The Pilot Partnership Programme for Cyber Security Information Sharing
網絡安全資訊共享夥伴試驗計劃

Cybersec Infohub

Mr. Jason PUN

Assistant Government Chief Information Officer
Cyber Security & Digital Identity
12 June 2018

Cybersec Infohub

Cyber security information to be shared

Threat information and analysis

Security alerts, news, vulnerabilities

Mitigation advisories

Situational awareness

Best practices and tips

Strategic analysis

Key participants

- ISPs
- Critical Infrastructure
- Critical Internet Infrastructure
- IT & Security Vendors
- Researcher
- GovCERT.HK HKCERT Local CERTs

Methods of Exchange

- Via the Platform
- Industry Event
- Tele-conference
- Webinar
- Working Group

Programme Objectives

Establish a cross-sector, trusted collaborative network to share cyber security information

Provide a collaborative platform for sharing information, to give a better visibility of cyber security situational awareness

Cultivate local collaborative culture among the industry for effective cyber security information sharing

To enhance the cyber resilience of Hong Kong against territory-wide cyber attacks

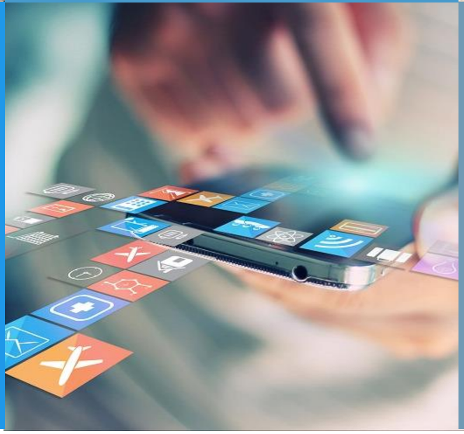
Sharing Model

Any Member of the Programme interact and share with any other Members

Involve social media and collaboration elements

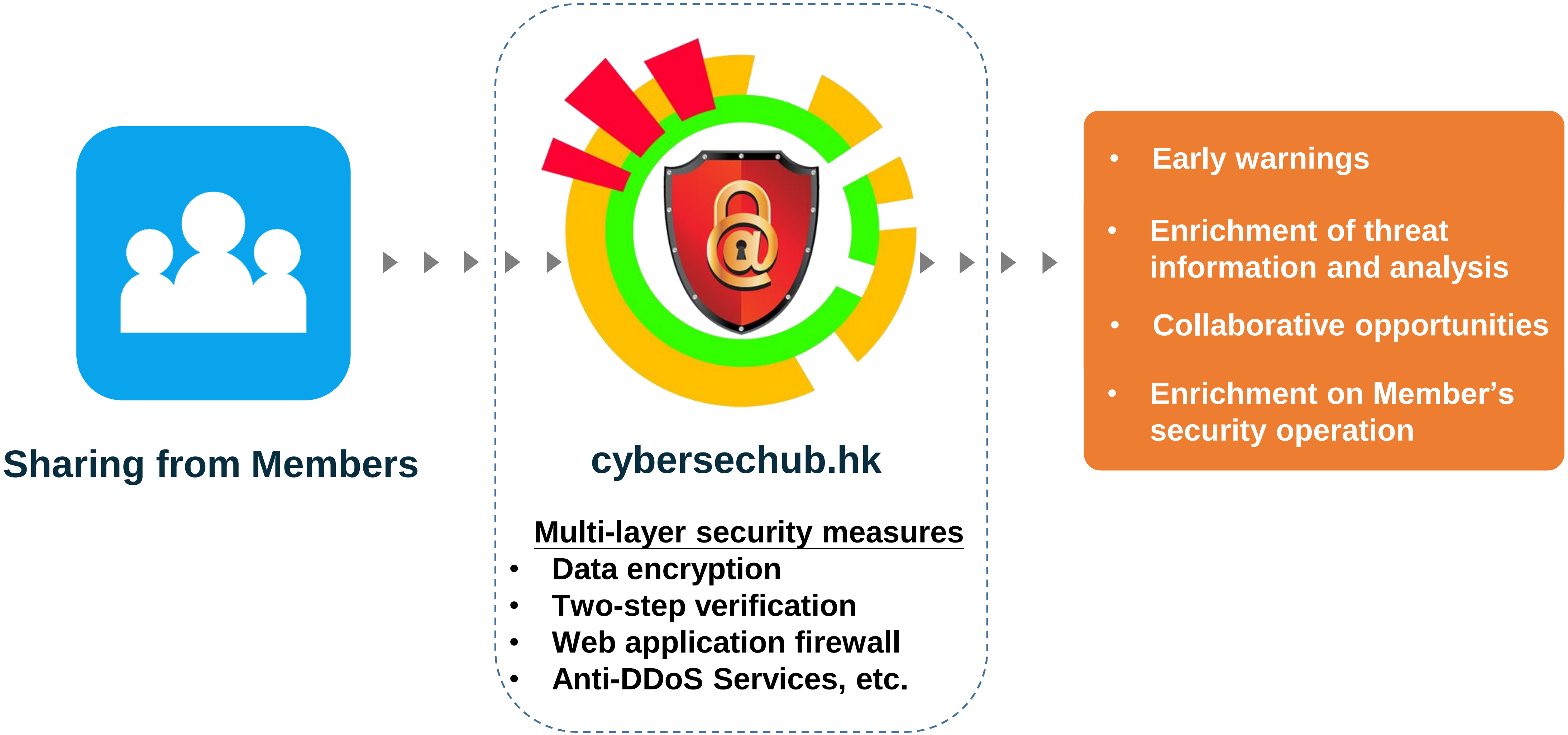
Trusted circles - based on trust and common interests for sharing of valuable / actionable information

