กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA

AJCCBC
ASEAN JAPAN CYBERSECURITY
CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

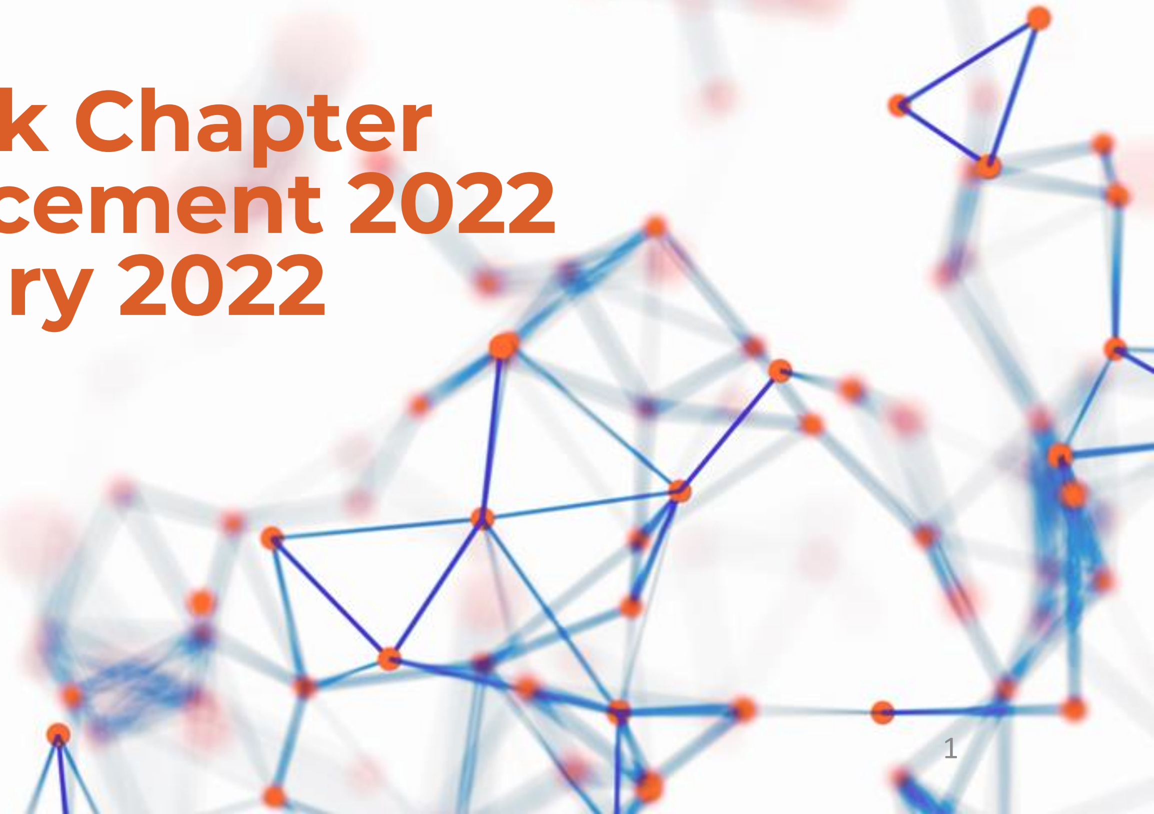
JAIF
Japan-ASEAN Cooperation

MIC
Ministry of Internal Affairs and Communications

OFFICIAL (ISC)² CHAPTER

AJCCBC Project Overview

(ISC)² Bangkok Chapter
Official Announcement 2022
22nd February 2022



What is AJCCBC?

The **9th ASEAN-Japan Information Security Policy Meeting** in 2016 noted that a shortage of cybersecurity professionals will become more serious in the coming years since many organizations and institutions increasingly conduct their communication, processes and businesses on-line, in many cases exclusively. Cyber-attacks have been continuously happening all over the ASEAN region, and the cyber-attack techniques have been advancing rapidly.

Recognising the importance of strengthening cooperation among ASEAN and Japan on cybersecurity development and capacity building initiatives, the 12th ASEAN Telecommunications and Information Technology Ministers Meeting with Japan **(12th TELMIN+Japan)**[1], in Siem Reap, Cambodia, 2017, agreed on the establishment of the **ASEAN-Japan Cybersecurity Capacity Building Centre (the Centre) in Bangkok.**

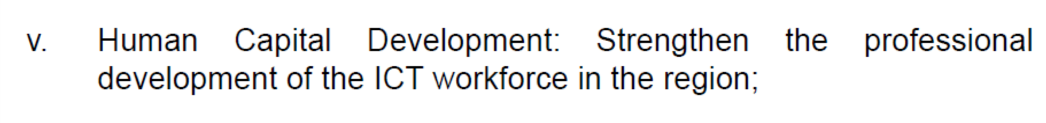
The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) was established under the guidance of TELMIN/SOM in 2018 and funded by Japan ASEAN Integration Fund (JAIF 2.0) for **$5M** to advance the competence of those involved in cybersecurity, particularly from the **governmental agencies** and the **Critical Information Infrastructure** operators. The objective of the Centre is to develop a cybersecurity workforce of **700+** over **4 years** to enhance the capacity of cybersecurity experts and specialists in the AMS by providing them with professional trainings in Incident Response, Malware Analysis and Network Forensics and other relevant activities.

Alignment with Master Plan

AEC Blueprint 2025

AJCCBC contributed to the enhancement of capacity development within ASEAN, which aligned with the AEC Blueprint 2025 in C. Enhanced Connectivity and Sectoral Cooperation
(C.2 Information and Communications Technology)

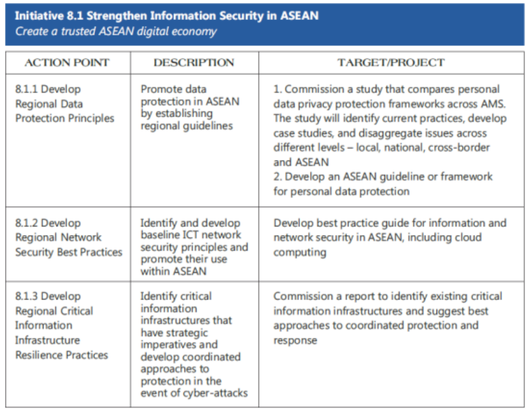
ASEAN
ECONOMIC COMMUNITY
BLUEPRINT 2025


v. Human Capital Development: Strengthen the professional development of the ICT workforce in the region;

