

網絡安全資訊共享夥伴試驗計劃

The Pilot Partnership Programme for Cyber Security Information Sharing



Cybersec Infohub

Mr Nicky YICK

Senior Systems Manager (Cyber Security)

Office of the Government Chief Information Officer



Cybersec Infohub

A new government initiative to promote closer collaboration among local information security stakeholders of different sectors (a 2-year pilot programme)

Why we have such initiative?

Cyber attacks continue to increase in frequency and sophistication

Difficult for individual organisation to scout the Internet continuously and to guard against cyber threats

Challenges for organisations to protect their digital assets

Sharing information and early warnings can help mitigate risks

Programme Objectives

Establish a cross-sector collaborative network

Cultivate local collaborative culture



Provide a collaborative platform for a better visibility of situational awareness

Enhance the overall cyber resilience of Hong Kong

Core Principles

Collaboration

Trust

Sharing



Cybersec Infohub



Key participants



ISPs



Critical Infrastructure



Critical Internet Infrastructure



IT & Security Vendors



Researcher

GovCERT.HK



Local CERTs



Other Sectors

Sharing Model

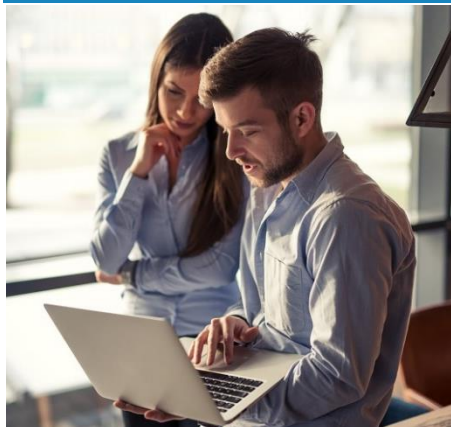
Any Member of the Programme interact and share with any other Members



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



Membership



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.

Advisory Group

Multi-stakeholder model



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

Contribute useful cyber security operational advice

Cybersechub.hk - Public Zone

Highlights

<p>CERT Publications</p> <p>Cyber Security Threat Trends 2018-M12</p> <p>GovCERT.HK keeps observing the cyber security threat trends and shares some observations in December 2018...</p> <p>GovCERT.HK 10 Jan 2019, 10:59 (HKT) #IoT Security #Trends #Information Leakage #Unauthorised Access</p>	<p>Insights</p> <p>Emotet Malware Spreading Via IRS Theme Based Spam Email</p> <p>SonicWall RTDMI engine detected an archive attachment consisting of malicious word documents inside...</p> <p>Eric MOY Cyber Range Training Centre Limited 28 Dec 2018, 15:09 (HKT) #Malware</p>	<p>CERT Publications</p> <p>Analysis Report (AR18-352A) - Quasar Open-Source Remote Administration Tool</p> <p>Quasar, a legitimate open-source remote administration tool (RAT), has been observed being used maliciously...</p> <p>US-CERT 19 Dec 2018, 12:37 (HKT) #Analysis #APT #Hacker Tools</p>
<p>Insights</p> <p>Extortion Email Alert</p> <p>Recently, HKCERT received a number of reports from students and alumni of a local university who received...</p> <p>Herman LEI HKCERT 12 Dec 2018, 18:07 (HKT)</p>	<p>Insights</p> <p>US Congressional Report Of Equifax's Mega Hack</p> <p>Equifax is one of several large Consumer Reporting Agencies (CRA) in the United States. CRAs gather consumer...</p> <p>Bernard KAN HKCERT 12 Dec 2018, 12:32 (HKT) #Information Leakage #Analysis</p>	<p>CERT Publications</p> <p>Cyber Security Threat Trends 2018-M11</p> <p>GovCERT.HK keeps observing the cyber security threat trends and shares some observations in November 2018...</p> <p>GovCERT.HK 05 Dec 2018, 17:30 (HKT) #Cryptomining #Information Leakage #Malware #Phishing #Ranso...</p>
<p>CERT Publications</p> <p>Activity Alert AA18-337A: SamSam Ransomware</p> <p>The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center...</p>	<p>Insights</p> <p>Cybersecurity Alert For SMEs In Hong Kong</p> <p>Cybersecurity Alert Many SMEs in Hong Kong are having their IT support outsourced to external IT service...</p>	<p>CERT Publications</p> <p>Technical Alert TA18-331A: 3ve - Major Online Ad Fraud Operation</p> <p>This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security...</p>