Members-driven, sharing when, what, and with whom as Members see fit



No “gatekeeper” governing how, when and what sharing occurs,
incl. event-based sharing

Sharing via cybersechub.hk



Sharing from Members

cybersechub.hk

Multi-layer security measures

- Data encryption
- Two-step verification
- Web application firewall
- Anti-DDoS Services, etc.

- Early warnings
- Enrichment of threat information and analysis
- Collaborative opportunities
- Enrichment on Member’s security operation

Data Protection

Comply with Government IT security policy and guidelines

Regular security risk assessment and audit

Data centre certified w/ ISO 9001 & ISO/IEC 27001

Data centre located in Hong Kong

Membership

JOIN

Any Hong Kong company or organisation with its business address in Hong Kong, which manage an electronic communications network and has operational needs for cyber security information, is eligible to become a **Member** provided that it confirms that it complies and is willing to continue to comply with the terms and conditions of the Programme.

The Programme Management Committee (OGCIO and HKPC) reserves the right to determine the Membership and the maximum number of Representatives for Members according to operation of the Programme.

Members' Responsibilities

Information Sharing Boundary

- Use Traffic Light Protocol (TLP)

TLP: RED

TLP: AMBER

TLP: GREEN

TLP: WHITE

Handling Confidentiality

- Use the information for the Programme objectives
- Ensure the information sharing comply with TLP
- Due diligence to take care the confidentiality

Handling Malicious Content

- Do not upload malware samples to the Platform
- Use masked URL, such as replacing "http" with "hxxp" and "." with "[.]"

Unintended Disclosure

- Notify the Originator of any unintended disclosure

TLP for Information Sharing

Forum of Incident Response and Security Teams (FIRST) Traffic Light Protocol (TLP) V1.0			
TLP: RED	Not for disclosure, restricted to recipients only	TLP: AMBER	Limited disclosure, restricted to recipients’ organisations
TLP: GREEN	Limited disclosure, restricted to relevant community on the platform	TLP: WHITE	Disclosure is not limited

Members’ Responsibilities (Cont’d)

1 Members shall strictly follow the terms and conditions of the Programme.

2 Supply and receipt of Information through the Programme shall comply with any applicable legal obligation.

3 Information shared in the Programme is provided “as-is”; The Originator shall not be liable for any errors or omissions in the information and shall not be liable for any loss, injury or damage of any kind arising from or in connection with its use to the extent permitted by law.