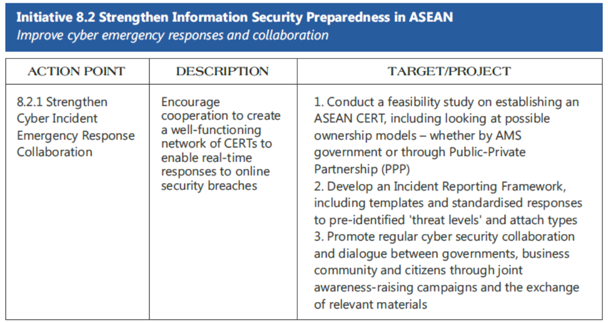
THE ASEAN ICT Masterplan 2020

8. Information Security and Assurance

THE ASEAN ICT
Masterplan 2020

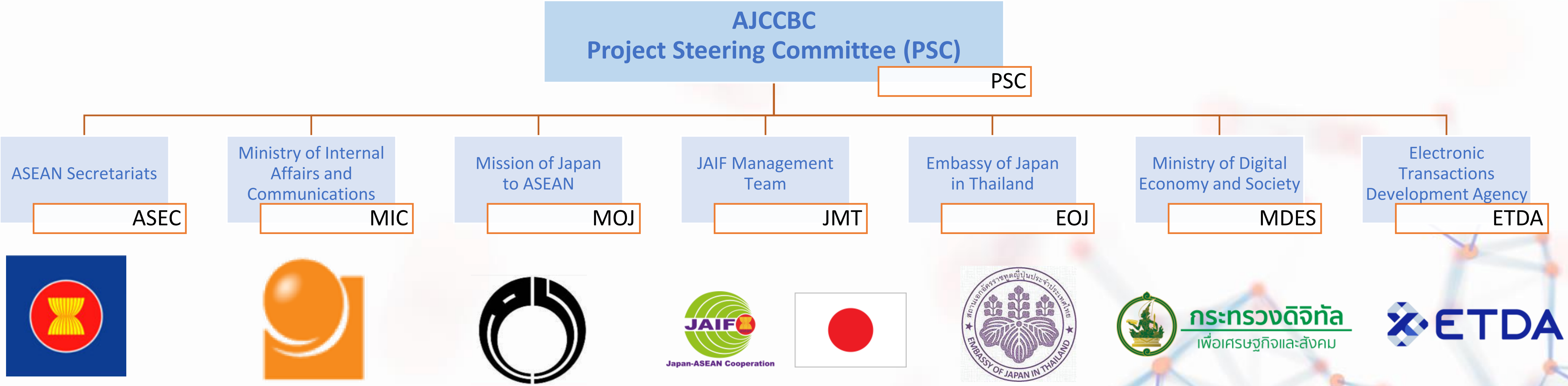

Initiative 8.1 Strengthen Information Security in ASEAN
Create a trusted ASEAN digital economy

ACTION POINT	DESCRIPTION	TARGET/PROJECT
8.1.1 Develop Regional Data Protection Principles	Promote data protection in ASEAN by establishing regional guidelines	1. Commission a study that compares personal data privacy protection frameworks across AMS. The study will identify current practices, develop case studies, and disaggregate issues across different levels – local, national, cross-border and ASEAN 2. Develop an ASEAN guideline or framework for personal data protection
8.1.2 Develop Regional Network Security Best Practices	Identify and develop baseline ICT network security principles and promote their use within ASEAN	Develop best practice guide for information and network security in ASEAN, including cloud computing
8.1.3 Develop Regional Critical Information Infrastructure Resilience Practices	Identify critical information infrastructures that have strategic imperatives and develop coordinated approaches to protection in the event of cyber-attacks	Commission a report to identify existing critical information infrastructures and suggest best approaches to coordinated protection and response


Initiative 8.2 Strengthen Information Security Preparedness in ASEAN
Improve cyber emergency responses and collaboration

ACTION POINT	DESCRIPTION	TARGET/PROJECT
8.2.1 Strengthen Cyber Incident Emergency Response Collaboration	Encourage cooperation to create a well-functioning network of CERTs to enable real-time responses to online security breaches	1. Conduct a feasibility study on establishing an ASEAN CERT, including looking at possible ownership models – whether by AMS government or through Public-Private Partnership (PPP) 2. Develop an Incident Reporting Framework, including templates and standardised responses to pre-identified 'threat levels' and attach types 3. Promote regular cyber security collaboration and dialogue between governments, business community and citizens through joint awareness-raising campaigns and the exchange of relevant materials

AJCCBC’s Relevant stakeholders



AJCCBC
Project Steering Committee (PSC)
PSC

- ASEAN Secretariats — ASEC
- Ministry of Internal Affairs and Communications — MIC
- Mission of Japan to ASEAN — MOJ
- JAIF Management Team — JMT
- Embassy of Japan in Thailand — EOJ
- Ministry of Digital Economy and Society — MDES
- Electronic Transactions Development Agency — ETDA

Center's Facility

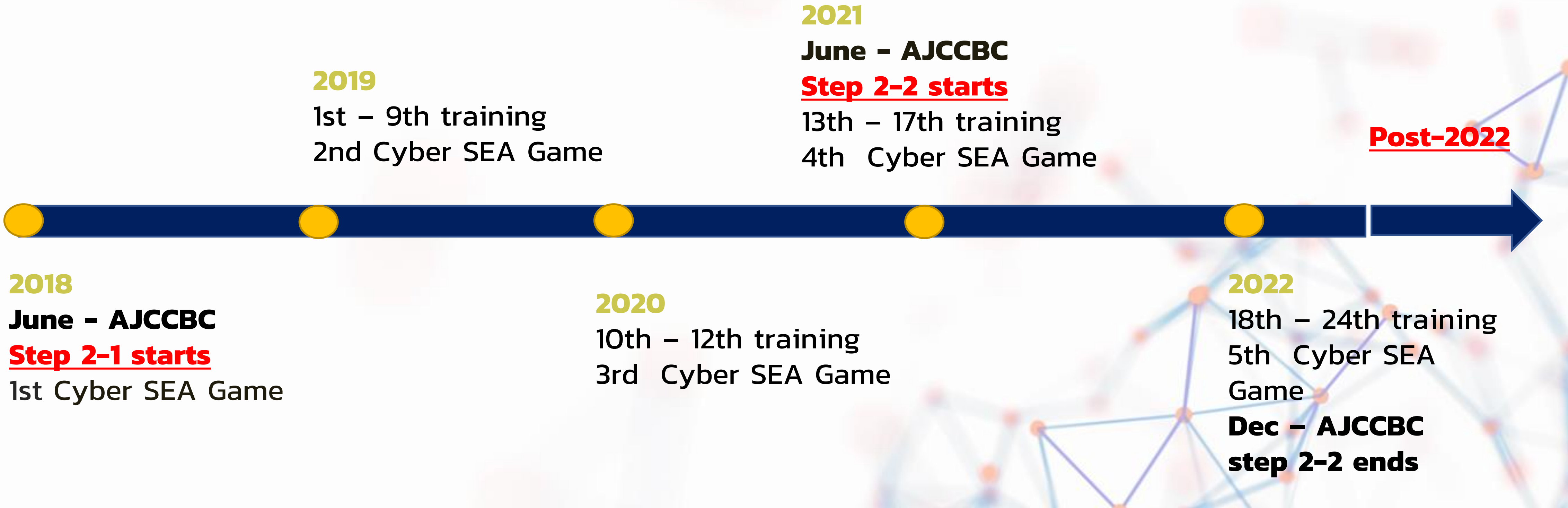
Training facility (Training & Cyber SEA Game)	40 seats
Seminar	60 seats
Co-working Space	30 seats
Computer and peripherals	27 Units
Management Office	10 seats
Server and Cloud services	2 Units

ASEAN-Japan Cybersecurity Capacity Building Centre : AJCCBC
The 9th Tower Grand Rama9 Building (Tower B) Floor 15
33/4 Rama 9 Road, Huai Khwang, Bangkok 10310

AJCCBC Virtual Tour

AJCCBC Timeline

- AJCCBC was established in June 2018 and has accomplished its step 2-1 in June 2021.
- AJCCBC Step 2-2 has been approved in June 2021 and has been operated ever since.
- AJCCBC proposal to extend the operation period beyond 2022 has been approved.



2018
June - AJCCBC
Step 2-1 starts
1st Cyber SEA Game

2019
1st – 9th training
2nd Cyber SEA Game

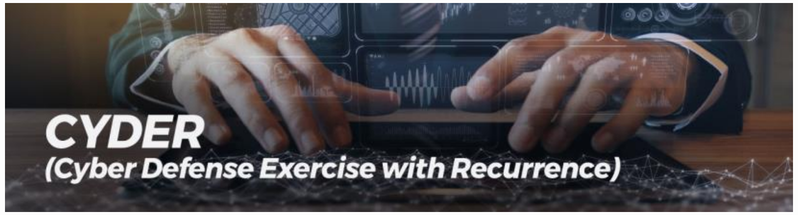
2020
10th – 12th training
3rd Cyber SEA Game

2021
June - AJCCBC
Step 2-2 starts
13th – 17th training
4th Cyber SEA Game

2022
18th – 24th training
5th Cyber SEA Game
Dec – AJCCBC step 2-2 ends

Post-2022

AJCCBC Training Courses



based on "practical cyber defense exercises (CYDER)" carried out in the MIC, Japan which focuses on the improvement of the incident response ability to correspond against the cyberattacks, participants can experience and learn the method of incident handling based on an actual cyberattack.

