SECURITYALLIANCE

iCAST - Intelligence led Cyber Attack Simulation Testing

The threat landscape for financial services in Hong Kong

The importance of the Hong Kong Banking Industry's role in the Asia Pacific (APAC) region, as well as the global financial system, necessitates continuous examination of the threats it faces from increasingly skilled adversaries.

Hong Kong is home to many systemically important financial institutions and as a consequence its resilience to cyber threats is paramount.

Despite this, it is infeasible to protect against the sheer volume and variety of cyber threats the banking industry faces. The interconnected nature of the industry and the financial sector as a whole, added to its increasing reliance on digital assets and third-party systems, is creating a large and complex attack surface.

For these reasons, industry collaboration is essential, as is the need for the industry to take an intelligence-led approach to understand the most likely and most dangerous threats, together with the supporting context necessary to prepare for them.

What is iCAST?

Intelligence-led Cyber Attack Simulation Testing (iCAST)

iCAST is a component of the Cyber Resilience Assessment Framework (C-RAF) implemented by the Hong Kong Monetary Authority (HKMA) to strengthen the cyber resilience of authorised financial institutions (banks).

Banks with High and Medium level inherent risk profiles are required to carry out iCAST exercises, along with risk and maturity assessments. The regulatory requirements aside, iCAST is the perfect solution to measure and demonstrate an organisation's cyber defence capability and maturity, by replicating bespoke intelligence-led real-world attack scenarios.

An iCAST engagement builds on industry-wide and specific cyber threat intelligence, so that critical functions and their underlying systems can be tested for their cyber resilience in a controlled manner, mimicking the techniques of the most likely and dangerous attackers. iCAST has been designed, taking into account other internationally recognised frameworks, including the CBEST framework created by Bank of England in UK.

How is iCAST different from current-day penetration testing?

A current-day penetration test typically covers a limited scope, for example the technical assessment of a single system o, application or network. A shortcoming is that more sophisticated threat actors will not just use conventional hacking techniques, but most probably leverage a variety of techniques, including spear-phishing and social engineering to target employees, the most vulnerable element of the protection of your systems, and often will use of crafted malware.

An iCAST assessment is preferably carried out on the organisation's live production environment to simulate a real-life attack, which will realistically measure how your people, processes and technology hold up against real world threats.

Benefits of iCAST

The benefit of iCAST is that delivers controlled, bespoke, intelligence-led cyber security assessments that replicate the behaviours of the threat actors that pose a genuine threat to the critical assets of an organisation. By combining accurate intelligence, based on the most likely and dangerous threats to an organisation, with a simulated attack service, Banks gain a clear understanding of their level of exposure to real cyber risks, and the potential impact to the organisation. In turn, the iCAST exercise enables the organisation to direct its cyber security budget in a more intelligent manner.

CREST. CREST STAR CBEST TIBER THE BRITISH ASSESSMENT BUREAU ISO9001 THE BRITISH ASSESSMENT BUREAU ISO27001 CYBER ESSENTIALS PLUS Crown Commercial Service Supplier

Phases of iCAST

Project planning and scoping

The organisation will outline key business and support functions, the critical services and systems under each key function. This information is used to determine the threat categories for these assets.

Developing threat intelligence analysis

The threat intelligence will enable the iCAST engagement to be tailored to the specific organisation to focus on TTPs (tactics, techniques and procedures) of threat actors that would most likely target the organisation.

Developing testing scenarios

Several testing scenarios are developed to simulate real life attacks. Each scenario has a story line that includes the test goals, initiation of the test, chain of tasks, milestones, timeline and conditions of continuing or stopping the testing activity.

Intelligence led testing

During the testing phase the test team will carry out actions outlined in the testing scenarios and gathering evidence of possible execution of the outlined actions. The test team will closely communicate with the organisation to provide updates regarding the testing activity.

Reporting

Once testing is complete, the iCAST simulation test summary, threat intelligence report and simulation testing report are produced. The iCAST simulation test summary is created to outline the recommended way forward, remediate the problems found and create a strategy to improve the overall cyber security posture of the organisation.

Generic Threat Intelligence

Security Alliance has authored a Generic Threat Assessment document for companies with medium inherit risk level that is available for purchase.

Intelligence-led simulated tests

An iCAST engagement takes the same Cyber Threat Intelligence Assessment output and adds a layer of actual, simulated attack penetration tests on top. This methodology uses the same framework that Security Alliance use for their CREST STAR and CBEST assessments. The testing team use the simulated attack scenarios generated in the iCAST Report to:

- Reflect the real risks and vulnerabilities defined according to evidence
- Mimic the methodologies and attack vectors of defined threat actors, on assets and targets known to be valuable
- Measure your ability to detect and respond to attacks based on real threats

The additional benefits of conducting a full iCAST engagement over and above an Intelligence assessment are the additional reporting and additional strategies that become available after testing. Detailed testing reports that include remediation advice can help define and guide the cyber security strategy of an organisation on a continuous risk and response basis.

Why Security Alliance is different

As a CREST registered company and a CBEST approved supplier of Threat Intelligence services, Security Alliance delivers against recognised frameworks with our team of seasoned cyber intelligence professionals and experienced penetration testers. With a global understanding of the hybrid and complex threat landscape, Security Alliance is working with some of the world's leading intelligence and risk-based security providers.

We combine the field experience of our highly trained intelligence staff with the deep specialisations of penetration testers, to bring you the highest quality services, designed and delivered by experts. Every client engagement at Security Alliance is unique, and our threat intelligence is generated based on each client's individual profile.