iCAST — intelligence-led Cyber Attack Simulation Testing

iCAST is a framework introduced by the Hong Kong Monetary Authority ("HKMA") in response to the changing cybersecurity landscape. Under the **HKMA Cyber Resilience Assessment Framework**, banks which aim to attain the "**intermediate**" or "**advanced**" maturity level are required to conduct iCAST. Not only is it a regulatory requirement, intelligence led simulation testing uses real-world scenarios tailored to the target organisation which can demonstrate an organisation's cyber defence capability to the board, help to measure their maturity and stay ahead of the evolving threat landscape.

What is the driver?

Financial Services is an **increasingly desirable target** for well-funded threat actors. Sophisticated malware and botnets are threatening computer networks across a wide range of sectors, in particular the FS industry.

Skilled individuals are working in **organised groups and sharing their attack techniques**. There is therefore an increased need to gain intelligence on and share these techniques in the white-hat community in order to rapidly develop tests in response to their execution in the wild.

Other regulators have been using threat intelligence-led security testing (e.g. Bank of England CBEST) , recognising the systemic risk cyber presents to industry and their responsibilities to oversee its security and resilience.

What does it involve?

Project Planning Workshops:
Conduct workshops with our cyber team to define the scope of the assessment, the targets, and attack scenarios.

Survey:
Gather information on the organisation and information from our threat intelligence team which will help to tailor our attack platform to simulate real-world attacks.

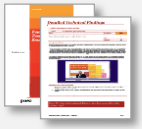
Intrusion:
Exploit vulnerabilities to gain unauthorised access to systems. Simulate actions of a real-world attacker: pivot to additional systems, maintain persistence, and avoid detection.

Assess Exposures:
Analyse weaknesses in controls and clean up affected systems. Deliver interactive workshops to feedback results. Evidence gathered throughout the test will also be used to complete a security operations maturity assessment.

Project planning & scoping → Threat intelligence → APT scenario execution → Testing setup → Analysis and Reporting

What are the outputs?

Threat intelligence report:
Our threat intelligence report will provide an in-depth overview of the current threat landscape based on our research into the organisation's key lines of services, critical assets and ongoing business relationships. Technical details on specific threat actors and scenarios will also be provided.



Security testing report:
Our assessment report will provide technical descriptions of the issues found and the recommended risk prioritised remediation actions.

Detection and response assessment report:
The detection and response assessment report will describe the overall maturity of the organisation's responses relative to the types of attack using our proprietary model. This will include high level commentary of observations made during the assessment.

What are the benefits?

Helps you understand the cyber threats facing the organisation (who, what and why) , and helps to **inform** internal risk and control assessments.

Tailored specifically to the organisation, taking into account factors that could affect its threat profile, such as: critical services, use of technology, geopolitical aspects, insider threat, third party and industry exposures.

Provides **realistic** simulation of how the organisation could be attacked. This is different from traditional testing which is often limited in scope and relies on generic tools and techniques.

Helps assess the **effectiveness** of the **detection** and **response capability**, which is different from traditional security assessment models.

pwc

iCAST — Why PwC?

Only large professional services firm with CBEST accreditation for threat intelligence and penetration testing. **1**

Only firm to offer globally coordinated end-to-end red team assessments, from testing to risk prioritised action plans. **2**

Close relations with regulators around the globe and sharing on our CBEST and local red teaming experiences. We know the hot topics in the regulators' mind and how to avoid common regulatory compliance pitfalls. **3**

Large pool of Cyber resources in China/Hong Kong with over 140 experts in Strategy & Transformation, Privacy and Consumer Protection, Implementation and Operations, and Incident and Threat Management. **4**

Our proven track record of delivering cyber attack simulations to reputable companies in Mainland China, Hong Kong and Macau. **5**

Developed a comprehensive set of KPI metrics accumulated from the extensive red teaming exercises carried out locally and globally. **6**

Our staff professional certifications:

(e.g. CREST Certified Threat Intelligence Manager; CREST Certified Simulated Attack Manager; CREST Certified Simulated Attack Specialist; CREST Registered Penetration Tester; GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) ; GIAC Penetration Tester (GPEN) ; GIAC Web Application Penetration Tester (GWAPT) ; GIAC Malware Reverse Engineering specialist (GREM) ; and GIAC Certified Incident Handler (GCIH). **7**

Our team

Kenneth Wong, Partner
Cybersecurity & Privacy National Practice Leader - China/Hong Kong
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

Marin Ivezic, Partner
Cybersecurity & Privacy
+852 2289 1817
marin.ivezic@hk.pwc.com

Felix Kan, Senior Manager
Cybersecurity & Privacy
+852 2289 1970
felix.py.kan@hk.pwc.com

Peter Tai, Senior Manager
Cybersecurity & Privacy
+852 2289 1370
peter.sy.tai@hk.pwc.com

Jason Ho, Senior Manager
Cybersecurity & Privacy
+852 2289 1213
jason.wk.ho@hk.pwc.com