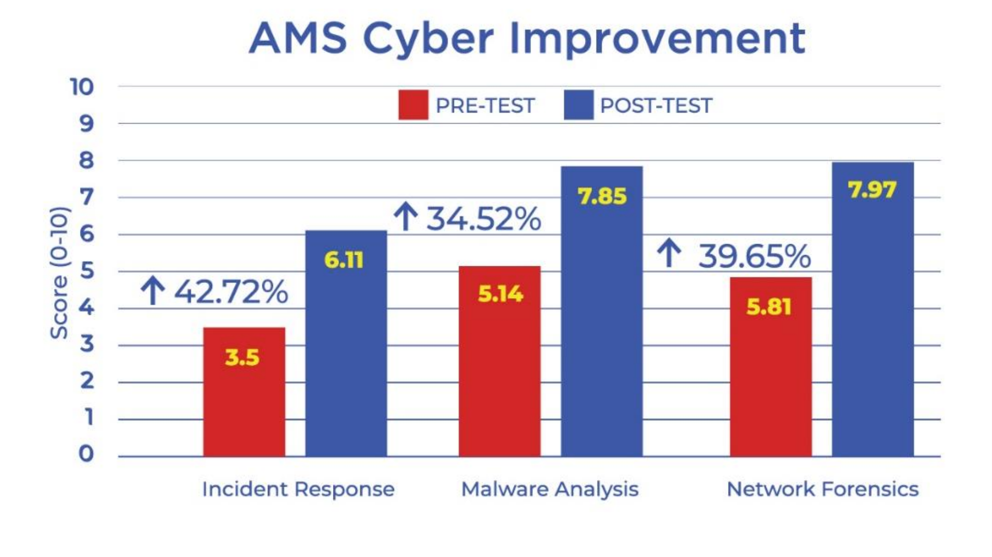
provides the participants key skills in network forensic techniques including how attackers attack servers in DMZ, how attackers attack client's computers etc. which is based on simulation attack.

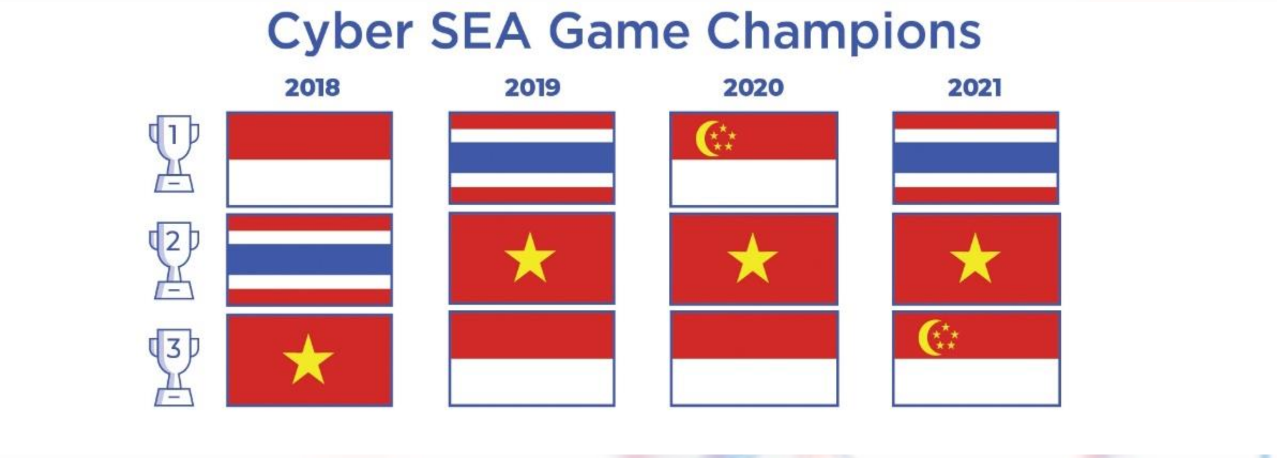
provides you key skills in how to assume the behavior of malware and its impacts by surface analysis, how to identify the behavior of malware and its impact by dynamic analysis, how to identify the actual behavior of malware and its impact by static analysis.

A Technical contest in the form generally called CTF (Capture the Flag), a special kind of cybersecurity competition designed to challenge its participants to solve computer security problems, where young generation of cybersecurity professionals can develop cybersecurity-related skills as well as make connections with each other.

AJCCBC Overall Results (2018 – January 2022)

- The Centre delivered **760** AMS Participants from **18** training sessions (Courses include Incident Response, Malware Analysis, and Network Forensics), **4** Cyber SEA Games, and **2** workshops.





The comparison between pre-test and post-test suggests that the capacity of the personnel was remarkably enhanced:

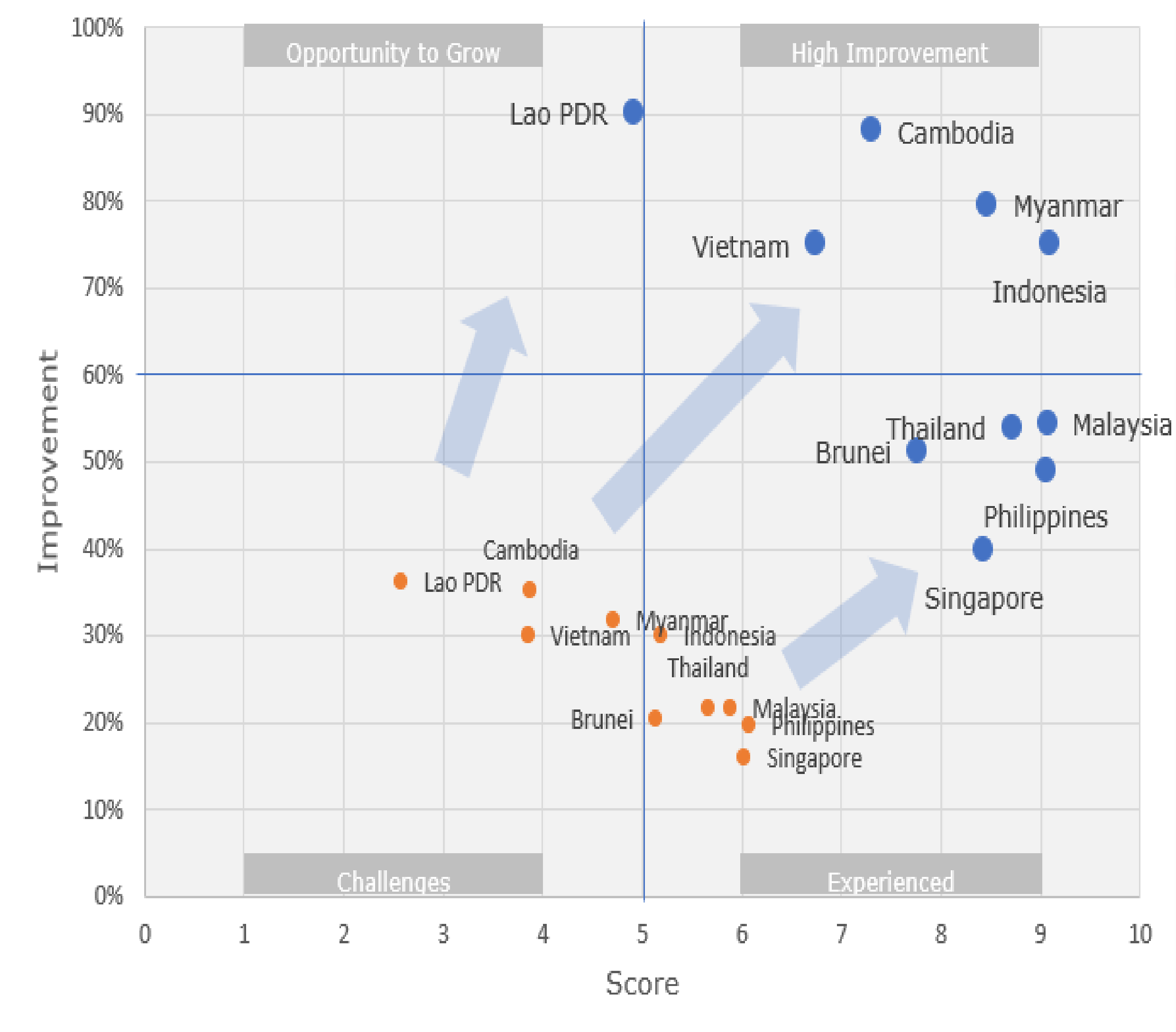
- Incident Response increased from 3.5 to 6.11 out of 10.
- Malware Analysis increased from 5.14 to 7.85 out of 10.
- Network Forensics increased from 4.81 to 7.97 out of 10.

