NEWS & UPDATE

AiSP New Corporate Partners

AiSP would like to welcome SecurID - RSA and IBM as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

Digital Transformation Summit Asia

AiSP Committee Member, Tony Low spoke at the Digital Transformation Summit Asia held on 27 August 2021. He shared his insights related to this year's theme: SAFEGUARDING ORGANIZATIONS FROM CYBER THREATS: SECURING THE DIGITAL TRANSFORMATION. It was an insightful session along with other distinguished speakers in the panel.

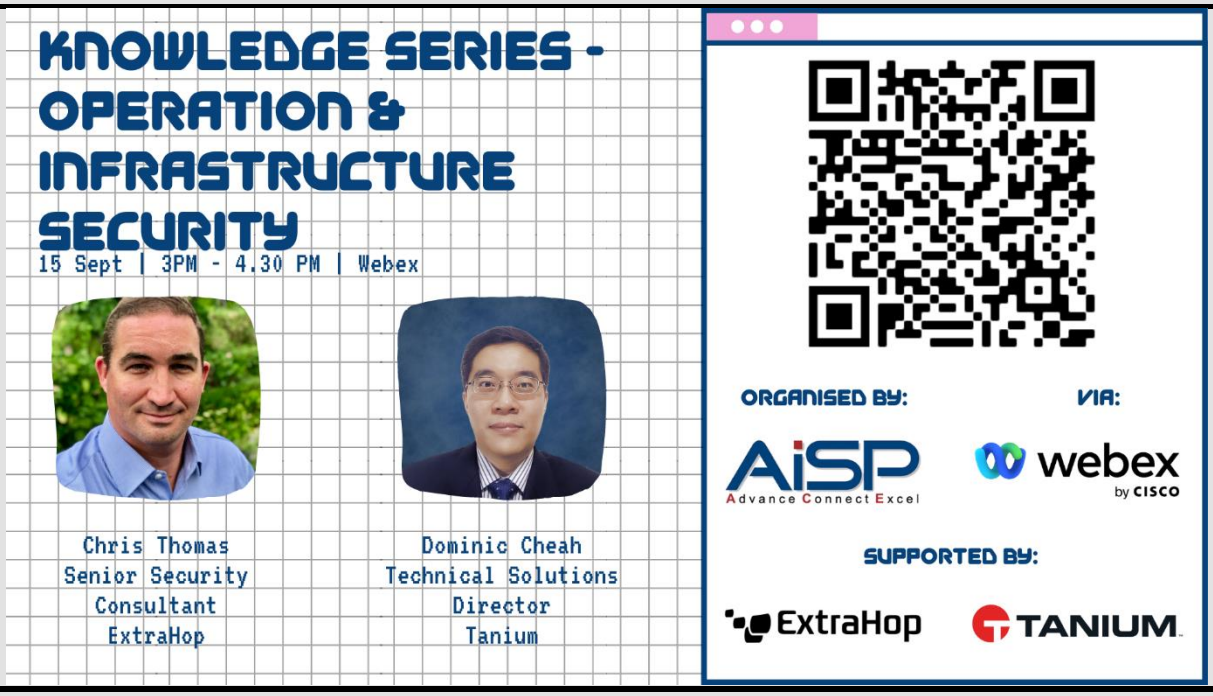
AiSP Knowledge Series Events

Upcoming BOK Events

Operation & Infrastructure

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

AiSP Knowledge Series – Operation & Infrastructure Security



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

Defining an XDR strategy: What does it mean for your organisation?
By Chris Thomas, Senior Security Consultant, ExtraHop

XDR (extended detection and response) is the hot new buzzword in the security industry but so far there isn't a lot of agreement on what defines XDR. The goal makes sense. Extend your detection capabilities across your hybrid network to catch

advanced threats like zero days, supply chain attacks, and insider threats, and respond quickly before damage can be done.
Join us as we explore the pros and cons of XDR such as, is it realistic that one vendor can offer you all the tools you need for detection and response or will you need to create a strategy to achieve your own extended detection and response ecosystem.
Attendees will walk away with a better understanding of:

- How to define what XDR means for your organisation
- How to create your own XDR strategy
- Why network data is an essential building block for any XDR ecosystem

Accelerate Your Operations and Regain Visibility and Control
By Dominic Cheah, Technical Solutions Director, Tanium

The number of point solutions used across IT Operations and Security teams have skyrocketed over the past few years. To ensure data privacy compliance alone, organizations are using an average of 43 disparate tools.
The result is a slow, complex and siloed IT environment that's hard to operate and even harder to secure, with teams and tools increasingly working in silos. Legacy tools and disjointed point solutions place limitations on IT Operations and Security teams who are faced with increasingly frequent and dynamic threats.
Hear examples of how organizations can take a holistic approach, with a unified endpoint management and security platform. It will provide organizations with accurate data on their environment in real time to improve their Cyber Hygiene. This will create a process to allow continuous identification of risks and vulnerabilities across their assets and fix them with speed and at scale.

Date: 15 September 2021 (Wed)
Time: 3.00PM – 4.30PM
Venue: Webex
Registration:
https://aisp.webex.com/aisp/j.php?RGID=r81a75a61a334fd076693f24c2e8c1d73

Follow AiSP Today to CONNECT with us!		
Facebook	Instagram	LinkedIn

About our Knowledge Series

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its **Information Security Body of Knowledge 2.0** topics. Our scheduled topics for webinars in 2021 are as follows (*may be subjected to changes*),

1. CTI SIG, 29 Sep (hybrid*)
2. IOT, 27 Oct*
3. Emerging Trends – Blockchain & AI for Cyber Security, 17 Nov
4. Red Team VS Blue Team, 9 Dec

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

Please let us know if your organisation is keen to be our sponsoring speakers in 2021!