Alerts

- 17 Jan CVE-2018-18814 - The TIBCO Spotfire authentication component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Plat...
- 17 Jan CVE-2018-18812 - The Spotfire Library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS M...
- 17 Jan CVE-2018-5741 - To provide fine-grained controls over the ability to use Dynamic DNS (DDNS) to update records in a ...
- 17 Jan CVE-2018-5740 - "deny-answer-aliases" is a little-used feature intended to help recursive server operators protect ...
- 17 Jan CVE-2018-5739 - An extension to hooks capabilities which debuted in Kea 1.4.0 introduced a memory leak for operator...
...more

Tags

Analysis, Trends, Malware, Ransomware, APT, Information Leakage, Phishing, Vulnerability, Hacker Tools, IoT Security, Cryptomining, Exploit, Web Security, Botnet, Threat Intel

Events



"Cyber Security for Healthcare"
Seminar
21 January 2019

Alerts

Advisories

CERT Publications

Insights

Cybersechub.hk - Member Zone

Traffic Light Protocol

“KOL” of Cybersechub.hk

Trusted Groups Discussion

User Anonymity

Directory for Connections

Private Messaging

Export IOCs for Operation

Social Media “Like” Feature

Industry Best Practices

Use Traffic Light Protocol (TLP)

TLP: RED

TLP: AMBER

TLP: GREEN

TLP: WHITE

Structured Threat Information eXpression (STIX)

Trusted Automated eXchange of Intelligence Information (TAXII)

Data encryption, Two-step verification, WAF, Anti-DDoS

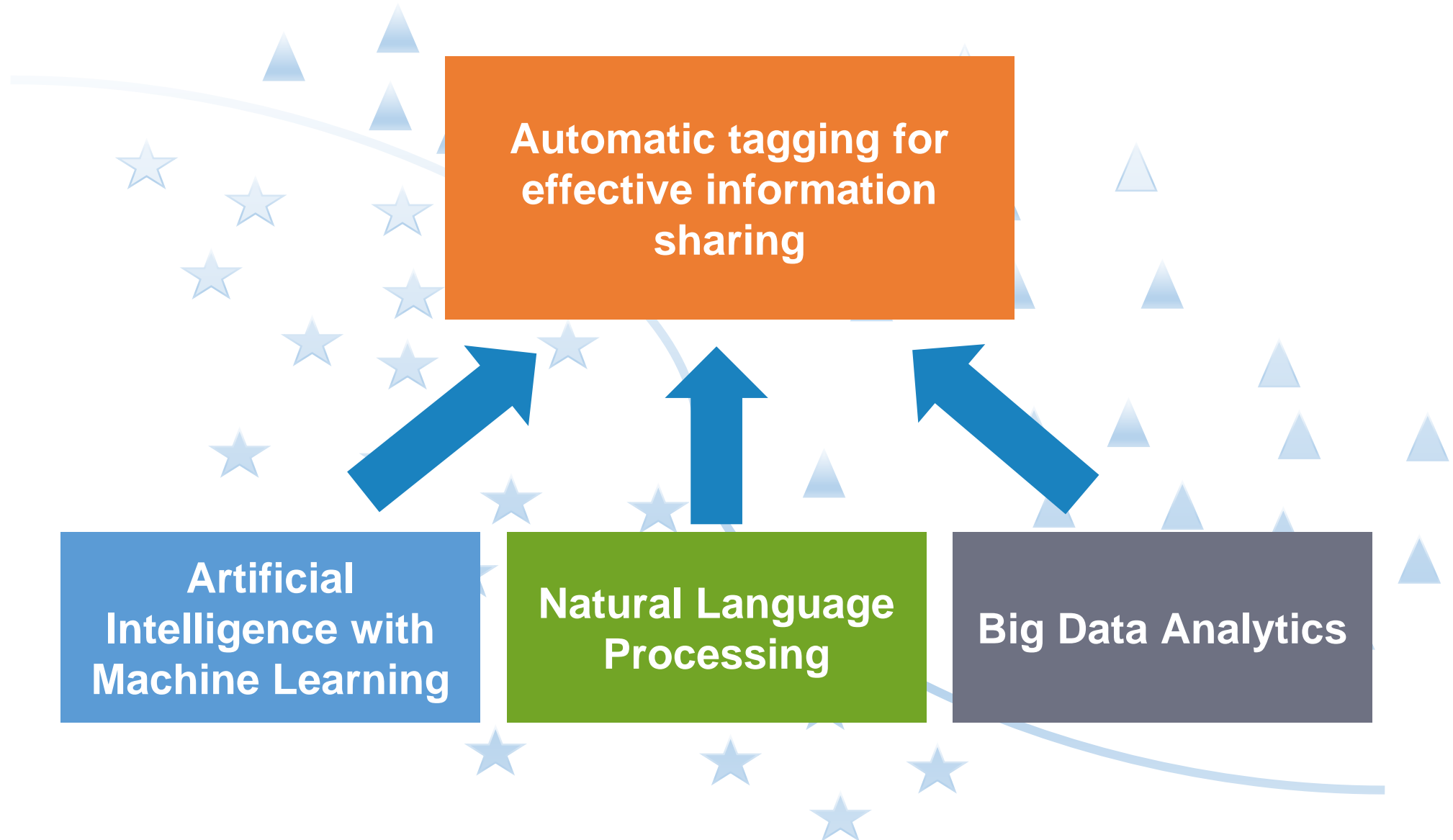
Comply with Government IT security policy and guidelines