Four Cyber SEA Games were conducted and the winners of each year are:

- 2018: Winner: Indonesia, Runner Up: Thailand, 2nd Runner Up: Vietnam
- 2019: Winner: Thailand, Runner Up: Vietnam, 2nd Runner Up: Indonesia
- 2020: Winner: Singapore, Runner Up: Vietnam, 2nd Runner Up: Indonesia
- 2021: Winner: Thailand, Runner Up: Vietnam, 2nd Runner Up: Singapore

Note: The project duration was extended from 24 months to 36 months. Since some trainings had to be conducted online, the budget for Airfare and Per Diem not utilized in on-site trainings were realigned for system preparation for online trainings.

AJCCBC Overall Results (2018 – January 2022)



Based on the comparison between pre-test and post-test, there are three different groups:

1. The group with the opportunity to grow, including *Lao PDR*.

2. The group with high improvement, including *Cambodia, Myanmar, Vietnam, and Indonesia*.

3. The group with most experiences, including *Brunei, Thailand, Malaysia, Vietnam, Philippines,* and *Singapore.*

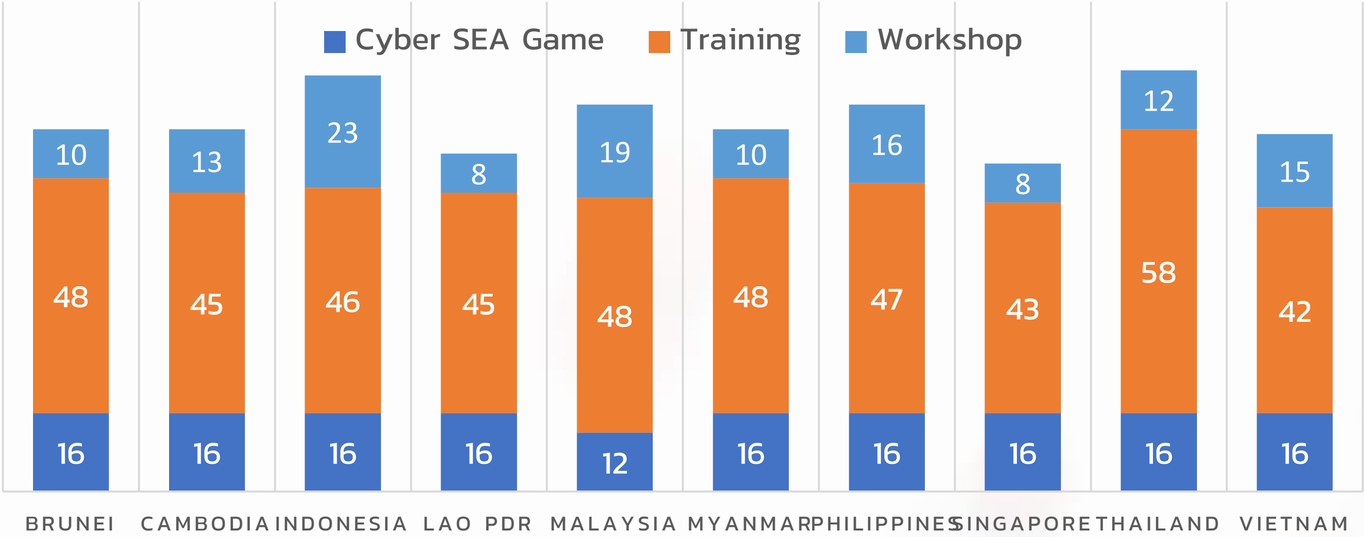
RESULTS

of Participants

Since the project commencement date (June 2018), AJCCBC has trained **760** participants from ASEAN Member States. The participants are government officials and critical information infrastructure operators.

The Centre has now accomplished the objective of training 700 AMS personnel yet will keep providing the trainings for the benefits of the region.

JUNE 2018 – JANUARY 2022



18 Training Sessions **4** Cyber SEA Games **2** Workshops

Participants from AMS
760/700

Training Sessions
18/24

Annual Cyber SEA Games
4/4

Training Sessions

Objectives

- Improve ability and preparedness of network administrators in cybersecurity incident handling training
- Improve ability for undertaking the forensic and malware analysis

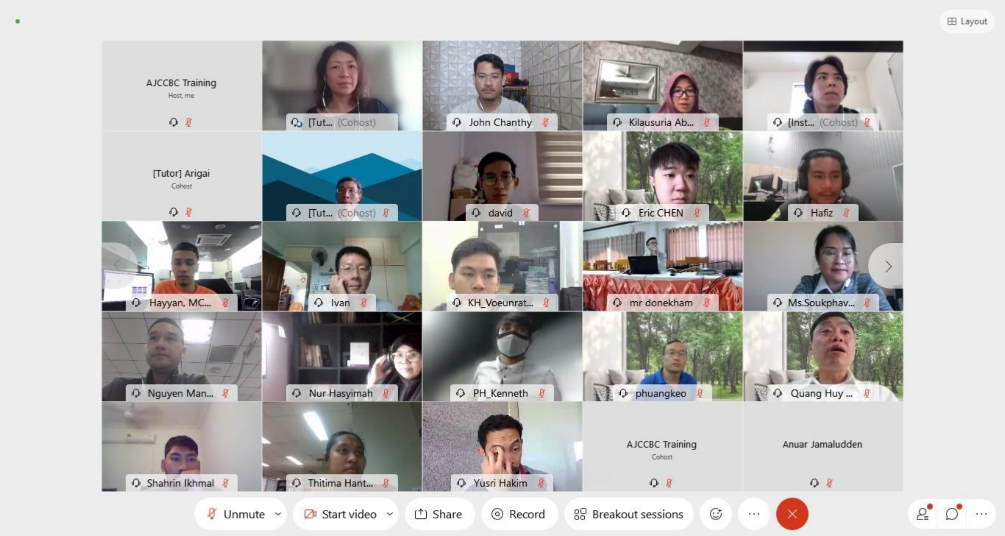
Achieved

AJCCBC successfully conducted 18 training sessions and other related activities to improve capabilities in

(1) cybersecurity incident handling
(2) forensic analysis
(3) malware analysis

for **470** AMS participants.