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

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

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

Students
4. Students

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

The Cybersecurity Awards 2021 winners will be announced at The Award Ceremony 2021.

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

TCA2021 Sponsors & Partners

Organised by

Supported by

Supporting Associations

Community Partner

Supporting Organisation

Platinum Sponsors

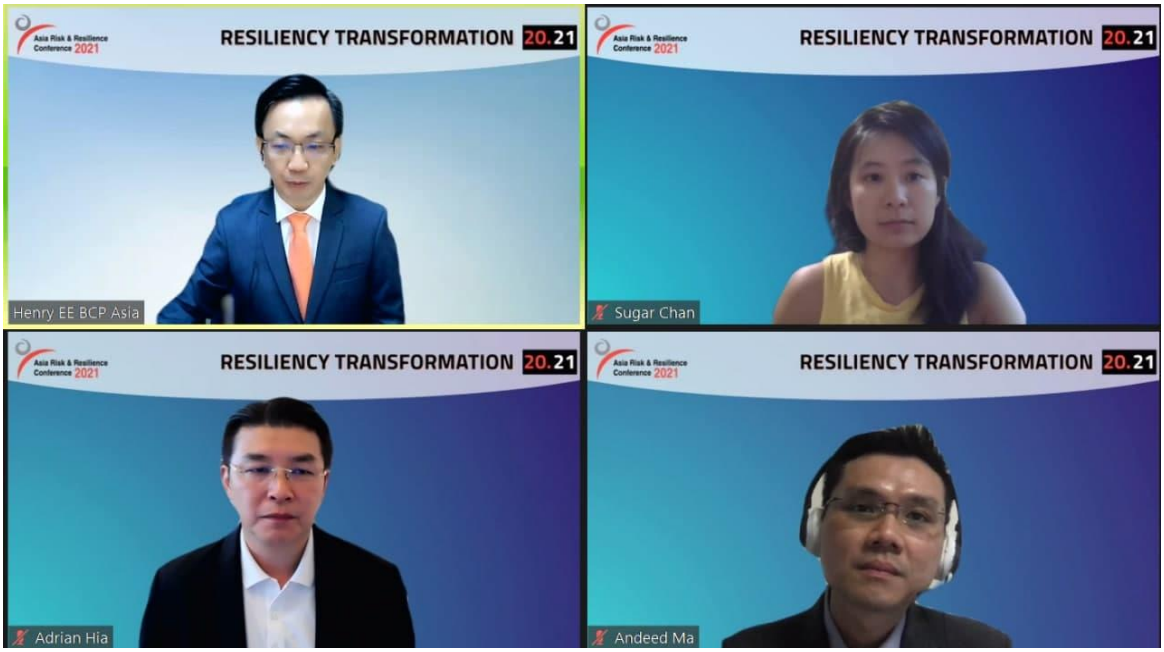
Gold Sponsors

Silver Sponsors

Cybersecurity Awareness & Advisory Programme (CAAP)

Asia Risk & Resilience Conference (ARRC) 2021 on 18 August

On 18 August, Asia Risk & Resilience Conference 2021 commenced with the theme of "Resiliency Transformation 20.21". Ms Sugar Chan (AiSP Committee Member) was one of the panel speakers on the topic of Cyber Security. During the 2-day conference, ARRC 2021 will focus on the huge transformations that almost all industries and organisations had to make in a short period of time and how this flexibility lent great strength to the resiliency of the business.



Upcoming CAAP Events

AiSP hope to elevate Cybersecurity Awareness as integral part of SME Business Owner Fundamentals and Establish a Self-Sustainable Support Ecosystem programme with active participation from Agencies, Business Associations, Security Communities and Vendors.

Join our upcoming events below to expand your knowledge on cybersecurity issues.

AiSP x PA CAAP Focus Group Discussion – Singapore SMEs' Digital Adoption and Concerns

AiSP hope to elevate Cyber Security Awareness as integral part of SME Business Owner Fundamentals and Establish a Self-Sustainable Support Ecosystem programme with active participation from Agencies, Business Associations, Security Communities and Vendors.

In partnership with PA's Emergency Preparedness Division and Association of Information Security Professionals, this focus group discussion aims at raising SMEs' awareness of cyber risks and adoption of cyber practices. It caters to SMEs across industries, particularly those not in the IT fields to better protect your businesses in the cyber space.

Join us in this focus group discussion as we discuss together about the immediate concerns arising from rising cyber threats, concerns about cybersecurity incidents in companies and sentiments about the importance of cybersecurity for your business from your management and staff.

Date: 08 Sept 2021 (Wed)
Time: 7.00pm to 9.00pm
Venue: Ensign InfoSecurity, 30A Kallang Place, #08-01, Singapore 339213
Registration: forms.office.com/r/msWyEmt7s1

AiSP SME Cybersecurity Conference 2021

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

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

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

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

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

Date: 11 November 2021 (Thursday)
Time: 10:00 am – 4:00 pm
Venue: Lifelong Learning Institute

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

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

Organised by: **Supported by:**

Sponsors

Supporting Partners

Student Volunteer Recognition Programme (SVRP)

Our **SVRP 2021 nomination form** is available now for IHL students to apply! To encourage more students to volunteer, secondary school and pre-university students are welcome to participate! Please refer to **SVRP framework** and **SVRP 2021 nomination form for secondary school and pre-university students**! We are having a student volunteer drive from now till Dec 2021 for those who are interested to volunteer but not sure where to start. Please **click here** to apply today.