Advisory Group

Multi-stakeholder model

Contribute useful cyber security operational advice

Collect inputs from wider community on the strategy and priority of the Programme

Advisory Group

Composition

Member can nominate representative to join

Confidentiality

Advisory group members shall safeguard the entrusted information and discussions

Roles and Responsibilities

Advise on:

- the model, mechanism and methodology of information sharing;
- advanced technologies to be adopted; and
- any other areas contributing to the effective and secure information sharing for the Programme

Latest Development of the Programme

HKPC
Hong Kong Productivity Council
香港生產力促進局
QUANN
THE ART AND SCIENCE OF BEING CYBER SECURE
ADVSTAR
LABORATORY
MASTER
CONCEPT

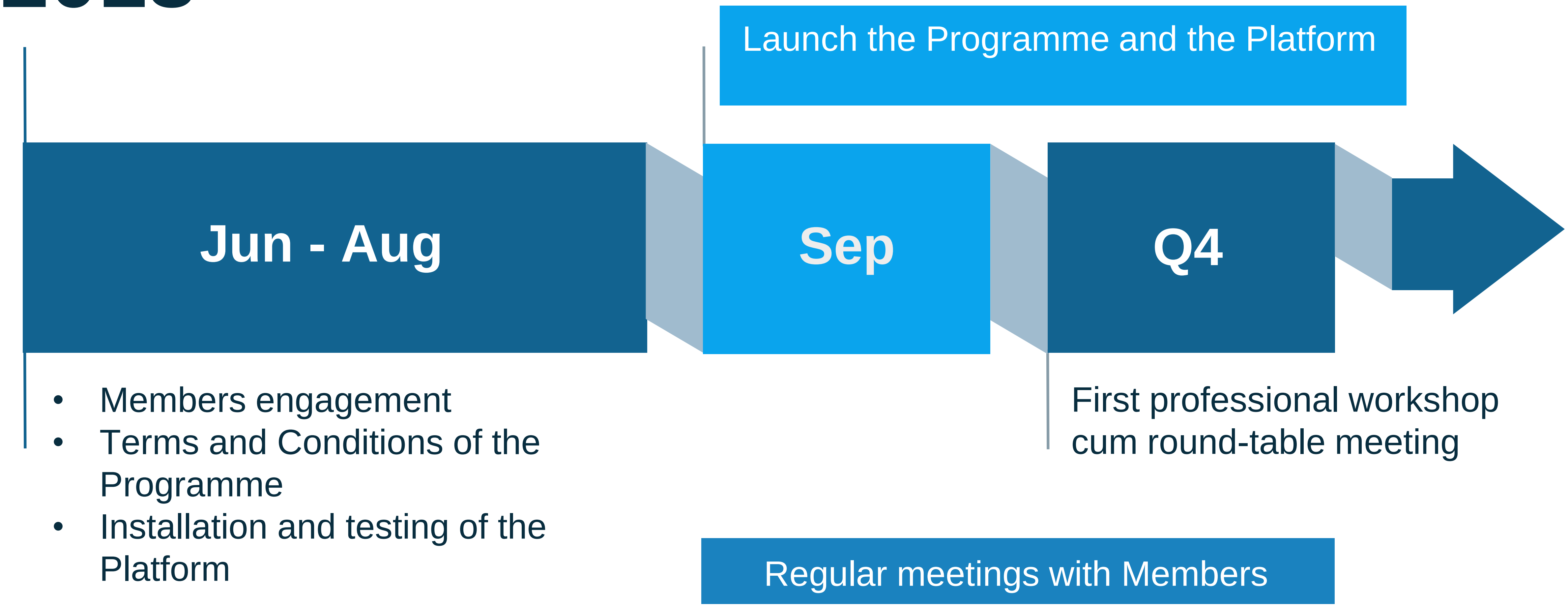
Consultancy services and total programme management for devising information sharing model, T&C of the Programme and ToR of Advisory Group