10th Training (on-site)



14th Training (online)

Cyber SEA Games

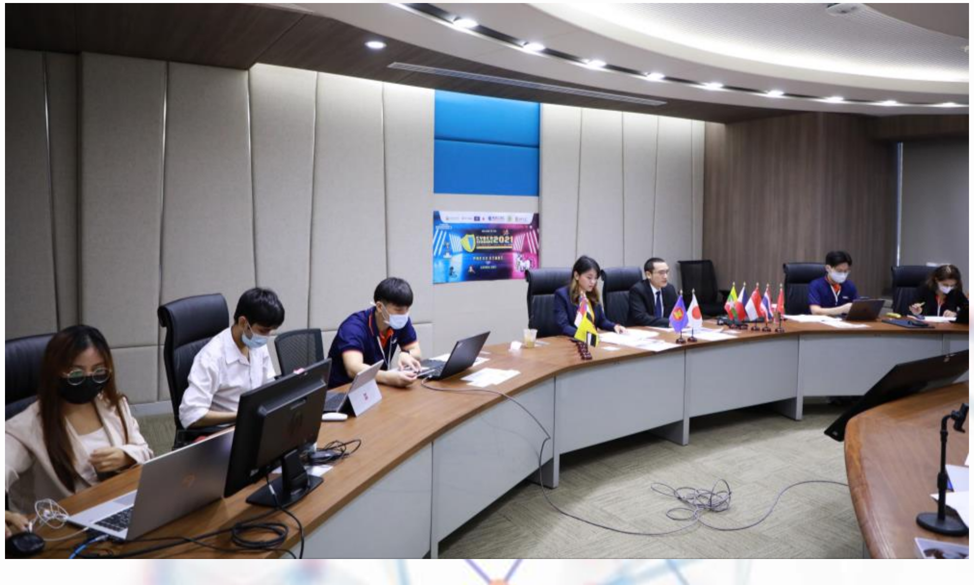
Objective

Raise awareness of the need for expertise, recognition for talents and enhanced knowledge through sharing on cyber security

Achieved

AJCCBC successfully conducted 4 Cyber SEA Games: 2018, 2019, 2020 and 2021 Cyber SEA Games for **156** AMS participants.

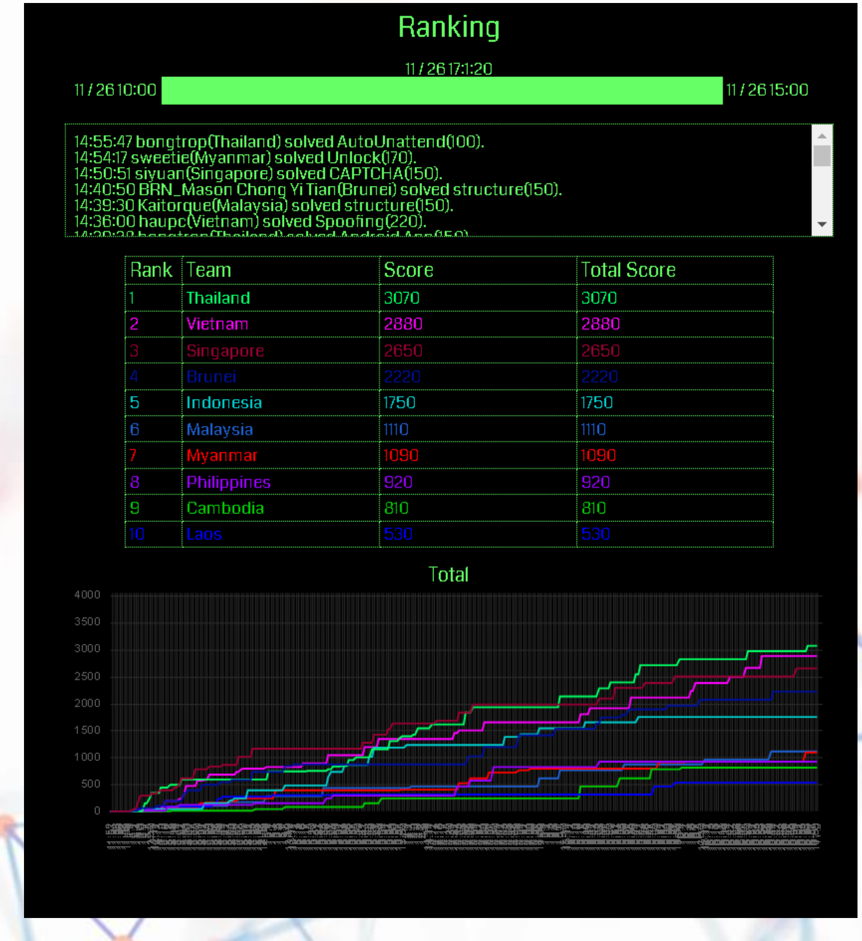
Cyber SEA Game 2019 (on-site)



Cyber SEA Game 2021 (online)

Cyber SEA Games 2021

CYBER SEAGAME 2021
ASEAN | SECURITY CONTEST | CAPTURE-THE-FLAG By AJCCBC
This Project is Supported by Japan-ASEAN Integration Fund (JAIF 2.0)
ETDA
AJCCBC
MIC
1st Award
Thailand


Ranking

11 / 26 17:1:20

11 / 26 10:00 — 11 / 26 15:00

```
14:55:47 bongtrop(Thailand) solved AutoUnattend(100).
14:54:17 sweetie(Myanmar) solved Unlock(170).
14:50:51 siyuan(Singapore) solved CAPTCHA(150).
14:40:50 BRN_Mason Chong Yi Tian(Brunei) solved structure(150).
14:39:30 Kaitorque(Malaysia) solved structure(150).
14:36:00 haupc(Vietnam) solved Spoofing(220).
14:30:38 bongtrop(Thailand) solved Android App(150).
```

Rank	Team	Score	Total Score
1	Thailand	3070	3070
2	Vietnam	2880	2880
3	Singapore	2650	2650
4	Brunei	2220	2220
5	Indonesia	1750	1750
6	Malaysia	1110	1110
7	Myanmar	1090	1090
8	Philippines	920	920
9	Cambodia	810	810
10	Laos	530	530

Total

Participant Engagement Statistic

AJCCBC Online Platform	The Number of Engagement
Alumni list	**800+** Alumni
Alumni's Facebook private group	**159** members
Official Facebook page	**434** likes **479** followers
Official LinkedIn page	**41** followers
Engagement hub	In progress

AJCCBC Activity Update

Project Continuation: Activity Plan 2022

Activity	Expected Period of Activity	Format	Course
Training 18	10 – 14 January 2022	Online	Incident Response & Malware Analysis
Online CTF Course	12 January – 11 March 2022	Self-learning	Cyber Investigations
Exercise For SOC Analysts	7 – 11 February 2022	Online	Security Operation Center
Cybersecurity Awareness Self-learning	15 February 2022	Self-learning	Cyber Awareness
Training 19	21 – 25 February 2022	Online	Incident Response & Network Forensics
Secure Provision	14 – 15 March 2022	Online	Secure Provision (Software Development)
Training 20	25 - 29 April 2022	Online	Incident Response & Malware Analysis
Training 21	13 - 17 June 2022	Online/On-site	Incident Response & Network Forensics
Training 22	1 - 5 August 2022	Online/On-site	Incident Response & Malware Analysis
Training 23	3 - 7 October 2022	On-site	Incident Response & Network Forensics
Cyber SEA Game 2022	10 - 11 November 2022	On-site	Cyber SEA Game
Training 24	19 - 23 December 2022	On-site	Incident Response & Malware Analysis

Note: The on-site activity plan proposed may be changed according to COVID-19 situation.