Under AiSP's **Academic Partnership Programme (APP)**, the IHLs can include AiSP Student Chapter in their respective institutes. Please refer to our **Student Chapters** for the list of current committee members and we look forward to expanding the list in 2021!

SINGAPORE CYBER SECURITY INTER ASSOCIATION (SCSIA) CYBER DAY QUIZ

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

From 25 March onwards, 3 questions will be posted on Facebook and Linkedin every Thursday. **Answers will be revealed after 30 September** (when the competition ends). Please note that you must complete all **29 weeks of questions** to qualify for the total scoring.

E-Certificate of Participation will be given to all participants. **Attractive Prizes will be given to the top scorers.** You may find the link access below to the past quiz questions. Stay tuned to our Facebook and LinkedIn for the upcoming quiz questions!

Week 1 Quiz https://forms.office.com/r/XGHBUPQJJe	Week 2 Quiz https://forms.office.com/r/gWsMr1ZfLs
Week 3 Quiz https://forms.office.com/r/ikiwzBiSnV	Week 4 Quiz https://forms.office.com/r/C0XdFvtqcs
Week 5 Quiz https://forms.office.com/r/bPYdNn3Ytm	Week 6 Quiz https://forms.office.com/r/gmgSSn2syS
Week 7 Quiz https://forms.office.com/r/dV0m8WmvHP	Week 8 Quiz https://forms.office.com/r/9B9ifeCibT
Week 9 Quiz https://forms.office.com/r/1fx4XZq8fx	Week 10 Quiz https://forms.office.com/r/QTgzkfkckJ

Week 11 Quiz https://forms.office.com/r/iKTdAXy4Wc	Week 12 Quiz https://forms.office.com/r/G60xJEqHpb
Week 13 Quiz https://forms.office.com/r/FrwapxXVZP	Week 14 Quiz https://forms.office.com/r/ruKgZ3XaUp
Week 15 Quiz https://forms.office.com/r/5B4Wq1LqZS	Week 16 Quiz https://forms.office.com/r/x880GsNhNs
Week 17 Quiz https://forms.office.com/r/TnfYnVEWhc	Week 18 Quiz https://forms.office.com/r/PUuZKeK7xa
Week 19 Quiz https://forms.office.com/r/AKLFC1HGay	Week 20 Quiz https://forms.office.com/r/VQ4RNvE4Yb

Week 21 Quiz https://forms.office.com/r/jq9ZL1618S	Week 22 Quiz https://forms.office.com/r/ttKVX2MhzL
Week 23 Quiz https://forms.office.com/r/zuiFfc0Buk	

Singapore Cyber Day 2021

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

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

SCSIA aims to inspire future generation of youths on opportunities in Cybersecurity. They are reaching out to primary and secondary schools and pre-universities to talk about the cybersecurity profession and how everyone can take part in Singapore's cybersecurity ecosystem and contribute towards our cyber resilience.

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

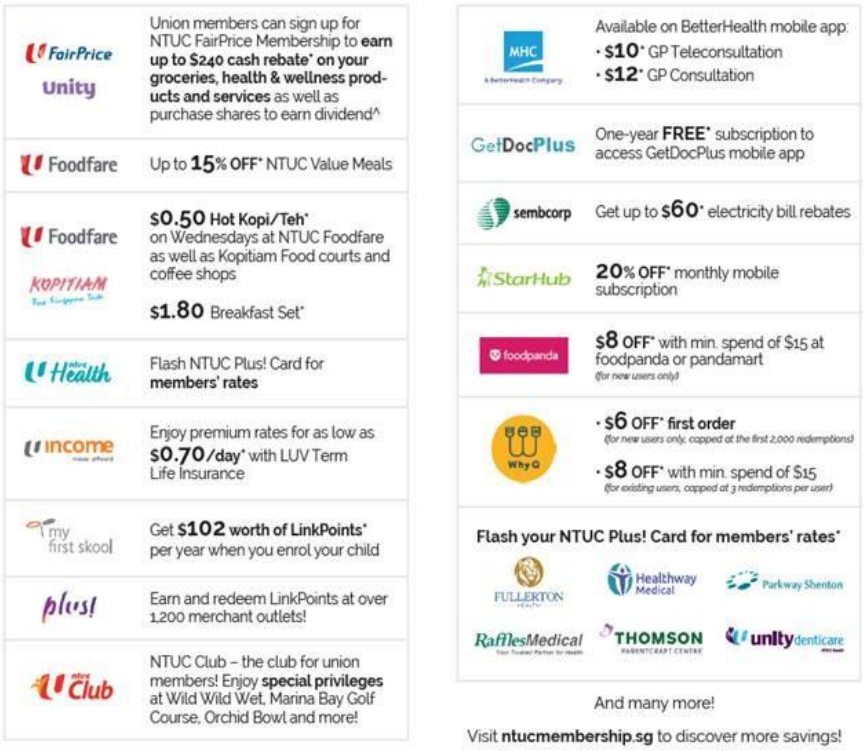
1. Part 1: Virtual Event with the launch of videos and quiz and sharing by speakers from the professional bodies and associations.
2. Part 2: Videos and quiz for the students to take part in during the school holidays. The Singapore Cyber Security Inter Association (SCSIA) has organized an online quiz competition for primary, secondary and tertiary students (aged 25 years and below) in Singapore with the support from the Cyber Security Agency of Singapore. This competition aims to pique interest in students and equip them with knowledge on Cyber Security. This initiative was announced on 2 November 2020 and officially launched on 25 March 2021.