Information sharing and collaboration platform services – “cybersechub.hk”

Hosting and security monitoring services

Programme Timeline

2018



Launch the Programme and the Platform

Jun - Aug

Sep

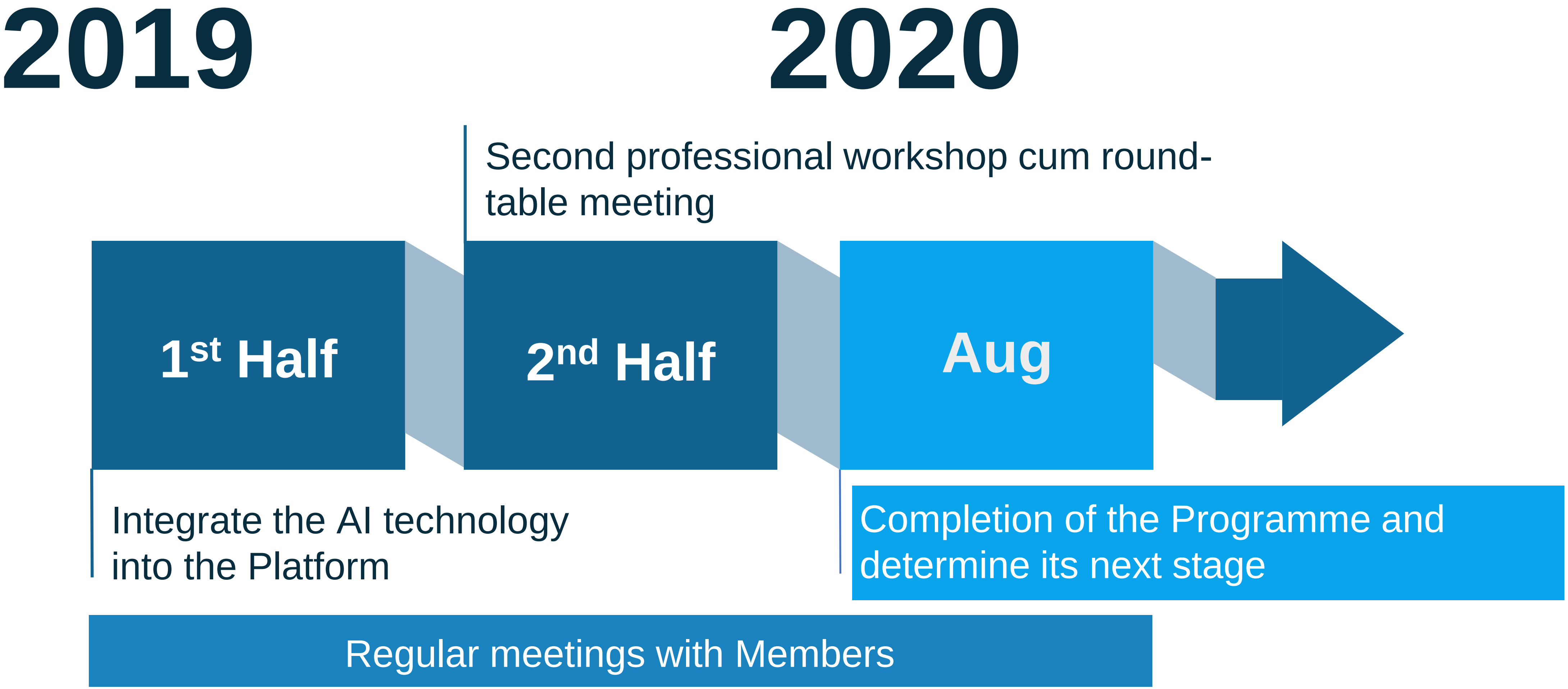
Q4

- Members engagement
- Terms and Conditions of the Programme
- Installation and testing of the Platform

First professional workshop cum round-table meeting

Regular meetings with Members

Programme Timeline (Con’t)