AJCCBC Post-2022

Project

Project for Enhancing ASEAN-Japan Capacity Building Programme for Cybersecurity and Trusted Digital Services

Objectives

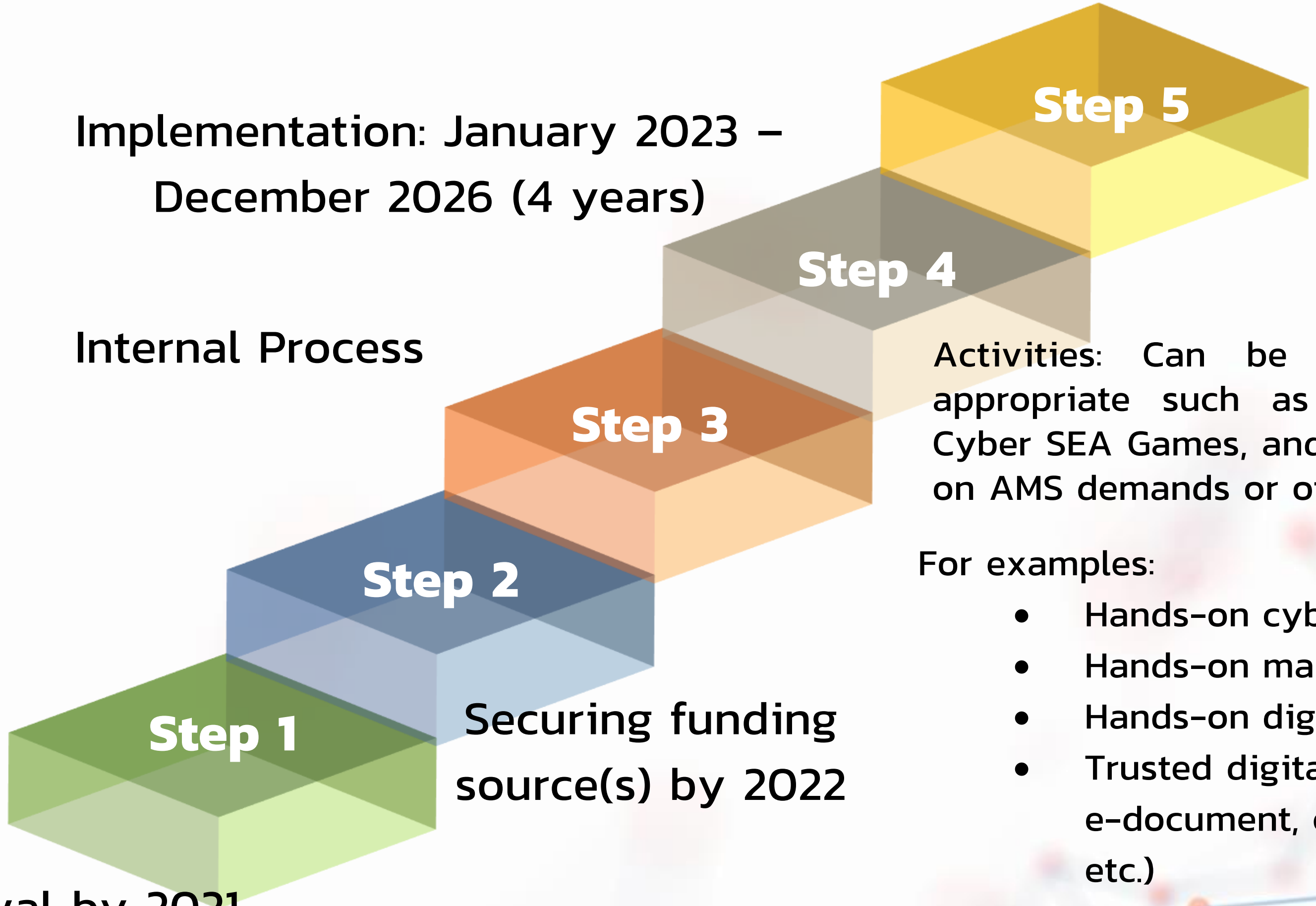
To continue the Centre’s activities, which are built upon the AJCCBC existing project, to provide capacity building programmes at the Centre to fulfil AMS’ training needs and support the desired outcomes of the ADM 2025 through activities such as: on-site or online cyber incident response exercise, malware analysis, digital forensics, and trusted digital services courses, Cyber SEA Games, workshops, conferences, and seminars.

Funding

Estimate USD 5M Under discussion with ASEAN Dialogue Partner-Japan (JICA) and contribution by Thailand

Note” Desired Outcomes (DOs) of the ADM 2025 DO 3: The delivery of trusted digital services and the prevention of consumer harm, DO 6: Digital services to connect business and to facilitate cross-border trade, DO 7: Increased capability for business and people to participate in the digital economy

Post-2022 Project Plan



ASEAN approval by 2021

Securing funding source(s) by 2022

Internal Process

Implementation: January 2023 – December 2026 (4 years)

Ends: January 2027

Activities: Can be arranged on-site or online as appropriate such as regular training courses, annual Cyber SEA Games, and ad-hoc activities or courses based on AMS demands or offered by collaborating partners.

For examples:

- Hands-on cyber incident response exercises
- Hands-on malware analysis courses
- Hands-on digital forensics courses
- Trusted digital services courses (Digital ID, e-signature, e-document, certificate authority, time-stamp service, etc.)
- Cyber SEA Games
- Workshops, conferences, and seminars.
- Others

AJCCBC Third-Party Collaboration

- Swiss Proposal : 2-day intermediate level course on “Secure Provision” (Software Development)

  Organisation
  The University of Applied Sciences and Arts of Southern Switzerland (SUPSI) and In The Cyber Group SA (private sector).

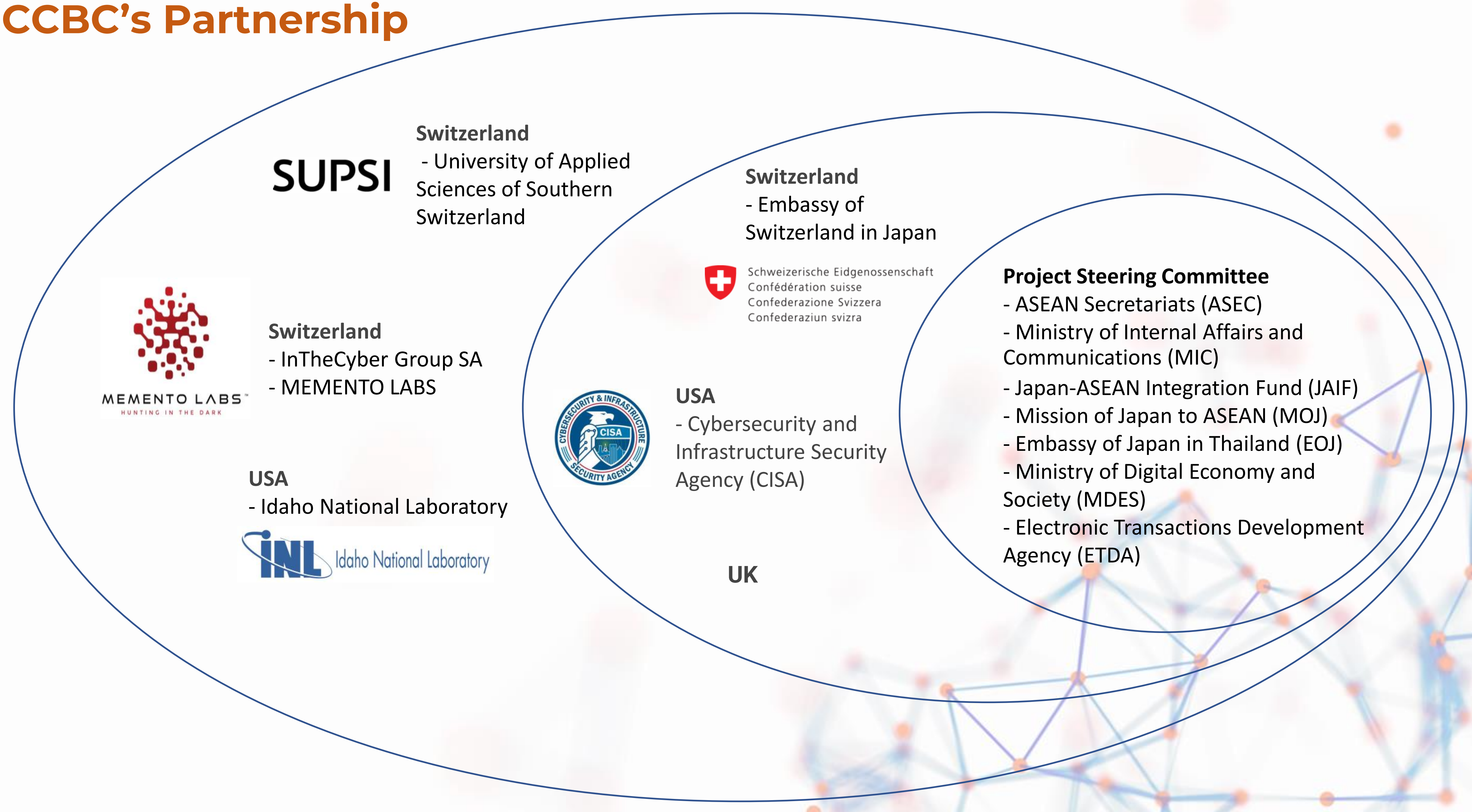
  Purpose
  Secure programming course peculiarity is to provide not only the knowledge of the best practices, instead, it will be shown to attendees the “attacker perspective” against vulnerable applications, providing a unique view on the possible issues and the real associated risk generated by the usage of bad coding practices.