Information sharing boundary

Information exchange

Security

Advanced Technologies

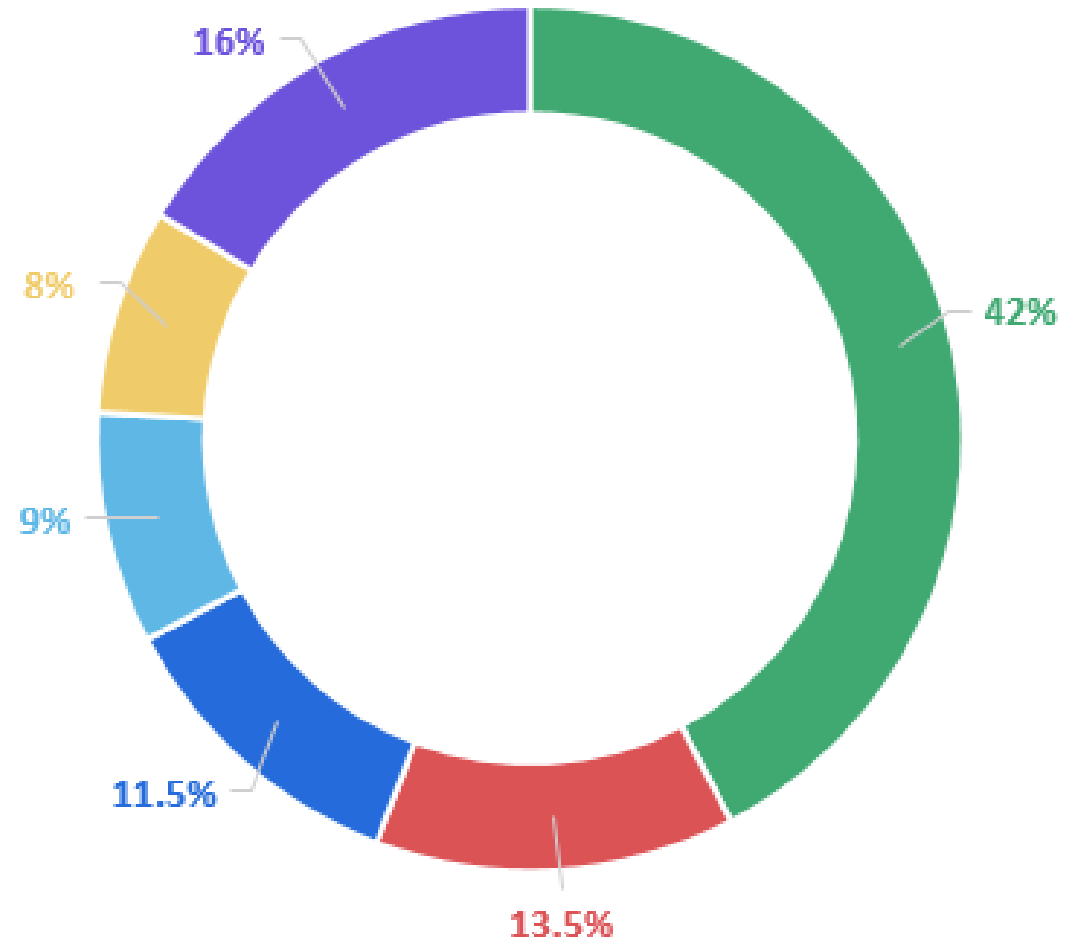


Members Information

As at
Dec 2018

Over
100
Member
Organisations

More than
300
Representatives



● Innovation & Technology ● Finance & Insurance ● Education ● Non-Profit Organisation ● Telecommunications ● Others

