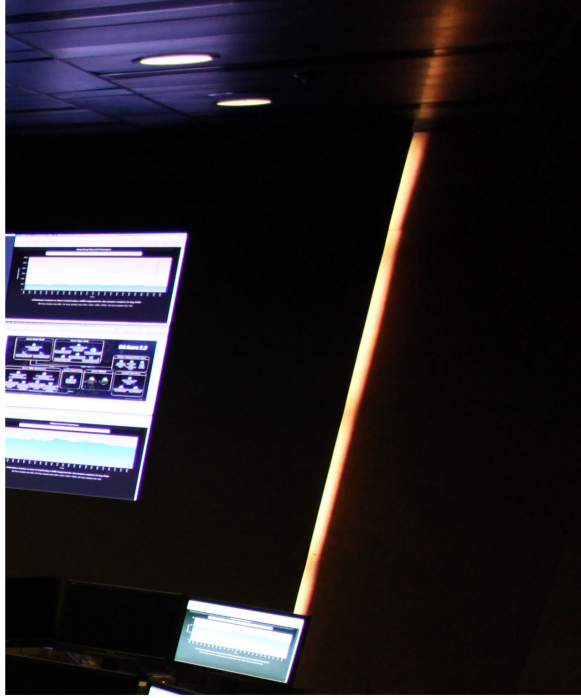
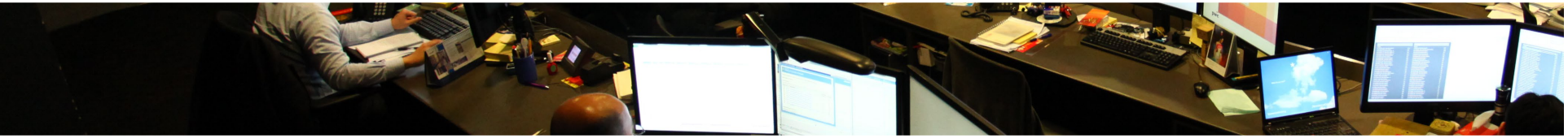
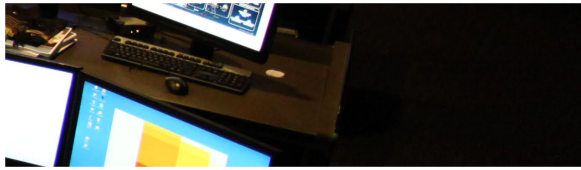
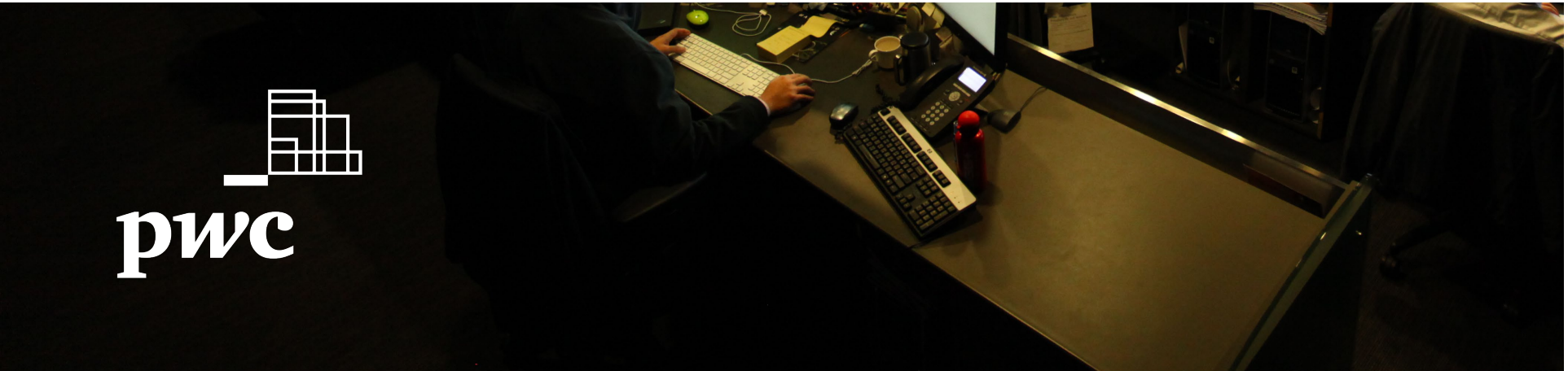
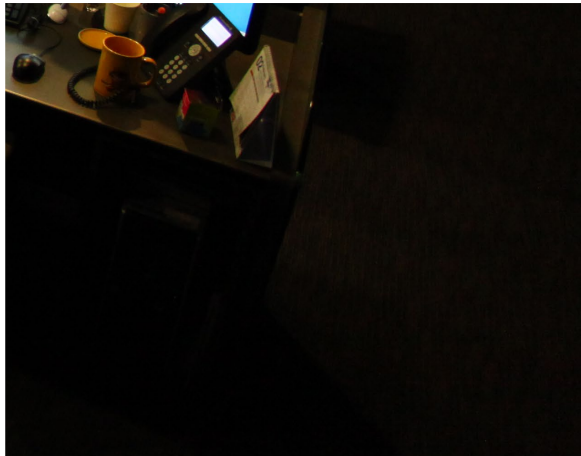
Cyber threat intelligence











pwc

Observed trends in today's global and local cyber threat landscape

Threat actors are increasingly sophisticated – Speed, Scale and Complexity

Weaponisation of CVEs
Occur mere hours after POCs released – either in public or dark web