- CISA Proposal : 1.5-day CSET Exercise

  Organisation
  CISA (CYBERSECURITY & INFLUSTRUTURE SECURITY AGENCY) of the USA Department of Homeland Security.

  Purpose
  To provide learners from CII operators with knowledge on how to use CSET tool and how to conduct organization assessment effectively.

AJCCBC’s Partnership



Switzerland
- University of Applied Sciences of Southern Switzerland

Switzerland
- InTheCyber Group SA
- MEMENTO LABS

USA
- Idaho National Laboratory

Switzerland
- Embassy of Switzerland in Japan

USA
- Cybersecurity and Infrastructure Security Agency (CISA)

UK

Project Steering Committee
- ASEAN Secretariats (ASEC)
- Ministry of Internal Affairs and Communications (MIC)
- Japan-ASEAN Integration Fund (JAIF)
- Mission of Japan to ASEAN (MOJ)
- Embassy of Japan in Thailand (EOJ)
- Ministry of Digital Economy and Society (MDES)
- Electronic Transactions Development Agency (ETDA)

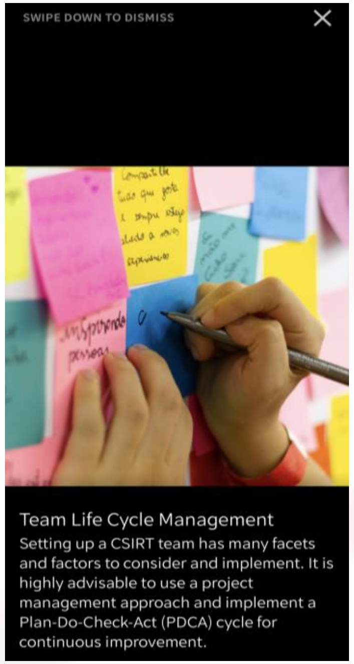
SUPSI
MEMENTO LABS
HUNTING IN THE DARK
INL Idaho National Laboratory
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Updated on 22nd February 2022

AJCCBC Self-Learning Courses

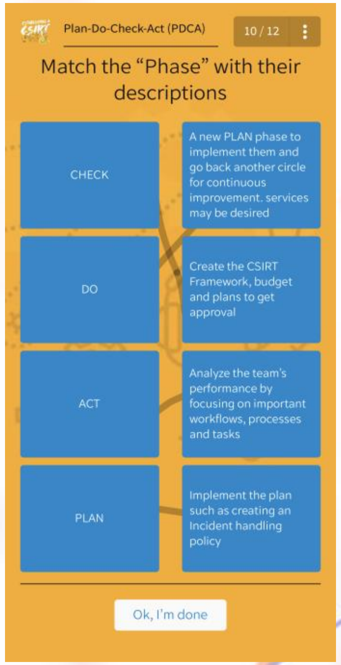
Amidst the pandemic, the Centre decided to leap forward by exploring more into the online world by trialing new formats for learning as micro-learning or self-learning courses, where the participants can learn anywhere and anytime at their convenience through a platform called EdApp.

- Course Title: 1.) Establishing a CSIRT 2.) Cybersecurity Awareness
- Format: Online self-learning course on **EdApp**
- Learning Period: Available until 18th April 2022.
- Price: free-of-charge, supported by ETDA



Team Life Cycle Management

Setting up a CSIRT team has many facets and factors to consider and implement. It is highly advisable to use a project management approach and implement a Plan-Do-Check-Act (PDCA) cycle for continuous improvement.



Match the "Phase" with their descriptions

CHECK

A new PLAN phase to implement them and go back another circle for continuous improvement. services may be desired

DO

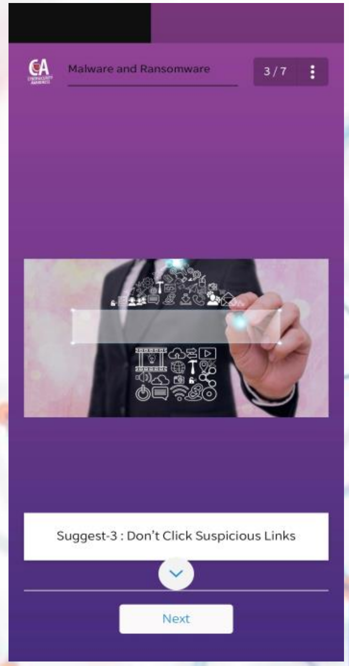
Create the CSIRT Framework, budget and plans to get approval

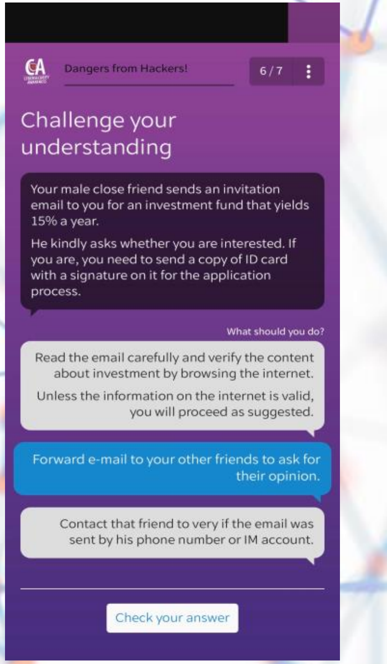
ACT

Analyze the team's performance by focusing on important workflows, processes and tasks

PLAN

Implement the plan such as creating an Incident handling policy





Challenge your understanding

Your male close friend sends an invitation email to you for an investment fund that yields 15% a year.

He kindly asks whether you are interested. If you are, you need to send a copy of ID card with a signature on it for the application process.

What should you do?

Read the email carefully and verify the content about investment by browsing the internet.