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

Supporting Associations

Sharing of Cybersecurity with NTUC Members

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



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

Ladies in Cybersecurity

Ladies Talk Cyber Series

For the Fifth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Daisy Radford, BAE Systems' Head of Operations and Delivery for APAC. She shared on her experiences with BAE Systems and how we can encourage more women to enter the field.

How to be successful in cybersecurity field

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

Introducing women with a deep interest in cybersecurity

Daisy Radford is BAE Systems' Head of Operations and Delivery for APAC, based in Singapore she leads a team of programme managers, engineers and software developers in delivering communication intelligence and cyber defence capabilities.

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

International Cyber Women Day 2021

(Photo taken in 2019 during the AiSP Ladies Night)

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

AiSP will also be organising a few ladies in cyber events in September to commemorate International Cyber Women Day 2021. We looked forward to having you in our AiSP Ladies in Cyber events.

To find out how you can sponsor, volunteer, or play a part in our programmes, please contact us at secretariat@aisp.sg today.

AiSP Ladies in Cyber Spill the Tea on 1 September 2021

Join Alina, Ee Lin & Sherin moderate by Faith on 1 September 2021 at 7pm to celebrate International Cyber Women Day 2021 as we hear what our 4 female leaders experience and their biggest setback that they faced in their Cyber Security journey in a Spill the Tea Session. This is part of Cyber Security Agency of Singapore SG Cyber Women X Series.

All female students and professionals with an interest in Cybersecurity are welcome to join in the webinar. Sign up at https://tinyurl.com/lic010921. Registration will close 1 hour before the webinar.

AiSP Ladies in Cyber Learning Journey & Fireside Chat on 24 Sept 21 (Fri) at CISCO Office (Hybrid Format)

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

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

This September, **AiSP Ladies in Cyber** is organizing a hybrid fireside chat together with our Corporate Partner Cisco Systems. Join **SMS Sim Ann, Wendy, Catherine and Sherin** - our female leaders from Cybersecurity industry as they share their experience, advice and provide guidance on career in IT industry for females.

Date: 24 Sep 21 (Fri)
Time: 7.30pm to 8.45pm (Please join in 5 mins before the session)

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

Please email to secretariat@aisp.sg to find out more details on the event.

AiSP Ladies in Cyber Inaugural Symposium on 10 Nov 21

As part of celebrating SG Women 2021, AiSP will be organising the inaugural Ladies in Cyber Symposium for the female Youths that highlights 4 different topics on cybersecurity, including the importance of cybersecurity, and how women can play a role in it. We are expecting 150 Youths and professionals (Subject to COVID-19 restrictions) at the event. The theme for this year Symposium is "**How can Women in Tech define the future of Cyber & Tech".**

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

The event will be held on 10 November 2021 at Life-Long Learning Institute with Minister Josephine Teo as the Guest of Honour. She will be having a dialogue session with the attendees during the event. Visit https://www.aisp.sg/cyberfest/ladies_symposium.html for more details on the event. Contact AiSP Secretariat at secretariat@aisp.sg for more information of the event and if you sponsor and be part of it.

Supported by:

CYBER YOUTH SINGAPORE

ENSIGN INFOSECURITY

CONQUER THE UNKNOWN

Sponsors

Checkmarx

CISCO

DBS

GOVTECH

ST Engineering

TANIUM

Women on Cyber

Special Interest Groups

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

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

We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together in 2021. Please contact us if you are keen to be part of our SIGs as we are actively recruiting members for 2021!

Special Interest Group (SIG) Events

Date	Event
16 September 2021	AiSP SIG Induction Event
9 November 2021	Combined SIG Event

Data Security Webinar on 24 August

It was an informative session with the panel which includes Mr Cecil Su (AiSP Assistant Secretary) who shared about various Data Security frameworks and process of data discovery and classification.

We would like to thank all participants and our CPP Partner, Micro Focus as well as Tindo for the enjoyable sharing session.

Article on Cyber Threat Intelligence

Is Cyber Threat Intelligence necessary?

Cyber Threat Intelligence (CTI) may seem like a recent development[1] among cybersecurity practitioners, but its concept and uses can be considered as important as warfare or business intelligence. Challenged by conflicting demands for resources and efforts, organisations worldwide can leverage CTI to develop a proactive cybersecurity posture based on informed decision-making and proved detection of threats. As defined by Gartner, threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets.

Similar in warfare, intelligence is key for successful detection and deterrence to unknown adversaries. Military intelligence uses information collection and analysis approaches to provide guidance and direction to assist in decision-making. An assessment of data from a range of sources, directed towards the mission requirements or as input gathered as part of operational or campaign planning. In order to provide analysis, information requirements are first identified, and then incorporated into intelligence collection, analysis, and dissemination.

Types of Threat Intelligence

There are a number of service providers offering CTI insights and analysis to companies that are susceptible to cyber threats. Faced with wide-ranging of risks and dynamic developments in the threat landscape, CTI helps CISOs and IT security teams to identify their blind spots quickly and assess readiness of their protective measures and defence mechanism. The aggregated findings on threat patterns—especially when it is segmented by industries, would raise the credibility and robustness of in-house cybersecurity assessment when the Board and management ask for relevant data. Thus, there are three types of threat intelligence: Tactical, Operational and Strategic, where organisations may focus on all three or selected one/s for their business purposes, such as the uses of threat intelligence:

1) **Tactical Cyber Threat Intelligence** analyses interactions between the technology environment and threats and is typically used to assist in mitigation of active or expected threats such as a malicious domain name or attacks such as phishing. It is the easiest to be deployed in terms of resources among the three types to identify simple indicators of compromise, but it has very short lifespan.