Latest Development



Discussions on major incidents



Monthly active contributors



2 closed groups created



Enhanced notification

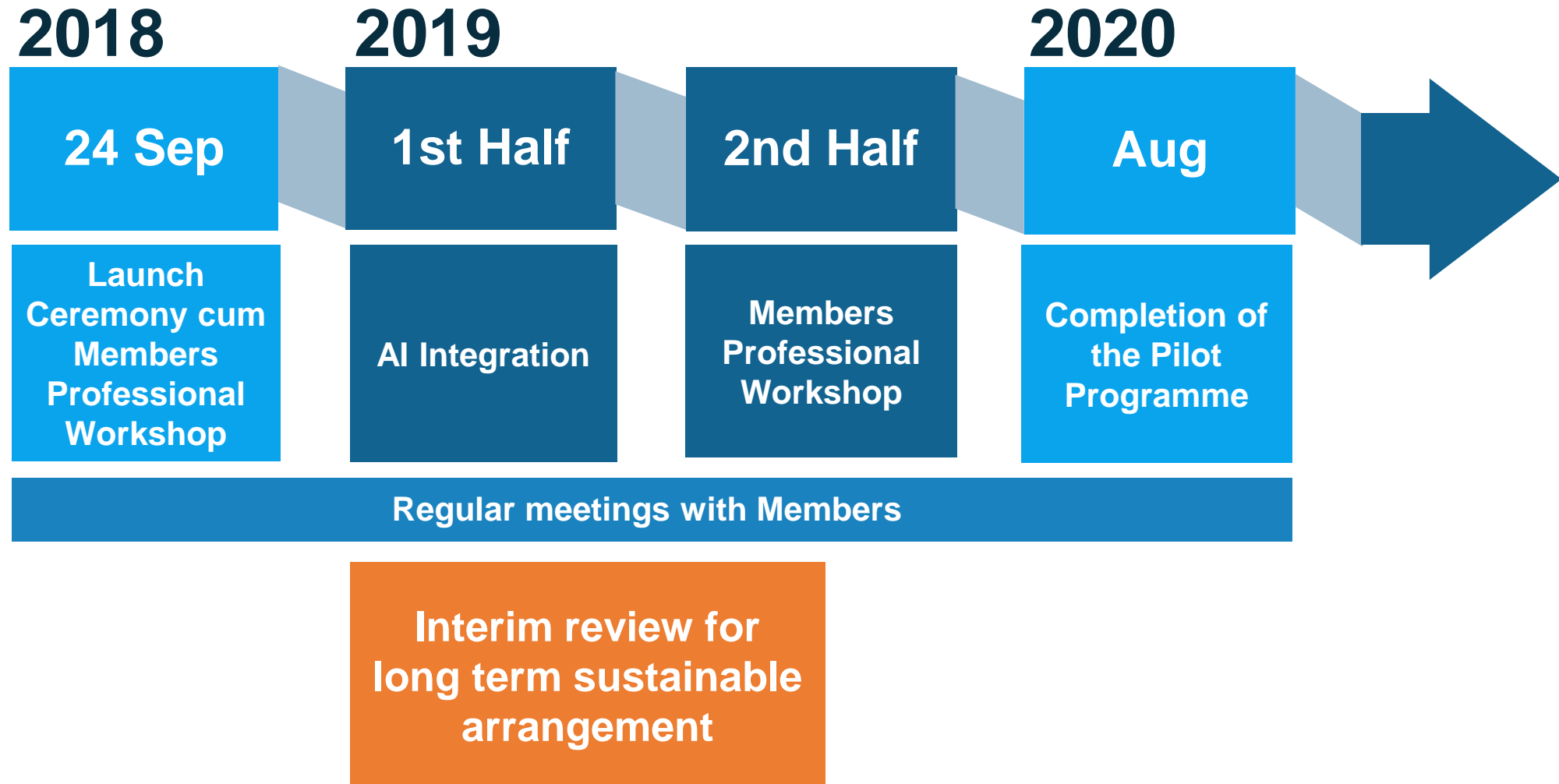


Monthly newsletter



RSS feed

Programme Timeline



網絡安全資訊共享夥伴試驗計劃

Cybersec Infohub

www.cybersechub.hk