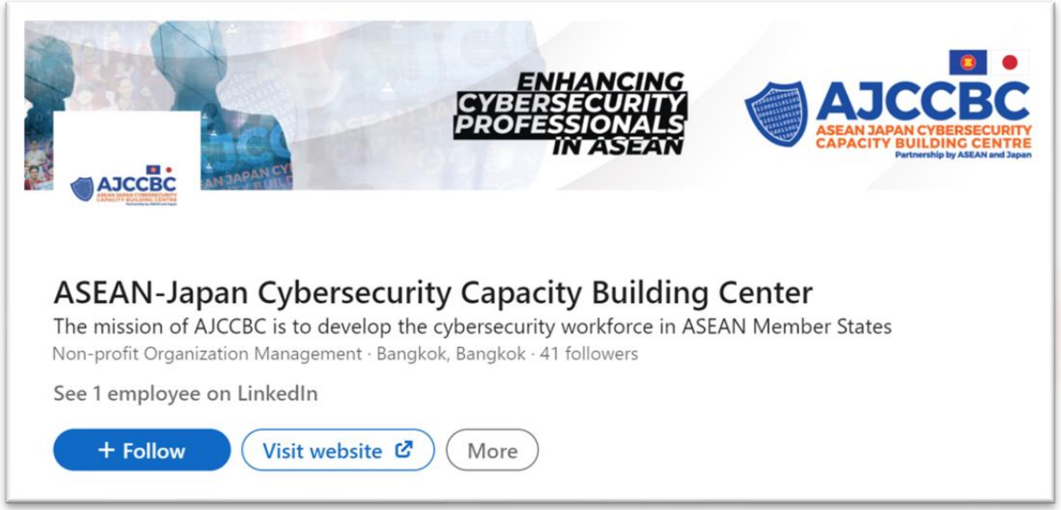
Unless the information on the internet is valid, you will proceed as suggested.

Forward e-mail to your other friends to ask for their opinion.

Contact that friend to very if the email was sent by his phone number or IM account.

https://go.ajccbc.org/cyberawareness

AJCCBC Social Networks & Promotional Video



ENHANCING CYBERSECURITY PROFESSIONALS IN ASEAN
AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

ASEAN-Japan Cybersecurity Capacity Building Center

The mission of AJCCBC is to develop the cybersecurity workforce in ASEAN Member States

Non-profit Organization Management · Bangkok, Bangkok · 41 followers

See 1 employee on LinkedIn

+ Follow
Visit website
More

LinkedIn Page

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan
Send message

ASEAN-Japan Cybersecurity Capacity Building Centre

@AJCCBC · Public & Government Service

Facebook Page

International Publication: Global Cyber Expertise Magazine Issue 10

The Global Cyber Expertise Magazine is a bi-annual magazine on global cyber policy developments and capacity building projects. The Magazine is jointly published by the African Union, the European Union, the Global Forum on Cyber Expertise (GFCE) and the Organization of American States.

AJCCBC, as a member of the **Global Forum on Cyber Expertise (GFCE)**, has submitted an article to obtain more recognition in Issue 10 of Global Cyber Expertise Magazine On Cybil online platform. The article was published in November 2021.

INTRODUCING THE ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE (AJCCBC)

ISACA Journal Vol.3

ISACA is the Journal that provides important information on industry advancements and professional development to those involved in the IS audit, information security and governance communities.

The Centre has submitted an article on **ASEAN Region's Resilience in Capacity Building**, pertaining **project background** and **programme development through the pandemic with resilience** to be published in the ISACA Journal Vol 3 in May/June 2022. The article is now going through second peer review process after it was initially review recently.

List of References

ONLINE SOURCES

www.ajccbc.org

AJCCBC Official Website

AJCCBC Facebook Page

AJCCBC LinkedIn Page

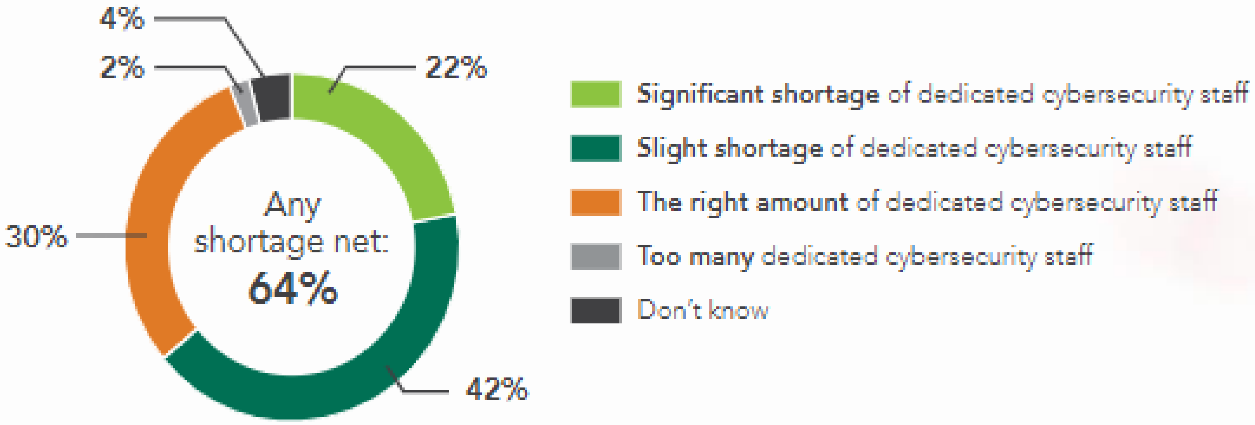
AJCCBC Facebook Group Member

Alumni's Closed group

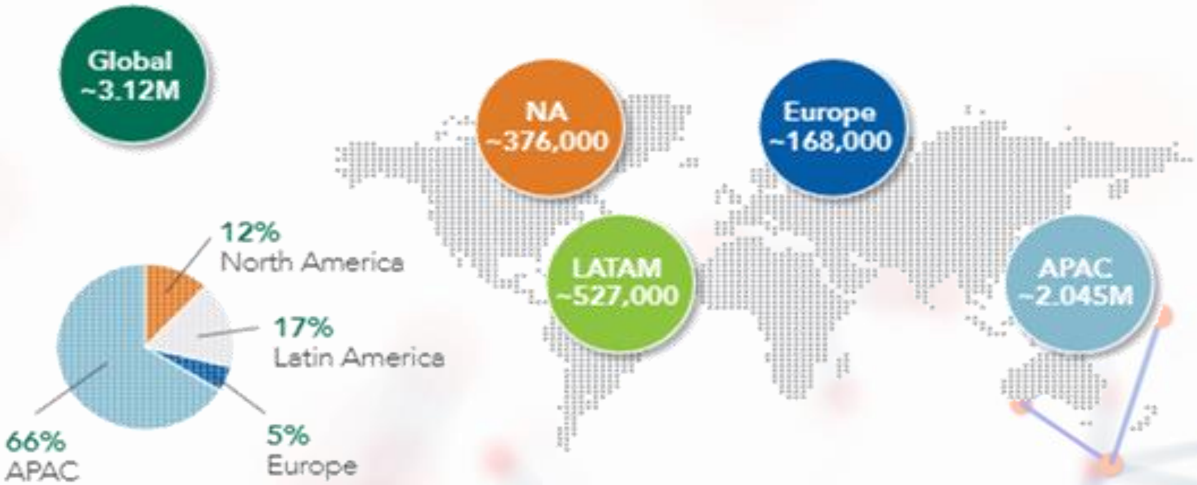
AJCCBC Engagement Hub

AJCCBC Activities and Documents Archive

The Cybersecurity Workforce Gap by Region



The global gap in the cybersecurity workforce varies by region, dominated by a gap of more than 2 million in the Asia-Pacific region.



A cybersecurity workforce shortage has become a major issue around the world as indicated in the **ISC2 Workforce Study 2020**. The study suggested **that 64%** of organizations have encountered or are on the verge of encountering cybersecurity staff shortage while cyber threats have been advancing and have become unavoidable.

The study suggested **that Asia-Pacific region** has a cybersecurity workforce gap of more than **2.045** million, being the widest gap compared to other regions worldwide.

Reference: (ISC)^2 CYBERSECURITY WORKFORCE STUDY, 2020