2) **Operational Cyber Threat Intelligence** considers historical capabilities, affiliations and motivations of threat actors, and is used mostly to make resource-allocation decisions around real and perceived threats. It has longer lifespan than tactical as most threat actors do not change the way they operate often and quickly. CTI

[1] See the United States of America's Cyber Information Sharing Act, 2015.

teams with the mission objective to better understand the adversaries (behind the attacks) would see value in this type of intelligence.

3) **Strategic Cyber Threat Intelligence** focuses on the future, including emerging trends, and is used to make longer-term decisions. Strategic intelligence tends to be the hardest form to generate. It requires good understanding of both cybersecurity and the nuances of the world's geopolitical situation during the data collection and analysis. For example, state-organised attacks are usually linked to geopolitical conditions. Also, financially-motivated cybercrime groups are always evolving their techniques to achieve bigger payoffs.

Information is not Intelligence

Raw and unfiltered information that is not actionable is not intelligence; such information needs to be evaluated and interpreted by trained analysts and be aggregated from reliable sources and cross-correlated for accuracy. To transform information to become intelligence for proper decision-making, organisations can consider the five steps:

1. **Planning and Requirements**
   A clear mission based on your CTI programme's requirements, sets a clear path on the types of information collected and the outcomes in mind.

2. **Collection and Processing**
   There is a lot of information available but not all of types of information is meaningful to your mission. Thus, data acquisition should address how, when, why and what should be collected to fulfil the requirements. Automated tasks for data collection would help to reduce time if the organisations have multiple systems and tracking mechanisms.

3. **Analysis**
   Intelligence analysts would evaluate, analyses and interpret the processed information against requirements, in order to assess the confidence, relevance, likelihood and threat impact. Teams can also assess the gaps in data collection at this stage.

4. **Production**
   The intelligence products such as briefings and technical reports, are produced in a timely manner and be actionable and relevant to stakeholder needs. Any deficiency to requirements should be documented for future improvements to the intelligence cycle.

5. **Dissemination and Feedback**
   Intelligence products are presented to stakeholders, with outline on expected courses of actions and how stakeholders can evaluate the intelligence received. Feedback is important for the CTI team to review programme's requirements

continuously, especially when adversaries' behaviours and tactics can change across time.

Personnel involved

The cost for CTI implementation depends on the organisation's purpose for such information. For companies that wish to disseminate the threat insights to their subsidiaries and as a way to audit their critical vendors, it pays to invest in information collation from credible data points. CIT personnel should ideally have some understanding in risk assessment, to ascertain if the information gathered is valid and useful for their organisation's cybersecurity posture and identified vulnerabilities. There would be a need to connect the dots across during information analysis, to make sense if there could be any hidden spots that are not immediately apparent. Such information may not be limited to system issues or software performance, as breaches can be caused by both external and internal actors. For instance, are we relying on key suppliers handling our business data, that are using on systems that require regular patching? Has there been organisational-wide retrenchment in one of our supply-chain partners?
Personnel and stakeholders involved in any of the three types of threat intelligence are as follows:

1) Tactical – Security Operations Center (SOC) analyst, and personnel involved in SIEM, firewall, endpoints or IDS/IPS.
2)Operational – Threat hunter, SOC analyst, personnel involved in vulnerability management, incident response or insider threat
3) Strategic – CISO, CIO, CTO, Executive Board, personnel involved in strategic intelligence

Potential Pitfalls

While CTI can be used by all organisations of different sizes and scale, not all organisations are able to benefit meaningfully from their investment in CTI. Some potential pitfalls for CIT deployment are:

1) **No or limited analysis to the information collected:** Most organisations focus their efforts on basic use cases, such as integrating threat data feeds with existing network, IPS, firewalls, and SIEMs — without leveraging the insights offered. Without insight, there is no intelligence for proper decision-making.

2) **Significant amount of information collected that is irrelevant to the organisation's specific requirements**: For instance, a pharmaceutical company would value its industry's root cause analysis on data breaches more as compared to latest strategies deployed by cyber attackers for IT industry. Framing the information criteria in the context of companies' business needs not only strengthen companies' focus in their cybersecurity posture, but also add value to CISO's efforts in buy-in from the management, especially when seeking additional budget and resources.

3) **Not able to garner stakeholders' feedback to improve the relevance of intelligence presented**: CTI cannot be effective if it only depends on the efforts of the technical personnel. It requires input from management on the business requirements, so that intelligence can be sharpened and address organisational needs better.

4) **Not able to sustain CTI efforts across time**: While it takes some efforts to start a CTI programme, the intelligence gathered improves across time with timely feedback loop from stakeholders and team's continuous improvement to the intelligence cycle. Aborting the programme before it has the chance to mature, would not enable the organisation to establish its fundamentals in intelligence gathering and threat analysis.

Should my organisation implement CTI?

It depends on your organisational needs and if CTI can play an important part in enhancing your competitive edge and cybersecurity posture. There are various approaches to implement a CTI programme, and companies need to first allocate time, efforts and resources to ensure their programmes can be fine-tuned along the way. Results are not overnight; Management's project sponsorship and pre-determined outcomes are integral drivers to CTI team's performance and value-add in order to achieve organisation's cybersecurity maturity.

About the Author

Yvonne Wong |AiSP Committee Member

Yvonne is a Committee Member of AiSP. She is volunteering in the Cyber Threat Intelligence Special Interest Group (SIG), and Data and Privacy SIG. Yvonne has been a practitioner, consultant and trainer for Governance, Risk and Compliance (GRC) since 2015. Prior to GRC, she has been involved in branding, communications, intellectual property management and strategic planning work in private and public sectors. She is presently the Senior Manager in the Yishun Health Data Protection Office.