2019

2020

Second professional workshop cum round-table meeting

1st Half

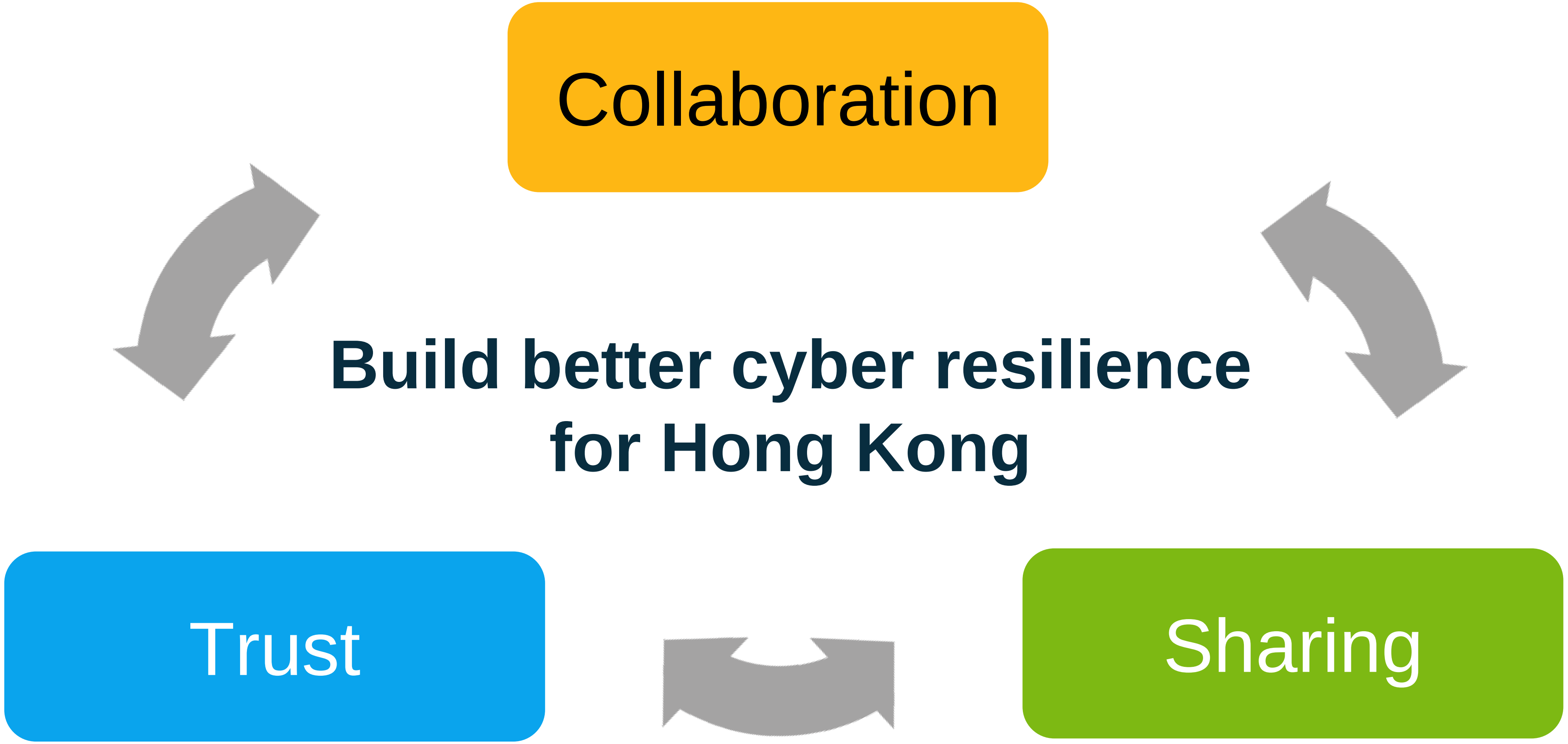
2nd Half

Aug

Integrate the AI technology into the Platform

Completion of the Programme and determine its next stage

Regular meetings with Members



Collaboration

Build better cyber resilience for Hong Kong

Trust

Sharing

Thank You