibility, and segmentation—go a long way towards securing critical infrastructure. They're like the basic food groups. After that you can go back to the toy store to make cybersecurity continually stronger. To learn more about how you can secure your critical infrastructure, [visit our IoT security page](#) or [contact us](#) to have a conversation around your industrial IoT security challenges.

Article from The Cybersecurity Awards 2021 Winner – Responsible Cyber



I, Magda Chelly, with my co-founder Mikko Laaksonen and our team at Responsible Cyber are enormously proud and humbled to receive the Cybersecurity Award 2021 – SME Vendor Category. I would like to thank the Association of Information Security Professionals from the bottom of my heart for the honor of being selected and for receiving the award.

This award has humbled me. The award has caused me to reflect. And perhaps mostly, I hope this award demonstrates that sometimes small company's efforts can play an important role in the lives of security professionals, and the overall cybersecurity ecosystem.

But this award is for every member of the team. They have been instrumental in supporting our business and achieving several milestones during our journey.

In a world where cyber breaches are at epidemic levels, it is now more important than ever for SMBs to have the right tools in place so they can stay safe; our cybersecurity community bears the civic responsibility for educating the wider public to build a safer cyber environment. That is why our team has been working tirelessly over two years now on IMMUNE—a platform that will enable SMBs to assess and remediate their cyber postures, and stay cyber safe, streamline and automate tedious form filling by insurance brokers whilst enabling them to educate and advise their clients on their cyber risks, and

allow managed service providers (MSPs) to efficiently manage their customers' cybersecurity positions.

Outside of developing IMMUNE, our very own SaaS cybersecurity platform, our team continued to take on consultation assignments, community engagements and got involved in community and collaborative work. We are thrilled to have been involved in Women on Cyber, and the Ladies-in-Cyber initiatives amongst others.

'Work from home' did not slow down our compact, international but close-knit team of eleven full timers and more interns carrying seven different passports – an attestation that there are no borders in the cyberworld.

The year ahead will be an exciting one for our team. We would like to thank AiSP for the honor. Winning this award has been an encouragement in its own right, a validation of all the hard work we have put in and will bolster our team's passion and efforts in the field going forward. As a team, we look forward to more opportunities to collaborate with our larger cybersecurity community to build a cyber safe environment for everyone.

About Responsible Cyber

Responsible Cyber has been in the business of empowering businesses, small and large, with comprehensive cyber security support through their innovative solutions, open sharing of cyber security know-how and extensive awareness outreach initiatives to those in and outside of the industry since its incorporation in 2016. With seasoned cyber security professionals at the helm, and as a newly-crowned World Economic Forum New Champion, Responsible Cyber activates impactful networks to bring our 360° cyber security platform, IMMUNE, to global markets and businesses.

Visit <https://responsible-cyber.com/> for more information.



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

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

New course by
EC-Council
www.eccouncil.org

A First of its kind
Vendor Neutral and
Vendor Specific Certification

The **Next Dimension**
in Cloud Computing

CCSE
Certified Cloud Security Engineer

Become a **Certified Cloud Security Engineer (CCSE)**

The CCSE Program Advantage

- 50+ Hands-on Intensive Labs
- Mapped to 20 Cloud Job Roles
- Mapped with Real-Time Industry Job Roles

AWS AWS Cloud

Azure Azure Cloud

Google Google Cloud Platform

REGISTER NOW

Brought to you by Wissen – EC-Council Exclusive Distributor APAC

WISSEN
Cyber Security Competency Development

Email us for more info
aisp@wissen-intl.com

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

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

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

[back to top](#)

Listing of Courses by ALC Council



Stand out from the crowd

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

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

Qualified Information Security Professional (QISP®) Course



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

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

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

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

COURSE DETAILS

2022 Course dates can be found on https://www.aisp.sg/qisp_training.html

Time: 9am-6pm

Fees: \$2,500 (before GST)*

*10% off for AiSP Members @ \$2,250 (before GST)

*Utap funding is available for NTUC Member

TARGET AUDIENCE

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

COURSE CRITERIA

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

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

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

Program Partner

Delivery Partners





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

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

Course Objectives

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

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

COURSE DETAILS

Training dates for year 2022 can be found on https://www.aisp.sg/cyberessentials_training.html

Time: 9am-6pm

Fees: \$ \$1,600 (before GST)*

*10% off for AiSP Members @ \$1,440 (before GST)

*Utap funding is available for NTUC Member

TARGET AUDIENCE

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

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

Program Partner



Delivery Partners



MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

If you are currently a full-time student in the IHLs that are onboard of our [Academic Partnership Programme \(APP\)](#), AiSP is giving you complimentary Affiliate Membership during your course of study. Please click [here](#) for the application form and indicate your student email address, expected graduation date and name of your institution in the form.

Complimentary Affiliate Membership for NTUC Members

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2021 to 2022) from 1 Sept 2021 to 31 Dec 2022. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. [This does not include Plus! card holder \(black-coloured card\), please clarify with NTUC on your eligibility.](#)

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

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

AVIP Membership

AiSP Validated Information Security Professionals ([AVIP](#)) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development and career progression for our professionals. Interested applicants should be qualified [AiSP Ordinary Members \(Path 1\)](#) for at least a year to apply for AVIP.

Your AiSP Membership Account

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

Membership Renewal

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

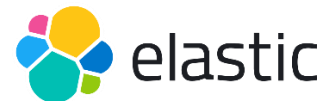
[Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!](#)

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



Acronis





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



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.



 www.AiSP.sg

 secretariat@aisp.sg

 +65 8878 5686

 116 Changi Road, #04-03 WIS@Changi, S419718

Please [email](#) us for any enquiries.