Sign up here: AiSP Special Interest Group Induction Event (office.com)

For AiSP Members only

As we are always looking for new ways to engage our members, AiSP has categorised the various ways for **member-only access** as part of our digital engagement during COVID-19 pandemic,

1. Members-only access for **webinar playback**
2. **LinkedIn closed group**
3. Participate in **member-only events** and closed-door dialogues by invitation
4. **Volunteer** in our initiatives and interest groups, as part of career and personal development

If you have missed our virtual events, some of them are made available for members' access via Glue Up platform. Please email (secretariat@aisp.sg) if you need any assistance.

We wish to remind our members to renew their 2021 membership if they have not done so.

Call for Volunteers

As AiSP focuses in raising the professional standing of information security personnel and professions in Singapore since 2008, we have been running various initiatives to address diverse needs and developments. Please **email us** for more details!

(Photo taken on 22 Feb 19 during CAAP Sharing)

Professional Development

QISP® is designed for entry to mid-level Information Security Professionals, and any IT Professionals who are keen to develop their knowledge in this field. It will be enhanced to complement AiSP's Information Security Body of Knowledge (IS-BOK) 2.0._Our online examination via Pearson VUE platform would be deployed worldwide in 2021.

QUALIFIED INFORMATION SECURITY PROFESSIONALS (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

Date Selection available till December 2021
Time: 9am-6pm
Fees: $2,500 (before GST)*

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

TARGET AUDIENCE

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

COURSE CRITERIA

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

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

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

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

Please **contact AiSP** if you are keen to leverage the enhanced QISP® for your learning and development needs, or you would like to develop courseware based on AiSP's IS-BOK 2.0 overseas.

CYBERSECURITY ESSENTIALS COURSE

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

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

Course Objectives

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

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

- Cybersecurity Operations

COURSE DETAILS

Date Selection available till December 2021
Time: 9am-6pm
Fees: $ $1,600 (before GST)*

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

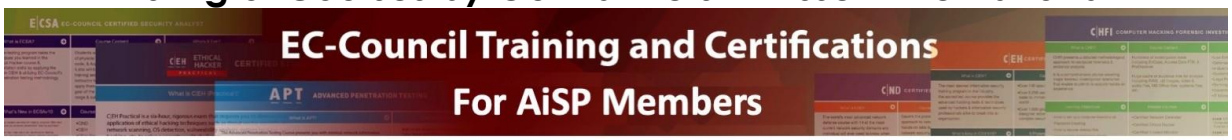
TARGET AUDIENCE

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

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

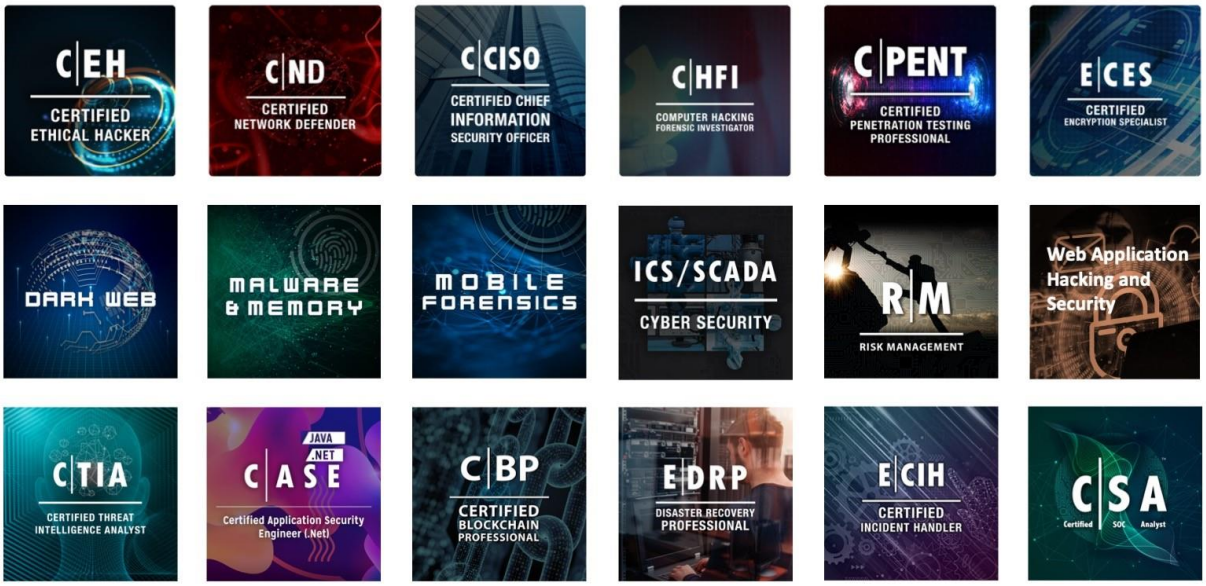
For registration or any enquiries, you may contact us via email at secretariat@aisp.sg or Telegram at ***@AiSP_SG****.*

Listing of Courses by Our Partners – Wissen International



Besides attending EC-Council training and certification courses at local authorised training partners,

AiSP members can now enjoy alternative learning options with members-only discounts!