Shift in focus to exploit Web-based Vulnerabilities due to Increased Connectivity and Digitalisation

Threat actors are Specialising and Crowdsourcing their Skillsets
And their varying motivations makes it unpredictable in root cause identification and attribution

Our value proposition

01

Threat Intelligence Monitoring and Subscription Services

Subscribe to Dark Vision, our proprietary threat intelligence platform, to enable 24x7 monitoring of your cyber hygiene. Obtain automated alerts to notify of potential risks to your:

(a) attack surface exposure (e.g., potential admin port, critical vulnerability, login portals, weak SSL certificates…

(b) dark web mentions, data leak, breached accounts, etc.

(c) young domain impersonations.

Alerts are accompanied with actionable intelligence to reduce cyber risk exposure.

02

Threat Modelling

Conduct threat modelling to identify the threat actors that may target your organisation based on your geography of operations, sector/industry, and business/security technology stack. Ascertain on a risk-based approach the MITRE ATT&CK TTPs that sophisticated adversaries would leverage to target your organisation. Evaluate the maturity of your security controls and output a cyber transformation roadmap to uplift your preventive, detective, and responsive controls.

03

Directed Research and Reporting

Receive regular and bespoke reports detailing the latest proprietary insights from our Cyber Threat Operations.

(a) Strategic Intelligence Reports for senior management and Cyber Awareness Training

(b) Tactical Intelligence Bulletins with operational insights (e.g., MITRE ATT&CK TTPs, IOCs, Yara Rules, etc.)

(c) Critical Vulnerability Alerts – out of band communications to recommend preventive/detective fixes, based on your technology stack.

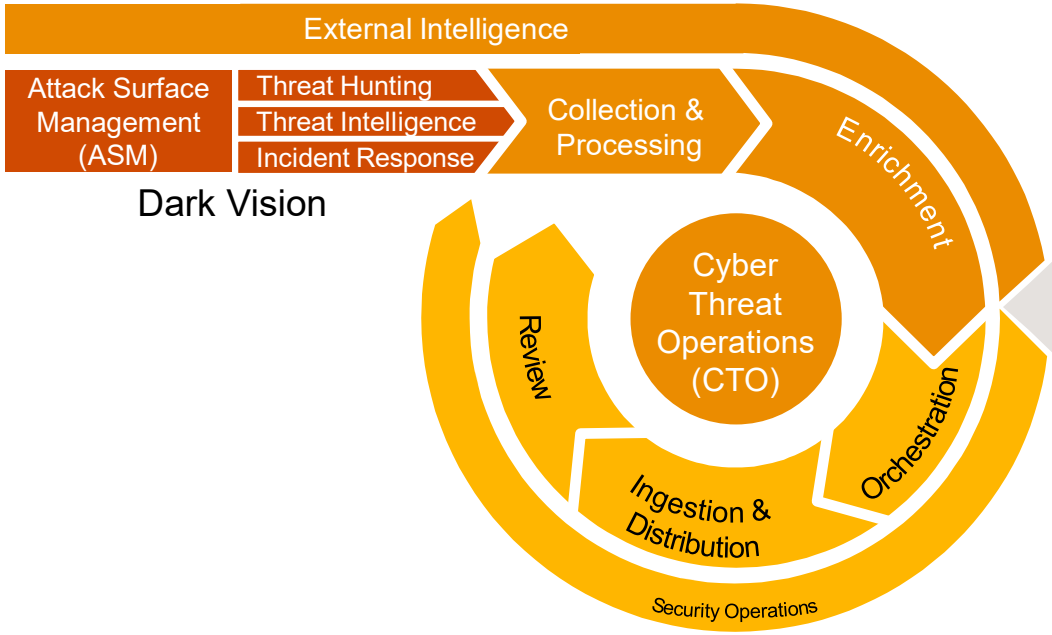
04

Cyber Threat Operations Support

Engage our team for technical support to:

- Obtain insights to expedite incident response.
- Develop tailored red-team simulation test scenarios.
- Integrate with our Malware Information Sharing Platform (MISP) to receive proprietary IOCs, TTPs and Yara Rules for enhanced security monitoring and threat hunt.

We know how to operationalise threat intelligence for proactive managed detection and response



11,820

Suspicious Young Domains detected and reported

82%

550

Threat Events' IOCs Identified by TI and ingested for SIEM's hunting

66%

72

Critical CVEs tracked and proactively alerted to likely vulnerable victims

95%

60

Cyber Incidents Responded in 2022

120%

50+

New Detection Rules Developed in Recent Year Based on DFIR and Threat Intelligence Insights

10%

Changes from 2021

Our differentiators

PwC's Dark Lab creates, uses, and enriches its own threat intelligence, across a wide variety of security services. This provides us with first hand knowledge and experience about generating and consuming threat intelligence.