Members enjoy 20% discount

Self-Paced Learning with Videos

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

Students enjoy academic price

Self-Paced Learning without Videos

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

Contact us for member's rate

Masterclass Training Workshop

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

CyberQ

Cyber range Platform-as-a-Solution

TRAIN I PRACTICE I ASSESS I COMPETE

EC-Council aware

When Everyone Protects

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

codered FROM EC-COUNCIL

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

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

Listing of Courses by Our Partners – ALC Training Pte Ltd

A CAREER IN SECURITY ARCHITECTURE

The Strategic Role of the Security Architect

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

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

SABSA® Security Architecture

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

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

SABSA® Certification Roadmap

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

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

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

CREST SINGAPORE CHAPTER

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

UPCOMING ACTIVITIES/ EVENTS

Ongoing Activities

Date	Event	By
Jan-Dec	Call for Female Mentors (Ladies in Cyber)	**AiSP**
Jan-Dec	Call for Volunteers (AiSP Members, Student Volunteers)	**AiSP**

Upcoming Events

Date	Event	By
1-Sep	Ladies in Cyber – Spill the Tea	AiSP
2-Sep	ISACA Singapore Annual GTACS 2021	Partner
8 – 9 Sep	OT-ISAC Summit 2021	Partner
8-Sep	AiSP x PA CAAP Focus Group Discussion	AiSP & Partner
9-Sep	AiSP x SCS CAAP Focus Group Discussion	AiSP & Partner
14-Sep	PDP Seminar	AiSP & Partner
15-Sep	Knowledge Series – Operation & Infrastructure Security	AiSP
15 – 16 Sep	CIISec Live by CII SEC	Partner
17-Sep	Empowering women on the Frontlines of Cybersecurity Webinar	AiSP & Partner
15 Sep to 30 Nov	SMEICC Conference Series 2021	Partner
16 Sep	SIG Combined Event	AiSP
18-Sep	ASEAN Students Contest on Information Security 2021 by VNISA	Partner
24-Sep	Ladies in Cyber Learning Journey & Dialogue Session at Cisco	AiSP & Partner
29-Sep	Knowledge Series - CTI	AiSP
20-Oct	AiSP X ASPRI CAAP Webinar	AiSP
26-Oct	ATIC Webinar	AiSP & Partner
27-Oct	Knowledge Series – Internet of Things	AiSP

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

CyberFest® is a community-led initiative that would take place from 08 to 12 Nov 2021 in Singapore.

CONTRIBUTED CONTENTS

Insights from The Cybersecurity Awards 2020 Winner – Acronis

In cyberattacks, SMBs face an existential threat

Cyberthreats, and ransomware in particular, have generated considerable news coverage this year. The attack on the Colonial Pipeline resulted in widespread gasoline shortages and mass transit disruptions, while a strike against JBS disrupted supply chains worldwide.

By utilizing supply-chain attacks against managed service providers (MSPs), attackers gain access to both the MSP business and all of its clients. As seen in the SolarWinds breach last year and the Kaseya VSA attack earlier in 2021, one successful attack means they can breach hundreds or thousands of SMBs downstream.

Now, with the Acronis Cyberthreats Report Mid-year 2021, we not only see troubling new developments in the threat landscape from the first half of the year: It's also clear that SMBs are now at significant risk — and service providers must react.

SMBs face greater risks than ever before

SMBs may feel safe in the supposition that they're "too small to target." In reality, they're increasingly vulnerable due to increases in attack automation and supply-chain attacks against their IT service providers. Cybercriminals are eagerly targeting managed service providers (MSPs) in a bid to compromise scores of their clients at once. For most SMBs, just one such incident could sound their death knell.

During the first half of 2021, **four out of five organizations** experienced a cybersecurity breach that originated from a vulnerability in their third-party vendor ecosystem. During that same period, the average cost of a data breach rose to around **$3.56 million**, and the average ransomware payment

topped **$100,000** — a 33% jump. While these figures would be a significant financial hit for any company, they're simply fatal for the average small or medium business.

Here are a few more of our key findings from the Acronis Cyberthreats Report Mid-year 2021:

- **Phishing attacks are rampant.** The use of social engineering techniques to trick unwary users into clicking malicious email attachments or links rose 62% from Q1 to Q2. That spike is of particular concern since 94% of malware is delivered by email. During the same period, Acronis blocked more than 393,000 phishing and malicious URLs per month, preventing attackers from accessing business-critical data and injecting malware into clients' systems (or your own).
- **Data exfiltration continues to increase.** Last year, more than 1,300 ransomware victims had their data publicly leaked after an attack. Cybercriminals are looking to maximize their financial gain, and these tactics increase the pressure on victims to pay up. During the first half of 2021, more than 1,100 data leaks have already been published — at this rate, we'll be looking at a year-end increase of 70% over 2020.
- **Remote workers continue to be a prime target.** The COVID-19 pandemic drove a major shift to remote-first work that continues today. Two-thirds of remote workers now use work devices for personal tasks and use personal home devices for business activities — and attackers have taken note. Acronis observed the number of global cyberattacks to more than double, with a 300% increase in brute-force attacks against remote machines via RDP.

SMBs turn to IT service providers because they lack the resources or technical expertise needed to counter today's rapidly evolving cyberthreats. As an MSP, your clients depend on you not only to turn to solutions that effectively defend against cutting-edge attacks, but also to stay abreast of the latest developments in the cyberthreat landscape and react accordingly.

About the Acronis Cyberthreats Report

The Acronis Cyberthreats Report Mid-year 2021 is based on examining attack and threat data collected by the company's global network of Acronis Cyber Protection Operations Centers (CPOCs), which monitor and

research cyberthreats 24/7. Malware data was collected by more than 250,000 unique endpoints around the world running Acronis Cyber Protect (either as a client of an MSP using Acronis Cyber Protect Cloud or a business running Acronis Cyber Protect 15). The mid-year update covers attacks targeting endpoints detected between January and June 2021.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain-based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on-premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,600 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages.

For more information or to get connected, please visit www.acronis.com or contact Seok Cheng at seokcheng.chia@acronis.com

Insights from our Corporate Partner Programme (CPP) – Extrahop

SANS on Defining and Measuring Cybersecurity Visibility

Security visibility is a lot like modern art—it varies from critic to critic, and while it's difficult to define, most people (and security experts) know it when they see it.

Set and Evaluate Visibility Strategy to Enhance Your Security Posture.

- Learn how to develop a well-defined strategy that aligns divergent goals
- Find out how to bridge visibility gaps to move toward proactive and predictive security
- Discover how to set meaningful metrics to objectively measure success

whitepaper

SIEM Alone Won't Stop Advanced Threats. Integrated NDR & SIEM Can. Here's Why.

Ransomware was a $350+ million dollar business in 2020, and all signs point to major growth in 2021. We saw increased usage of the double-extortion method, in which ransomware gangs exfiltrate data and threaten to release it publicly, on top of their traditional encryption-for-ransom scheme, to extract even greater payments from victims. You can now expose sophisticated attackers quickly with greater threat coverage, catch unknown threats and reduce response time with integrated NDR + SIEM.

Integrate ExtraHop network detection and response (NDR) with your security information and event management (SIEM) to modernize your security operations center (SOC) to catch more unknown threats and accelerate time to detect and respond. Enable next-gen security postures, such as Zero Trust and extended detection and response (XDR).

- Uncover critical details to quickly detect and respond to threats
- Learn how rich data and context builds a confident security team
- Discover how correlated forensics and SIEM logs improve investigation

Solution Brief

ExtraHop is the Founding NDR Provider in the XDR Alliance

Today, Exabeam announced the XDR Alliance™, a partnership of leading cybersecurity industry innovators committed to an inclusive and collaborative extended detection and response (XDR) framework and architecture. The XDR Alliance consists of leading vendors in security information and event management (#SIEM), endpoint detection and response (#EDR), network detection and response (#NDR), email security, and other key security product categories.

Link

Please contact Ms Stephanie Kwok at stephaniek@extrahop.com if you have any queries.

Insights from our Corporate Partner Programme (CPP) – SecurID

SecurID - Governance and Lifecycle Delivered From The Cloud

Remember about 15 months ago when we still accessed networks, resources, and apps directly from the corporate network?

For many of us, that ended with the onset of the pandemic: today, the bulk of these requests are made remotely. As businesses work through this change and shift to a permanent hybrid / work-from-anywhere dynamic, strong access governance becomes increasingly important to maintain control, accountability, and compliance. Whether you're managing new employees or working with staff who have switched roles internally, it's becoming increasingly important for security teams to maintain visibility and control throughout the joiner-mover-leaver process and limit users' ability to the bare minimum degree of access they need to do their job.

Simply put, you need to know **who** has access to **what**, **how** they got access, and **why** they need access. Since 2006, SecurID Governance and Lifecycle (G&L) has provided Fortune 100 and global enterprise customers with the Identity Governance and Administration (IGA) capabilities needed to gain visibility, insights, and control over access to all applications, systems, and data. SecurID G&L Cloud will offer our full-featured, high-performing solution and market-leading capabilities delivered from the cloud, ensuring that the world's most security-sensitive organizations can work dynamically, accelerate innovation, and advance zero trust security. It's a simpler, easier, and better way to answer **who**, **what**, **how**, and **why**.

SecurID G&L Cloud provides day-to-day operational and management support of the Cloud hosted solution, freeing up your resources to focus on your core business. Our team of experts let you work smarter by taking responsibility of management tasks of the G&L solution, such as:

- Monitoring, upgrades, maintenance, and patches
- Monitoring of access reviews and collections
- Reporting and dashboards
- Virus scans performance testing, penetration testing
- Resolution of stalled workflows and processes
- Customer success manager, 24/7 Support, Education subscription, and more.

With SecurID G&L Cloud, customers avoid the cost and time of building out their own IT infrastructure to support IGA and save on operational costs through our managed solution. Whether you are new to SecurID Governance and Lifecycle or are considering migrating an on-premise implementation to the cloud, we can help accelerate your digital transformation and deliver a flexible and scalable IGA solution to your business.

To learn more about SecurID Governance and Lifecycle, visit here. To help understand how well you are managing your identity risk, try our IAM Risk Intelligence calculator

Please contact Ms Audrey Ang at audrey.ang@rsa.com if you have any queries.

For more Contributed Contents please visit this link on our website

MEMBERSHIP

Complimentary Affiliate Membership for Full-time Students in APP Organisations

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

Complimentary Affiliate Membership for NTUC Members

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2020 to 2021) from 1 Sept 2020 to 31 Aug 2021. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. This does not include Plus! card holder (black-coloured card), please clarify with NTUC on your eligibility.

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

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

AVIP Membership

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

Your AiSP Membership Account

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

The platform allows our members to sign up for events and voluntary activities, and check membership validity.
Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!

Please check out our website on Job Advertisements by our partners.
For more updates or details about the memberships, please visit www.aisp.sg/membership.html

Be part of the Cybersecurity Ecosystem, JOIN AiSP!

AiSP CORPORATE PARTNERS

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

Visit https://www.aisp.sg/corporate_benefits.html if you wish to join our AiSP Corporate Partners Programme (CPP).

AiSP ACADEMIC PARTNERS

OUR STORY...

www.AiSP.sg
secretariat@aisp.sg
+65 6247 9552
116 Changi Road
#04-03 WIS@Changi
Singapore 419718

Our office is closed. We are currently telecommuting.

Please email us or message us via Telegram at @AiSP_SG

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.

Please contact **secretariat@aisp.sg** on events, membership, partnership, sponsorship, volunteerism or collaboration.