Our experience developing our own threat intelligence practice, as well as our experiences working with global clients, positions us with unique insights that we deliver through our services.

In-depth global visibility of threat landscape

We leverage our global threat intelligence visibility gleaned from both open and closed sources, as well as from our incident response engagements.

We understand the local business environment

Our research goes beyond purely technical data and includes strategic intelligence, tailored towards informing business decisions and higher level security strategy.

Informed and unique intelligence

All of the intelligence derived through research conducted by our in-house experts, informed by our global incident response services and both open and closed sources.

Work closely with subject matter experts

Our technical research team comprises a blend of expert malware, intrusion and cyber intelligence analysts working alongside geopolitical and strategic research analysts. Our local team members have diverse language skills including Chinese, Russian, Korean, Arabic, and more.

Stability

Dark Lab has been active in Hong Kong for 10+ years and will continue to be operating locally to serve clients in the region and globally.

Our cyber threat intelligence team possess an array of qualifications that rival global and exceed local peers

We are structured so that our clients benefit from our global expertise, depth of technical experience, industry specialisation, cutting edge technology partnerships and scale, but **delivered through local and easily accessible teams** that you can access with a single phone call, email or instant messaging services.

Our **Hong Kong team is CREST accredited** and acts as the central hub to maintain close relationships with clients and quickly respond to alerts, requests, and incidents throughout the region.

Per request, local PwC contacts will work with your teams to understand the geographic nuances of responding to incidents in each specific location, and to establish ways of working together, and testing our response processes.

Any request for support can be acknowledged within four (4) hours by our **Hong Kong based 24x7 call centre**; specific SLAs atop of those committed in the previous slide can be adapted based on your requirements.

The PwC network has a **presence in almost every corner of the world**: our 695 offices span 152 countries, with nearly 328,000 people.

PwC has **650+ headcount** under threat intelligence, incident response, and digital forensics and **60+ forensics labs globally**.

The **CREST-accredited** PwC Cyber Threat Intelligence Team is **situated in Hong Kong**, and has procedures in place to ensure knowledge is **cascaded down to local teams** without the need for lengthy wait for them to go on-site.

Dark Lab is worldwide security certification recognised

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that: PRICEWATERHOUSECOOPERS LIMITED
19/F, Tower A,
Manulife Financial Centre
223-231 Wai Yip Street
Kwun Tong
Kowloon
Hong Kong

Holds Certificate No: IS 733108

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The provision of information security monitoring, event log management and threat intelligence services to customers by Security Operation Centre. This is in accordance with the Statement of Applicability version: 1.3, dated 9-Nov-2020.

For and on behalf of BSI:

Chris Cheung, Head of Compliance & Risk - Asia Pacific

Original Registration Date: 2020-11-19
Latest Revision Date: 2020-11-19
Effective Date: 2020-11-19
Expiry Date: 2023-11-18

Page 1 of 1

...making excellence a habit.

ISO/IEC 27001 is an international standard on managing information security. It recognised the organisation has defined and put in place best-practice information security processes.

PwC is capable of **providing information security monitoring, event log management and threat intelligence service** to customers by Security Operation Center.

CREST.

Certificate of Membership

This is to certify that

PwC Mainland China/Hong Kong

Has successfully met the CREST requirements for Membership and is a full member organization in the following disciplines

CBEST Penetration Testing | CBEST Threat Intelligence | Cyber Incident Response | Penetration Testing | STAR Penetration Testing | STAR Threat Intelligence | STAR-FS Penetration Testing | STAR-FS Threat Intelligence

Operating in Global

Ian Glover, CREST President

Date: 01/04/2021

CREST Company ID: 9534847 - 10

This Certificate is valid for one year from the date above

This Certificate remains the property of CREST (International)
Registered Office: The Pavis Building, 1 Russell Way, Slough, Berkshire SL1 1PG, UK
Company Number 6669727

CREST is an international not-for-profit **accreditation and certification body** that represents and supports the **technical information and security market**. It provides international recognised accreditations for organisations providing penetration testing, cyber incident response, threat intelligence and Security Operations Centre (SOC) services.

PwC is capable of providing **CREST-recognised Threat Intelligence and Attack Simulation services** simultaneously.

Within the APAC region, PwC Hong Kong is one of the few CREST accredited firms with locally based **CREST accredited consultants qualified** to perform testing against the CREST criteria.

PwC is one of the few firms with both ISO27001 certificated and CREST accredited globally and in APAC

We are ready!

Get in touch with us

Kenneth Wong
Cybersecurity and Privacy Leader,
Risk Assurance, Mainland China
and Hong Kong
kenneth.ks.wong@hk.pwc.com

Kok Tin Gan
Partner
Founder of Dark Lab
kok.t.gan@hk.pwc.com

Daryl Li
Partner
daryl.li@hk.pwc.com

Jenius Shieh
Partner
jenius.h.shieh@hk.pwc.com

pwchk.com